Seminar Homological Algebra
The axiom of infinity

Kobe Wullaert

Abstract

In this paper we introduce the notion of the *natural number object* in a topos which generalizes the set of natural numbers to an object in an arbitrary topos (if it exists). After recalling the basics of the internal logic of a topos, we show that the natural number object satisfies the Peano axioms (in the internal logic) and that conversely an object with satisfies those axioms is the natural number object. This characterization even allows us to give two more characterizations and we can do arithmetic and trichotomy internally on this object. At the end we also discuss shortly the notion of a finite object in a topos and look at finite cardinals which are particular kind of finite objects in a topos with a natural number object.

1 The natural number object

This paper is based on ([1]). We will use the definitions and results of chapters 5 and 6.

Definition 1. *Let $\mathcal{E}$ be a (elementary) topos with terminal object $\mathbf{1}$. A **natural number object** in $\mathcal{E}$ is an object $\mathbb{N}$ together with morphisms $0 : \mathbf{1} \to \mathbb{N}, s : \mathbb{N} \to \mathbb{N}$ which are universal in the following sense: If there is another triple $(M, m : \mathbf{1} \to M, \sigma : M \to M)$, then there exists a unique factorization $\mu : \mathbb{N} \to M$ such that the following diagrams commute:*

$$\begin{array}{ccc} \mathbf{1} & \xrightarrow{0} & \mathbb{N} \\ & \searrow^{m} & \downarrow \mu \\ & & M \end{array} \quad , \qquad \begin{array}{ccc} \mathbb{N} & \xrightarrow{s} & \mathbb{N} \\ \downarrow \mu & & \downarrow \mu \\ M & \xrightarrow{\sigma} & M \end{array}$$

*The morphism 0 is called **zero** and s the **successor morphism**.*

The following lemma is a standard argument by the use of uniqueness of μ:

Lemma 1. *If a natural number object exists, it is unique up to isomorphism.*

Example 1.

- *Let $\mathcal{E} = \mathbf{Set}$ be the category of sets (with functions). The natural number object is then given by $\mathbb{N}$ (the set of natural numbers), $0 : \mathbf{1} \to \mathbb{N}$ the (constant) function 0 and $s : \mathbb{N} \to \mathbb{N} : n \mapsto n+1$ the successor.*
- *The category* **FinSet** *of finite sets (with functions) is a topos but it has no natural number object.*

  Proof. In order to show that $(\mathbb{N}, 0, s)$ is indeed a n.n.o. for **Set**, let $(M, m : \mathbf{1} \to M, \sigma : M \to M)$ be another triple in **Set**, define $\mu : \mathbb{N} \to M$ inductively by:

$$\mu(0) = m, \quad \forall n \in \mathbb{N} : \mu(n+1) = \sigma(\mu(n)).$$

  The commutativity conditions are automatically satisfied and we clearly have the uniqueness.
  Assume that **FinSet** has a n.n.o. We show in corollary (1), that the successor morphism must be a monomorphism, but any injection from a finite set to itself is always a bijection, so we can assume the natural number object (if it exists) would be a set of the form $[n] := \{0, 1, \cdots n-1\}$ where the zero and successor maps are given by:

$$0 : \{\star\} \to [n] : \star \mapsto 0, \quad [n] \xrightarrow{Id} [n] : m \mapsto m.$$

So if one considers the same data on $[n+1]$, we have that

$$i : [n] \to [n+1] : m \mapsto m, \quad j : [n] \to [n+1] : m \mapsto \begin{cases} (m+1), & \text{if } m > 0 \\ 0, & \text{if } m = 0 \end{cases}$$

makes the following diagrams commute:

$$\begin{array}{ccccc} [1] & \xrightarrow{0} & [n] & \xrightarrow{Id} & [n] \\ & \searrow^{0} & \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle i} \\ & & [n+1] & \xrightarrow{Id} & [n+1] \end{array} \qquad \begin{array}{ccccc} [1] & \xrightarrow{0} & [n] & \xrightarrow{Id} & [n] \\ & \searrow^{0} & \downarrow{\scriptstyle j} & & \downarrow{\scriptstyle j} \\ & & [n+1] & \xrightarrow{Id} & [n+1] \end{array}$$

but this contradicts the uniqueness of the factorization. □

Lemma 2. *Let $(\mathbb{N}, 0, s)$ be a n.n.o. in a topos $\mathcal{E}$. Then*

$$\mathbf{1} \xrightarrow{0} \mathbb{N} \xleftarrow{s} \mathbb{N},$$

is a coproduct diagram.

Proof. Consider the coproduct diagram:

$$\mathbf{1} \xrightarrow{s_1} \mathbf{1} \bigsqcup \mathbb{N} \xleftarrow[s_{\mathbb{N}}]{} \mathbb{N}$$

By the universal property of the coproduct, there exists a morphism $(0, s) : \mathbf{1} \bigsqcup \mathbb{N} \to \mathbb{N}$ such that

$$0 = (0, s) \circ s_1, \quad (0, s) \circ s_{\mathbb{N}} = s.$$

So the following diagram commutes:

$$\begin{array}{ccccc} \mathbf{1} & \xrightarrow{s_1} & \mathbf{1} \bigsqcup \mathbb{N} & \xrightarrow{s_{\mathbb{N}} \circ (0,s)} & \mathbf{1} \bigsqcup \mathbb{N} \\ & \searrow^{0} & \downarrow{\scriptstyle (0,s)} & & \downarrow{\scriptstyle (0,s)} \\ & & \mathbb{N} & \xrightarrow{s} & \mathbb{N} \end{array}$$

By (the existence of) the universal property of $\mathbb{N}$, there exists a g such that the following diagram commutes:

$$g \circ 0 = s_1, g \circ s = s_{\mathbb{N}} \circ (0, s) \circ g.$$

So we have that the following diagram commutes:

$$\begin{array}{ccccccc} \mathbf{1} & \xrightarrow{0} & \mathbb{N} & \xrightarrow{s} & \mathbb{N} \\ & \searrow^{s_1} & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle g} \\ & \searrow^{0} & \mathbf{1} \bigsqcup \mathbb{N} & \xrightarrow{s_{\mathbb{N}} \circ (0,s)} & \mathbf{1} \bigsqcup \mathbb{N} \\ & & \downarrow{\scriptstyle (0,s)} & & \downarrow{\scriptstyle (0,s)} \\ & & \mathbb{N} & \xrightarrow{s} & \mathbb{N} \end{array}$$

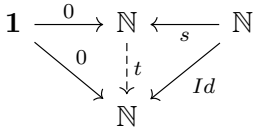
By the uniqueness of the universal property of $\mathbb{N}$, we conclude $(0, s) \circ g = Id_{\mathbb{N}}$.
That $g \circ (0, s) = Id_{\mathbf{1} \bigsqcup \mathbb{N}}$ holds follows from the uniqueness of the universal property of the pushout together with:

$$\begin{aligned} g \circ (0, s) \circ s_1 &= g \circ 0 = s_1 \\ g \circ (0, s) \circ s_2 &= g \circ s = s_{\mathbb{N}} \circ (0, s) \circ g = s_{\mathbb{N}} \end{aligned}$$

So we conclude that g and $(0, s)$ are eachother inverses which shows the claim. □

Corollary 1. *Let $(\mathbb{N}, 0, s)$ be a n.n.o. Then are 0 and s monomorphisms.*

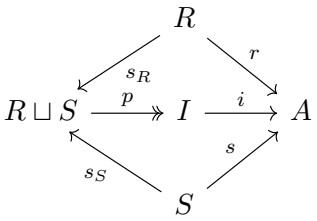
Proof. That 0 is a monomorphism is clear because it is a morphism starting from the terminal object. By the universality of the coproduct, there exists a $t : \mathbb{N} \to \mathbb{N}$ such that the following diagram commutes:



So because $t \circ s = Id_{\mathbb{N}}$, we conclude that s is a (split) monomorphism. □

Corollary 2. *Let $(\mathbb{N}, 0, s)$ be a n.n.o. Write $S_{\mathbf{1}}$ and $S_{\mathbb{N}}$ for the subobjects of $\mathbb{N}$ corresponding to 0 and s. Then $\mathbb{N} = S_{\mathbf{1}} \cup S_{\mathbb{N}}$.*

Proof. Recall that the union of (general) subobjects $r : R \to A$ and $s : S \to A$ is defined as follows. Let $(R \sqcup S, s_R, s_S)$ be the coproduct of r and s. This induces a (unique) morphism $R \sqcup S \to A$. This in general is not a monomorphism (and thus not induces a subobject), but in any topos we have an epi-mono factorization, so we factorize it through its image I. The union is then the monomorphism $i : I \to A$. Visually this is given by the following (commutative) diagram:

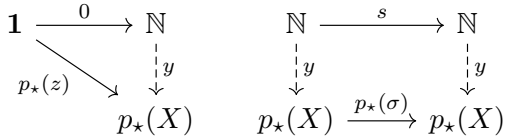


So applying this to $S_{\mathbf{1}}$ and $S_{\mathbb{N}}$: We have from lemma 2 that $\mathbb{N} \sqcup \mathbf{1} \xrightarrow{(0,s)} \mathbb{N}$ is an isomorphism, so its image is also $\mathbb{N}$ which is therefore the union. □

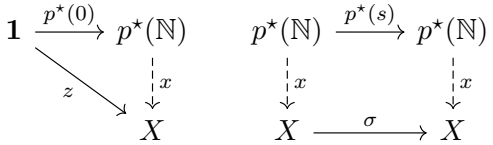
To show that each Grothendieck topos has a natural numbers object, we use the following lemma:

Lemma 3. *Let $p \equiv (p_\star, p^\star) : \mathcal{E} \to \mathcal{F}$ be a geometric morphism between (elementary) topoi. If $\mathcal{F}$ admits a natural number object $(\mathbb{N}, 0, s)$, it is preserved by $p^\star$. And hence also $\mathcal{E}$ has a n.n.o.*

Proof. Recall that p being a geometric morphism means that $p^\star \dashv p_\star$ and $p^\star$ is left exact, i.e. preserves finite limits.
We have to show that $(p^\star(\mathbb{N}), p^\star(0), p^\star(s))$ is the natural number object for $\mathcal{E}$. Let $z \in \mathcal{E}(\mathbf{1}, X)$ and $\sigma \in \mathcal{E}(X, X)$. The universal property of the natural number object yields a unique $y \in \mathcal{F}(\mathbb{N}, p_\star(X))$ such that the following diagrams commute (also using that $p_\star$ preserves the terminal object since $p_\star$ preserves limits as a right adjoint):



where y is the (unique) morphism given by the universal property of the natural number object.
Let $\eta : Id_{\mathcal{F}} \implies p_\star p^\star$ be the unit of adjunction $p^\star \dashv p_\star$. Then y corresponds with a unique $x \in \mathcal{E}(p^\star(\mathbb{N}), X)$ such that $p_\star(x) \circ \eta_{\mathbb{N}} = y$. We now show that x is the (unique) factorization such that the following diagrams commute:



Thus:

$$\begin{aligned} p_\star(\sigma \circ x) \circ \eta_{\mathbb{N}} &= p_\star(\sigma) \circ p_\star(x) \circ \eta_{\mathbb{N}} \\ &= p_\star(\sigma) \circ y \\ &= y \circ s \\ &= p_\star(x) \circ \eta_{\mathbb{N}} \circ s \\ &= p_\star(x) \circ p_\star p^\star(s) \circ \eta_{\mathbb{N}}, \quad \text{naturality of } \eta \\ &= p_\star(x \circ p^\star(s)) \circ \eta_{\mathbb{N}} \end{aligned}$$

By the bijection between the hom-sets of the adjunction, we conclude that $\sigma \circ x = x \circ p^\star(s)$.
Since $p_\star$ and $p^\star$ preserve the terminal object, we have that $\eta_{\mathbf{1}} : \mathbf{1} \to p_\star p^\star(\mathbf{1})$ is the identity on $\mathbf{1}$, thus

$$\begin{aligned} p_\star(x \circ p^\star(0)) \circ \eta_{\mathbf{1}} &= p_\star(x) \circ p_\star(p^\star(0)) \circ \eta_{\mathbf{1}} \\ &= p_\star(x) \circ \eta_{\mathbb{N}} \circ 0 \\ &= y \circ 0 \\ &= p_\star(z) \\ &= p_\star(z) \circ \eta_{\mathbf{1}} \end{aligned}$$

From which we conclude that $x \circ p^\star(0) = z$ (again using that we have a bijection between the hom-sets). So it remains to show the uniqueness of x. Assume that $\tilde{x} : p^\star(\mathbb{N}) \to X$ also satisfy the

$$\tilde{x} \circ p^\star(0) = z, \quad \tilde{x} \circ p^\star(s) = \sigma \circ \tilde{x}.$$

Consider its corresponding morphism $\tilde{y} : \mathbb{N} \to p_\star(X)$. We then have:

$$\begin{aligned} p_\star(\sigma) \circ \tilde{y} &= p_\star(\sigma) \circ p_\star(\tilde{x}) \circ \eta_{\mathbb{N}} \\ &= p_\star(\tilde{x}) \circ p_\star(p^\star(s)) \circ \eta_{\mathbb{N}} \\ &= p_\star(\tilde{x}) \circ \eta_{\mathbb{N}} \circ s \\ &= \tilde{y} \circ s \\ \tilde{y} \circ 0 &= p_\star(\tilde{x}) \circ \eta_{\mathbb{N}} \circ 0 \\ &= p_\star(\tilde{x}) \circ p_\star(p^\star(0)) \circ \eta_1, \quad \text{by naturality of } \eta \\ &= p_\star(z), \quad \text{since } \tilde{x} \circ p^\star(0) = z, \end{aligned}$$

So by the uniqueness of y, we conclude $y = \tilde{y}$ and thus (by the bijection between the hom-sets) $x = \tilde{x}$. □

Corollary 3. *Every grothendieck topos $\mathcal{E}$ has a natural number object.*

Proof. Since this is the case in **Set** (example (1)), it suffices to find a geometric morphism $(p_\star, p^\star) : \mathcal{E} \to \mathbf{Set}$ from which we conclude the statement by the previous lemma.
Every grothendieck topos has a (unique) geometric morphism $\Gamma : \mathcal{E} \to \mathbf{Set}$ where the left adjoint part is given by

$$\Gamma^\star : \mathbf{Set} \to \mathcal{E} : X \mapsto \bigsqcup_X \mathbf{1}.$$

Notice that this indeed defines a unique geometric morphism because the left adjoint preserves coproducts. That this indeed defines a geometric morphism can be found in [1] (proposition (4.1.4)). □

1.1 Prerequisites internal logic

In this section we recall the notions of the internal logic of an (elementary) topos. More detailed information can be found in chapter 6 of [1]. Let $\mathcal{E}$ be an elementary topos with subobject classifier Ω and terminal object $\mathbf{1}$.

Definition 2. *("**Mitchell-Bénabou language**") The **internal logic** of $\mathcal{E}$ consists of the following data:*

- *The types are given by the objects;*
- *For each type (i.e. object of $\mathcal{E}$), there are variables;*
- *For each global element $\mathbf{1} \to X$, there is a constant of type X*

The terms and formulas are recursively defined as follows:

- *Each constant of type X is a term of type X without free variables;*
- *Each variable x of type X is a term of type X with x its unique free variable;*
- *If τ is a term of type X and $f : X \to Y$ a morphism, then is $f(\tau)$ a term of type Y with the same free variables as τ;*
- *If $\tau_1 \cdots \tau_n$ are terms of types $X_1, \cdots, X_n$ with all the same free variables, then is $(\tau_1, \cdots, \tau_n)$ a term of type $X_1 \times \cdots \times X_n$ with the same free variables;*
- *The terms of type Ω are called formulas;*
- *We have formulas $true$ and $false$ without free variables;*
- *If ϕ is a formula with free variables $x_1, \cdots, x_{n+k}$ of types $X_1, \cdots, X_{n+k}$, then is $\{(x_1, \cdots, x_n | \phi\}$ a term of $\Omega^{X_1 \times \cdots \times X_n} = \mathbb{P}(X_1 \times \cdots \times X_n)$ with free variables $x_n, \cdots, x_{n+k}$;*
- *If τ, σ are terms of type X with the same free variables, then is $\tau = \sigma$ a formula with the same free variables;*
- *If τ is a term of type X and Σ a term of type Ω^X having both the same free variables, then is $\tau \in \Sigma$ a term of the same free variables;*
- *If ϕ is a formula, then is $\neg\phi$ a formula with the same free variables;*
- *If ϕ and ψ are formulas with the same free variables, then are $\phi \wedge \psi$, $\phi \vee \psi$ and $\phi \implies \psi$ formulas with the same free variables;*
- *If ϕ is a formula with free variables $x, x_1, \cdots, x_n$ of types $X, X_1, \cdots, X_n$, then are $\forall x \phi$ and $\exists x \phi$ formulas with free variables $x_1, \cdots, x_n$.*

This list is not complete, but this is not necessary for the sequel. The complete definition is definition 6.1.1 *in chapter* 6 *of [1].*

*Each term τ of X and with free variables of types $X_1, \cdots, X_n$ is given an **interpretation**, that is a morphism $\lceil \tau \rceil : X_1 \times \cdots \times X_n \to X$. These interpretations are also defined recursively, for example: If τ is a term of type X and interpreted by $\lceil \tau \rceil$ and $f : X \to Y$ a morphism, then is $f(\tau)$ interpreted as $\lceil f(\tau) \rceil := f \circ \lceil \tau \rceil$.*
*If ϕ is a formula and interpreted by $\lceil \phi \rceil : X_1 \times \cdots \times X_n \to \Omega$, then is ϕ **universally valid** if its interpretation $\lceil \phi \rceil$ factors through the morphism $true : \mathbf{1} \to \Omega$ and we then write $\vDash \phi$.*

Recall that intuitionistic logic is classical logic where we do not have the law of excluded middle, that is $p \vee \neg p$ is not necessarily true.

Theorem 1. *The axioms of the intuitionistic propositional -and predicate logic and set theory (without the axiom of infinity) are universally valid in the internal logic.*

That the axioms of propositional (resp. predicate) logic hold is theorem 6.7.1 (resp. theorem 6.8.1) in [1]. Section 6.9 in [1] is dedicated to proving the axioms of set theory.
In [1], all the axioms are labeled (always starting with T and ending with a number), we will now list some axioms/rules (together with their labeling) which are universally valid and which we'll use in the sequel.

- Modus Ponens ($T11$): If $\vDash \phi$ and $\vDash \phi \implies \psi$, then $\vDash \psi$ (a certain condition has to be true which is automatically true if ϕ and ψ have the same free variables).
- $(T12) + (T13)$: $\vDash \phi \wedge \psi$ if and only if $\vDash \phi$ and $\vDash \psi$.
- $(T31) :\vDash ((\phi \implies \psi) \wedge (\phi \implies \theta)) \implies (\phi \implies (\psi \wedge \theta))$.
- $(T53) : (\vDash \phi) \implies (\vDash \forall x \phi)$.
- $(T55)$: if $\vDash \phi \implies \psi$, then $\vDash \exists x \phi \implies \exists x \psi$.
- Axiom of extensionality: $(T92) :\vDash \forall a\, (a \in S \iff a \in R) \implies (S = R)$, where S, R are variables of type the powerobject of the type of a.

In the rest of this paper we will write both τ for the *abstract* term as for its interpretation and if a formula ϕ has a free variable of type X, we sometimes write $\phi : X$.
An important technique/result is the **localization principle** (proposition 6.6.25): A formula is universally valid in every topos if one can prove it in the case where the variables are replaced by global elements (of the corresponding type).
It it is important to note that this principle does not apply if we work with some fixed topos and use its particular structure.

1.2 Peano arithmetic

In this section, we show that the notion of a natural number object can be equivalently described using the internal logic.

Definition 3. *Let $\mathcal{E}$ be a topos. A **model of Peano arithmetic** in $\mathcal{E}$ is an object $\mathbb{N}$ together with morphisms $0 : \mathbf{1} \to \mathbb{N}, s : \mathbb{N} \to \mathbb{N}$ such that the following properties hold:*

(P1) $\vDash (n = 0) \vee \exists m (n = s(m))$

(P2) $\vDash \neg (s(n) = 0)$

(P3) $\vDash (s(n) = s(m)) \implies (n = m)$

(P4) $\vDash (0 \in P \wedge \forall n (n \in P \implies s(n) \in P)) \implies (P = \mathbb{N})$

where $n, m : \mathbb{N}$ and $P : \Omega^{\mathbb{N}}$.

The goal of this section to show that there is an equivalence between natural number objects and these models of Peano arithmetic.

Recall that a logical morphism (between topoi) is a functor which preserves finite limits, the subobject classifier and the cartesian closedness.

Lemma 4. *Every logical morphism $F : \mathcal{E} \to \mathcal{F}$ between topoi preserve models of Peano arithmetic.*

Proof. First notice that a logical morphism preserves the terminal object, thus if $(\mathbb{N}, 0, s)$ is a model of peano arithmetic in $\mathcal{E}$, its image also induces the data to be a model of Peano arithmetic. So we then have to check that F preserves the truth tables (here we need that the subobject classifier is preserved), i.e. it preserves the Heyting algebra structure on every poset of subobjects (on a given object) and the left and right adjoint of the pullback functor must be preserved so that the quantifier morphisms are preserved. This is shown in proposition 6.5.1 in [1]. □

Let $X \in \mathcal{E}$ be an object. We denote by $\mathcal{E}/X$ the slice category over X.

Proposition 1. *Let $\mathcal{E}$ be a topos and $X \in \mathcal{E}$ an object. The functor*

$$\mathcal{E} \to \mathcal{E}/X : A \mapsto (p_X : A \times X \to X),$$

preserves both the natural number object and models of Peano arithmetic.

Proof. Let $\mathbf{1}$ be the terminal object of $\mathcal{E}$. Since $\mathcal{E} \cong \mathcal{E}/\mathbf{1}$, we have that the functor is the pullback functor induced by the unique morphism $X \to \mathbf{1}$ (where $\mathbf{1}$ is the terminal object). So by the fundamental theorem of topoi (theorem 5.8.4 in [1]), this has both a left and right adjoint and thus together with its right adjoint it forms a geometric morphism (this functor indeed preserves finite limits as it has a left adjoint) and thus preserves the n.n.o.
Since this functor is logical (see for example proposition 5.11.2 in [1]), we conclude from the previous lemma that it therefore preserves models of Peano arithmetic. □

Proposition 2. *A n.n.o.* $(\mathbb{N}, 0, s)$ *in a topos* $\mathcal{E}$ *is a model of Peano arithmetic.*

Proof. Write S_1 and $S_{\mathbb{N}}$ for the subobjects corresponding to 0 and s. By corollary (2), we have

$$\mathbb{N} = S_1 \cup S_{\mathbb{N}} = \{a : \mathbb{N} | (a \in S_{\mathbf{1}}) \vee (a \in S_{\mathbb{N}})\}.$$

Thus

$$\vDash (n \in S_{\mathbf{1}}) \vee (n \in S_{\mathbb{N}}). \tag{1}$$

But $\vDash n \in S_{\mathbf{1}}$ means that n factorizes through 0 and the only morphism which does that is 0 itself, so we have $\vDash (n \in S_{\mathbf{1}}) \iff (n = 0)$.
Since $Im(s) = \{n | \exists m : n = s(m)\}$, we have

$$\vDash (n \in S_{\mathbb{N}}) \iff \exists m : (n = s(m)).$$

Thus equation (1) is equivalent to

$$\vDash (n = 0) \vee \exists m : (n = s(m)),$$

which is precisely $(P1)$.
To show $(P2)$, we also use $S_{\mathbf{1}}$ and $S_{\mathbb{N}}$ (as in the first part of this proof). Since finite coproducts are disjoint in any topoi (this is corollary 5.9.11 in [1]), we have $S_{\mathbf{1}} \cap S_{\mathbb{N}} = \emptyset$ (the initial object), thus

$$\begin{aligned}
\vDash s(n) = 0 \quad &\implies \quad (0 \in S_{\mathbf{1}}) \wedge (0 \in S_{\mathbb{N}}), \quad \text{since } 0 = s(n) \in Im(s) = S_{\mathbb{N}} \\
&\implies \quad 0 \in S_{\mathbf{1}} \cap S_{\mathbb{N}}, \ \text{since} S_{\mathbf{1}} \cap S_{\mathbb{N}} = \{a | a \in S_{\mathbf{1}} \wedge S_{\mathbb{N}}\} \\
&\implies \quad 0 \in \emptyset \\
&\implies \quad \exists x (x \in \emptyset), \quad \text{since } (\vDash \phi(t)) \implies \vDash \exists x \phi \\
&\implies \quad \textbf{false}, \quad \text{since the initial object is the unique object such that } \vDash \neg(\exists x : x \in \emptyset)
\end{aligned}$$

Since $\neg\phi \equiv (\phi \implies \textbf{false})$, we thus conclude $\vDash \neg(s(n) = 0)$ which is precisely $(P2)$.
We know by corollary (1) that s is a monomorphism which is precisely $(P3)$.
To show $(P4)$:

$$\vDash (0 \in P) \wedge \forall n (n \in P \implies s(n) \in P)) \implies (P = \mathbb{N}),$$

it suffices to show that

$$\vDash (0 \in P \wedge \forall n (n \in P \implies s(n) \in P)), \tag{2}$$

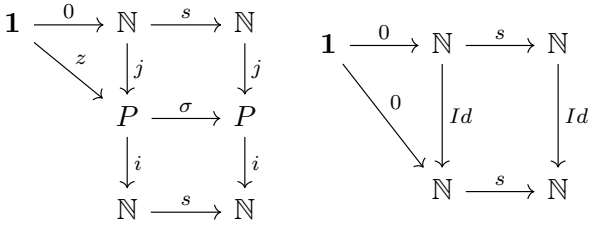
implies $\vDash P = \mathbb{N}$ by the principle of localization where $i : P \to \mathbb{N}$ is a subobject.
Equation (2) is equivalent to

$$\vDash (0 \in P), \quad \text{and } \vDash \forall n (n \in P \implies s(n) \in P).$$

So this translates to showing that if $0 : \mathbf{1} \to \mathbb{N}$ factors through P and $s : \mathbb{N} \to \mathbb{N}$ restricts to P, then $P = \mathbb{N}$.
Write $z : \mathbf{1} \to \mathbb{N}$ for the factorization of 0 and $\sigma := s|_P : P \to P$ for the restriction of s to P. So we have the following data:

$$\mathbf{1} \xrightarrow{z} P \xrightarrow{\sigma} P.$$

Thus by the universal property of the n.n.o. $(\mathbb{N}, 0, s)$, there exists a unique morphism $j : \mathbb{N} \to P$ such that $z = j \circ 0$ and $\sigma \circ j = j \circ s$. In particular we have that the following diagrams commutative:



So by the uniqueness of the universal property of the natural number object we have that $Id_{\mathbb{N}} = i \circ j$, thus i is a (split) epimorphism. But since i is also a monomorphism we have that i is an isomorphism, thus $P = N$. So we indeed have $(P4)$ which shows the proposition. □

Remark 1. *Notice that in the proof of the previous proposition, we have that $(P1), (P2)$ and $(P3)$ are universally valid as a consequence of lemma (2) and corollaries (2, 1). These corollaries only use the lemma, so without using the universality of the n.n.o.*

Proposition 3. *("**The principle of induction**") Let $\mathcal{E}$ be a topos with a model $(\mathbb{N}, 0, s)$ of Peano arithmetic. Let ϕ be a formula (with a single free variable of type $\mathbb{N}$). The following are equivalent:*

1. $\vDash \phi$;
2. $\vDash \phi(0)$ *and* $\vDash \phi(n) \implies \phi(s(n))$.

Proof. $(1 \implies 2)$: This follows from

$$(\vDash \phi) \implies (\vDash \forall m : \phi(m)) \implies \begin{cases} \vDash \phi(0) \\ \vDash \phi(s(n)) \end{cases}$$

where we note that since $\vDash \phi(s(n))$ hold, we definitely have $\vDash \phi(n) \implies \phi(s(n))$.
$(2 \implies 1)$: Let $P := \{n|\phi\}$. Since 2 holds we have

$$\begin{aligned} & (\vDash 0 \in P) \text{ and } (\vDash \phi(n) \implies \phi(s(n))) \\ \implies \quad & (\vDash 0 \in P) \text{ and } (\vDash \forall n : \phi(n) \implies \phi(s(n))) \\ \implies \quad & \vDash (0 \in P \wedge \vDash \forall n : \phi(n) \implies \phi(s(n))) \end{aligned}$$

So $(P4)$ implies that $P = \mathbb{N}$ which shows the proposition. □

Proposition 4. *A model of Peano arithmetic $(\mathbb{N}, 0, s)$ in a topos $\mathcal{E}$ is a natural number object.*

Proof. Let $X \in \mathcal{E}$ be an object and $z \in \mathcal{E}(\mathbf{1}, X), \sigma \in \mathcal{E}(X, X)$ be morphisms. We have to show that there exists a unique $g : \mathbb{N} \to X$ such that $z = g \circ 0$ and $\sigma \circ g = g \circ s$.
Consider the subobject $\mathcal{P}$ of $\Omega^{\mathbb{N} \times X}$ defined by:

$$\mathcal{P} := \left\{ P : \Omega^{\mathbb{N} \times X} | \, ((0, z) \in P) \wedge (\forall n \forall x : ((n, x) \in P \implies (s(n), \sigma(x)) \in P)) \right\},$$

and let G be its intersection, i.e.

$$G := \bigcap \mathcal{P} = \{(n, x) | \forall P (P \in \mathcal{P} \implies (n, x) \in P)\}.$$

To get a morphism $g : \mathbb{N} \to X$, we prove

$$\vDash \forall n \exists! x (n, x) \in G, \tag{3}$$

from which we deduce that there exists a unique morphism g such that

$$\vDash \forall n (n, g(n)) \in G.$$

We show equation (3) by induction, thus it suffices to show:

1. $\vDash \exists x(0,x) \in G$,
2. $\vDash \forall x \forall y \left(((0,x) \in G \wedge (0,y) \in G) \implies x = y\right)$,
3. $\vDash (\exists x(n,x) \in G) \implies (\exists x(s(n),x) \in G)$,
4. $\vDash \forall x \forall y \left((n,x) \in G \wedge (n,y) \in G \implies x = y\right) \implies \forall x \forall y \left((s(n),x) \in G \wedge (s(n),y) \in G \implies x = y\right)$

By definition of $\mathcal{P}$, we have

$$\vDash \forall P \left(P \in \mathcal{P} \implies (0,z) \in P\right).$$

Thus $\vDash (0,z) \in G$, thus (by $(T52)$) we conclude (1).
By $(T53)$, to show (2), it suffices to show

$$\vDash ((0,x) \in G \wedge (0,y) \in G) \implies x = y.$$

Since $(0,z) \in G$, it therefore suffices to show

$$\vDash (0,x) \in G \implies x = z.$$

For a term P of type $\Omega^{\mathbb{N} \times X}$, define the term (of same type):

$$\alpha(P) := \{(n,y) | (n,y) \in P \wedge (n = 0 \implies y = z)\}.$$

We first claim

$$\vDash P \in \mathcal{P} \implies \alpha(P) \in \mathcal{P}. \tag{4}$$

indeed:

$$\begin{array}{lll}
\vDash P \in \mathcal{P} \wedge (n,y) \in \alpha(P) & \implies & P \in \mathcal{P} \wedge (n,y) \in P \wedge (n = 0 \implies y = z), \quad \text{by definition of } \alpha(P) \\
& \implies & (s(n), \sigma(y)) \in P, \quad \text{by definition of } \mathcal{P} \\
& \implies & (s(n), \sigma(y)) \in P \wedge (\mathbf{false} \implies s(y) = z), \quad \text{since } \mathbf{true} \equiv (\mathbf{false}) \implies \phi \\
& \implies & (s(n), \sigma(y)) \in P \wedge (s(n) = 0 \implies s(y) = z), \quad \text{since } \mathbf{false} \equiv (s(n) = 0).
\end{array}$$

So in particular, we have

$$\vDash P \in \mathcal{P} \implies G \subseteq \alpha(P),$$

because $G = \bigcap \mathcal{P}$ and $\alpha(P) \in \mathcal{P}$. In particular we have (for $P = \mathbb{N} \times X \in \mathcal{P}$) that $\vDash G \subseteq \alpha(\mathbb{N} \times X)$ from which we conclude:

$$\begin{array}{lll}
\vDash (0,x) \in G & \implies & (0,x) \in \alpha(\mathbb{N} \times X) \\
& \implies & (0,x) \in (\mathbb{N} \times X) \wedge (0 = 0 \implies x = z), \quad \text{by definition } \alpha \\
& \implies & x = z, \quad \text{since } (0,x) \in \mathbb{N} \times X \text{ and } 0 = 0
\end{array}$$

Which shows (2).
To show (3), first consider the following computation:

$$\begin{array}{lll}
\vDash (n,x) \in G & \implies & \forall P \left(P \in \mathcal{P} \implies (n,x) \in P\right), \quad \text{by definition } G \\
& \implies & \forall P \left(P \in \mathcal{P} \implies (s(n), \sigma(x)) \in P\right), \quad \text{by definition } \mathcal{P} \text{ and since } (n, x \in P \in \mathcal{P}) \\
& \implies & (s(n), \sigma(x)) \in G, \text{ by definition } G \\
& \implies & \exists y : (s(n), y) \in G
\end{array}$$

By $(T55 :: if \vDash \phi \implies \psi), then \vDash \exists x \phi \implies \exists x \psi$ and $(T50 ::\vDash (\exists \phi) \implies \phi) when x not free variable of \phi)$, we the get

$$\vDash \exists x : (n,x) \in G \implies \exists y : (s(n), y) \in G$$

which shows (3).
In order to show (4), we first define:

$$H(n,x) := \{(m,y) | (m,y) \in G \wedge (m = s(n) \implies y = \sigma(x))\}.$$

We now claim

$$\vDash ((n,x) \in G \wedge (n,y) \in G) \implies x = y) \implies H(n,x) \in \mathcal{P}, \tag{5}$$

so we have to show:

- $(0,z) \in H(n,x)$;
- $\forall m \forall x : (m,y) \in H(n,x) \implies (s(m), \sigma(y)) \in H(n,x)$

That the first equation hold follows immediate because $\vDash (0,z) \in G$ holds and $\vDash 0 = s(n)$ is always false, thus $\vDash (0,z) \in G \wedge (0 = s(n) \implies y = \sigma(x))$ is true. To show the second equation (by definition of $H(n,x)$), we have to show

(a) $\forall m \forall x : (m,y) \in H(n,x) \implies (s(m), \sigma(y)) \in G$

(b) $\forall m \forall x : (m,y) \in H(n,x) \implies (s(m) = s(n) \implies \sigma(y) = \sigma(x))$.

That (a) holds is immediate because

$$\vDash (m,y) \in H(n,x) \implies (m,y) \in G \implies (s(m), \sigma(y)) \in G,$$

where the first implication holds by definition of $H(n,x)$ and the second implication holds by definition of G and $\mathcal{P}$.
To show (b), first notice:

$$\begin{aligned} \vDash ((m,y) \in H(n,x) \wedge s(m) = s(n)) &\implies ((m,y) \in H(n,x) \wedge m = n) \quad \text{by } (P3), \\ &\implies (m,y) \in H(n,x) \wedge (n,y) \in H(n,x) \\ &\implies (m,y) \in G \wedge (n,y) \in G, \quad \text{by definition } H(n,x) \end{aligned}$$

Thus

$$\begin{aligned} \vDash \quad & ((n,x) \in G \wedge (n,y) \in G) \implies x = y) \wedge (m,y) \in H(n,x) \wedge s(m) = s(n) \\ \implies \quad & ((n,x) \in G \wedge (n,y) \in G) \implies x = y) \wedge ((n,x) \in G \wedge (n,y) \in G) \\ \implies \quad & x = y \\ \implies \quad & \sigma(x) = \sigma(y) \end{aligned}$$

Since $G = \bigcap \mathcal{P}$, we the conclude

$$\vDash ((n,x) \in G \wedge (n,y) \in G) \implies x = y) \implies H(n,x) \in \mathcal{P} \implies G \subseteq H(n,x) \tag{6}$$

We also have

$$\begin{aligned} \vDash G \subseteq H(n,x) \wedge (s(n),u) \in G \wedge (s(n),v) \in G & \\ \implies (s(n),u) \in H(n,x) \wedge (s(n),v) \in H(n,x) & \\ \implies u = \sigma(x) \wedge v = \sigma(x) & \\ \implies u = v & \end{aligned} \tag{7}$$

So combining the equations (6) and (7), we conclude:

$$\begin{aligned} \vDash \forall x \forall y : ((n,x) \in G \wedge (n,y) \in G) \implies x = y) &\implies \forall x : G \subseteq H(n,x) \quad \text{since } G = \bigcap \mathcal{P} \\ &\implies \forall x : \forall u \forall v : ((s(n),u) \in G \wedge (s(n),v) \in G \implies u = v) \\ &\implies \forall u \forall v : ((s(n),u) \in G \wedge (s(n),v) \in G \implies u = v) \end{aligned}$$

This shows (b), thus we indeed conclude equation (5) which shows the fourth equation which we needed to show equation (3), i.e. we have shown

$$\vDash \forall n \exists! x(n, x) \in G.$$

Thus we get a unique morphism $g : \mathbb{N} \to X$ such that

$$\vDash \forall n : (n, g(n)) \in G.$$

We now show that g satisfies the relations and is the unique morphism which satisfies those.
That $g \circ 0 = z$ holds follows from the second equation which we had to show:

$$\vDash (0, z) \in G \wedge (0, g(0)) \in G \implies z = g(0).$$

We show $\sigma \circ g = g \circ s$ by induction. The base case is shown as follows:

$$\begin{aligned} \vDash (0, z) \in G \wedge (s(0), g \circ s(0)) \in G &\implies (s(0), \sigma(z)) \in G \wedge (s(0), (g \circ s)(0)) \in G \\ &\implies \sigma(z) = (g \circ s)(0) \\ &\implies (\sigma \circ g)(0) = (g \circ s)(0) \end{aligned}$$

The induction step is shown as follows:

$$\begin{aligned} \vDash (\sigma \circ g)(n) = (g \circ s)(n) &\implies (s(n), (\sigma \circ g)(n)) \in G \wedge (\sigma \circ g)(n) = (g \circ s)(n) \\ &\implies (s \circ s(n)), (\sigma \circ \sigma \circ g)(n)) \in G \wedge (\sigma \circ g)(n) = (g \circ s)(n) \\ &\implies (s \circ s(n)), (\sigma \circ g \circ s)(n)) \in G \\ &\implies (\sigma \circ g)(s(n)) = (g \circ s)(s(n)) \end{aligned}$$

The uniqueness of g is shown by induction as follows: Assume $h : \mathbb{N} \to X$ satisfies $h \circ 0 = z$ and $\sigma \circ h = h \circ s$, then:

$$\begin{aligned} &\vDash \quad h(0) = z = g(0) \\ &\vDash \quad h(n) = g(n) \implies h(s(n)) = (\sigma \circ h)(n) = (\sigma \circ g)(n) = (g \circ s)(n) \end{aligned}$$

Which shows the proposition. □

So the previous propositions gives us:

Corollary 4. *The data $(\mathbb{N}, 0, s)$ (in a topos $\mathcal{E}$) is a natural number object if and only if it is a model of Peano arithmetic.*

We have seen in lemma (2) that if $(\mathbb{N}, 0, s)$ is a natural number object, then is $\mathbb{N}$ the product of 0 and s. We will now show that if we have demand the following property (given by the lemma), the converse also holds.

Lemma 5. *Let $(\mathbb{N}, 0, s)$ be a natural number object, then is the unique morphism $\mathbb{N} \to \mathbf{1}$ the coequalizer of $Id_{\mathbb{N}}$ and s.*

Proof. Let $f : \mathbb{N} \to A$ be a morphism such that $f = f \circ s$. We have to show that f factors uniquely through $\mathbb{N} \to \mathbf{1}$.
Since $f = f \circ s$, the following diagram commutes:

$$\begin{array}{ccccc} \mathbf{1} & \xrightarrow{0} & \mathbb{N} & \xrightarrow{s} & \mathbb{N} \\ & \searrow^{f \circ 0} & \downarrow f & & \downarrow f \\ & & A & \xrightarrow{Id} & A \end{array}$$

Write ! for the unique morphism $\mathbb{N} \to \mathbf{1}$. Then (since $\mathbf{1}$ is terminal), we have

$$f \circ 0 = f \circ 0 \circ ! \circ 0, \quad Id_A \circ f \circ 0 \circ ! = f \circ 0 \circ ! \circ s.$$

So by the uniqueness of the factorization of the universal property of the n.n.o we have that $f = f \circ 0 \circ !$. Thus f indeed factorizes through the unique morphism $! : \mathbb{N} \to \mathbf{1}$. This factorization is clearly unique since $\mathbf{1}$ is terminal. □

Corollary 5. *The data $(\mathbb{N}, 0, s)$ (in a topos $\mathcal{E}$) is a natural number object if and only if $\mathbb{N}$ is the coproduct of s with 0 and the unique morphism $\mathbb{N} \to \mathbf{1}$ is the coequalizer of s with $Id_{\mathbb{N}}$.*

Proof. By the previous lemma it remains to show that the coproduct and coequalizer condition is sufficient. In remark (1) we have already noticed that the coproduct condition implies the validness of $(P1), (P2)$ and $(P3)$, so it remains to show

$$(P4) \vDash (0 \in P \wedge (n \in P \implies s(n) \in P)) \implies P = \mathbb{N},$$

where P is a variable of type $\mathbb{N}$. By the localization principle, we have to show that for any subobject $i : P \to \mathbb{N}$, if $0 : \mathbf{1} \to \mathbb{N}$ factorizes through i and $s : \mathbb{N} \to \mathbb{N}$ restricts to P, then is $P = \mathbb{N}$.
Instead of working with P, we restrict to its subobject $Im(0) \cup Im(s|_P)$ (which we still denote by P). This means that $(0, s)$ restricted to P is jointly epimorphic which allows us to conclude:

$$\begin{aligned}
\vDash s(n) \in P \quad &\implies \quad (s(n) = 0 \vee \exists m : (s(m) = s(n) \wedge m \in P)), \quad \text{by jointly epic,} \\
&\implies \quad \mathbf{false} \vee \exists m : (s(m) = s(n) \wedge m \in P), \quad \text{since } \vDash \neg(s(n) = 0), \\
&\implies \quad \exists m : (s(m) = s(n) \wedge m \in P) \\
&\implies \quad \exists m : (m = n \wedge m \in P), \quad \text{since } s \text{ mono.} \\
&\implies \quad n \in P
\end{aligned}$$

Since we already know $\vDash n \in P \implies s(n) \in P$, we have that P is closed under the equivalence relation given by the union of $(Id, s) : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ with $(s, Id) : \mathbb{N} \to \mathbb{N}$. We denote this relation by $(a, b) : S \to \mathbb{N} \times \mathbb{N}$. So that P is closed under S implies

$$\vDash \forall n \forall m : (n, m) \in S \implies (n \in P \iff m \in P).$$

Now consider the equivalence relation

$$T := \left\{ (n, m) | \forall \tilde{S} (\forall l : l \in \tilde{S} \iff s(l) \in \tilde{S}) \implies (n \in \tilde{S} \iff m \in \tilde{S}) \right\}.$$

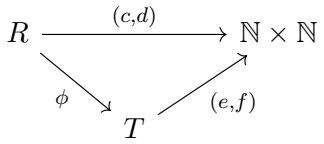
This is a subobject of $\mathbb{N} \times \mathbb{N}$ (write it as $(e, f) : T \to \mathbb{N} \times \mathbb{N}$) and it clearly contains S.
Since P is closed under S, it also closed under T because if $n \in P$ and $(n, m) \in T$, we have by definition of T that $m \in P$ (since P is closed under S).
Let $(c, d) : R \to \mathbb{N} \times \mathbb{N}$ be the kernel pair of $coeq(a, b)$ and denote by $g : \mathbb{N} \to coeq(a, b)$ the *coequalizer* of a with b. We will now show that because P is closed under T, it is also closed under R:
Since every equivalence relation is effective in a topos, there exists some morphism $h : \mathbb{N} \to Y$ such that its kernel pair is (e, f), i.e. the following diagram is a pullback square:

$$\begin{array}{ccc}
T & \xrightarrow{e} & \mathbb{N} \\
\downarrow{\scriptstyle f} & & \downarrow{\scriptstyle h} \\
\mathbb{N} & \xrightarrow{h} & Y
\end{array}$$

Thus $he = hf$ and since S is contained in T, we can restrict it to $(a, b) : S \to \mathbb{N} \times \mathbb{N}$ which gives us $h \circ a = h \circ b$. Thus h factorizes through $g : \mathbb{N} \to coeq(a, b)$ by some morphism $k : coeq(a, b) \to Y$, i.e. $h = k \circ g$.
Thus We have $g \circ d = g \circ d$ and thus

$$h \circ d = k \circ g \circ d = k \circ g \circ c = h \circ c.$$

Since T is the pullback of h along itself, we have that there exists a unique morphism $\phi : R \to T$ such that $d = f \circ \phi$ and $c = e \circ \phi$, thus we have a (unique) factorization



So we are now ready to conclude that P is closed under R, indeed: $\vDash (n,m) \in R$ means that $(n,m) : \mathbf{1} \to \mathbb{N}$ factors through $R \to \mathbb{N}\times\mathbb{N}$. But $R \to \mathbb{N}\times\mathbb{N}$ factors through $T \to \mathbb{N}\times\mathbb{N}$. So $\vDash (n,m) \in R \implies (n,m) \in T$, thus we get:

$$\begin{aligned} \vDash n \in P \wedge (n,m) \in R &\implies n \in P \wedge (n,m) \in T \\ &\implies m \in P, \quad \text{since } P \text{ closed under } T. \end{aligned}$$

So P is indeed closed under R. But R is the kernel pair of $coeq(a,b)$, we now claim that this is the terminal object (because $coeq(Id,s)$ is terminal), indeed: S contains the graph $\{(n,s(n)\}$ of s. Write $\tau : \{(n,s(n))\} \to S$ for the inclusion, thus $Id = a \circ \tau$ and $s = b \circ \tau$. Thus

$$g \circ Id = g \circ (a \circ \tau) = g \circ (b \circ \tau) = g \circ s.$$

So g factorizes through $coeq(Id,s)$ which is the terminal object (by hypothesis). But g is epi, thus $\mathbf{1} = coeq(Id,s) \to coeq(a,b)$ must be epi, but any morphism starting from the terminal object is mono, thus it is an isomorphism, hence $coeq(a,b)$ is indeed terminal.
But the kernel pair of the morphism $\mathbb{N} \to \mathbf{1}$ is $Id_{\mathbb{N}\times\mathbb{N}}$, so we have that P is closed under everything (i.e. the equivalence relation $Id : \mathbb{N}\times\mathbb{N} \to \mathbb{N}\times\mathbb{N}$). That $P = \mathbb{N}$ is valid now follows because $\vDash 0 \in P$, indeed:

$$\vDash \forall n : 0 \in P \wedge (0,n) \in \mathbb{N}\times\mathbb{N} \implies n \in P,$$

where the last implication holds because P closed under $R = \mathbb{N}\times\mathbb{N}$. □

1.3 Infinite objects in a topos

Up until this moment we have defined/characterized when some data $(\mathbb{N}, 0, s)$ forms a natural number object. In this section we will give a criteria for when a topos has a natural number object. It will turn out that a topos needs an object which is *infinite*.
Recall that a set is infinite if and only if there is a bijection with a proper subset:

Definition 4. *Let $\mathcal{E}$ be a topos with terminal object $\mathbf{1}$.*

- *A subobject $s : S \hookrightarrow A$ is **proper** if there exists a global element $a : \mathbf{1} \to A$ such that $\vDash \neg(a \in S)$.*
- *An object $A \in \mathcal{E}$ is **infinite** when there exists an isomorphism between A and a proper subobject of A.*

Example 2. *The natural number object $(\mathbb{N}, 0, s)$ is infinite.*

Proof. Since s is a monomorphism, we have $\mathbb{N} \to Im(s)$ is an isomorphism and by $(P2)$, we have $\vDash \neg(0 \in Im(s))$. So we have that $Im(s)$ is a proper subobject, thus $\mathbb{N}$ is indeed infinite. □

Although this is a *natural* definition of an infinite object, it has some unexpected behaviour in the sense that an object which contains an infinite subobject must not be infinite itself:

Example 3. *Let $\mathcal{E}$ be the presheaf topos on (the poset) $(\mathbb{N}, \leq)$. Let A be the presheaf defined by*

$$\begin{aligned} A(0) &= \mathbb{N} \\ A(n+1) &= \mathbb{N} \amalg \{\tilde{n}\}, \quad n \in \mathbb{N} \\ \tilde{n}|_m &= n, \quad m \leq n \end{aligned}$$

This object is not infinite but it contains the n.n.o.

Proof. We first claim that the n.n.o in $\mathcal{E}$ is the constant presheaf on the set $\mathbb{N}$, indeed: We know that in a Grothendieck topos, the (the underlying object of the) n.n.o. is given by

$$\bigsqcup_{\mathbb{N}} \mathbf{1}_{\mathcal{E}},$$

where $\mathbf{1}_{\mathcal{E}}$ is the terminal object of $\mathcal{E}$, i.e. terminal (pre)sheaf given by mapping everything to a singleton. The coproduct of presheaves is given by objectwise taking the coproduct which concludes the claim.
Assume $\sigma : A \to S$ is an isomorphism on a proper subobject $s : S \to A$. So we have that

$$A \xrightarrow{\sigma} S \xrightarrow{s} A,$$

is a non-epimorphic monomorphism, indeed: s is an epi if and only if $\vDash \forall b : \exists a : f(a) = b$, but $Im(f) = \{b | \exists a : f(a) = b\}$ and f is mono (thus $Im(f) = S$), thus we have

$$s \text{ epi} \iff \forall b : b \in S,$$

which is not possible since s is proper.
We now show that every monomorphism $\alpha : A \to A$ is an isomorphism which shows that there can't exists such a proper subobject s of A:
A morphism $\alpha : A \to A$ induces a function $\alpha_0 : \mathbb{N} = A(0) \to \mathbb{N} = A(0)$. By the naturality of α (and the definition of the restriction ρ) we have

$$\rho_0(\alpha_{n+1}(n)) = \alpha_0(\rho_0(n)) = \alpha_0(n) = \alpha_0(\rho_0(\tilde{n})) = \rho_0(\alpha_{n+1}(\tilde{n})).$$

From this, we conclude by definition of ρ_0 that

$$\alpha_{n+1}(\{n, \tilde{n}\}) \subseteq \{n, \tilde{n}\}.$$

Since α is a mono, α_{n+1} is an injection, thus this is an equality.
In particular have

$$\alpha_0(n) = \alpha_0(\rho_0(n)) = \rho_0(\alpha_{n+1}(n)) \in \rho_0(\{n, \tilde{n}\}) = \{n\},$$

where the last equality even holds for $n = 0$ because $A(0) = \mathbb{N}$. Thus $\alpha_0 = Id_{\mathbb{N}}$.
We now claim that $\alpha_{n+1}(m) = m$ for $m \neq n$ from which we can conclude that α_{n+1} is a bijection, and as this holds for all $n \geq 0$ (and since α_0 is a bijection), we conclude that α is an isomorphism which concludes the proof. So let $m \neq n$. Then we have indeed

$$m = \rho_0(m) = \alpha_0(\rho_0(m)) = \rho_0(\alpha_{n+1}(m)) = \alpha_{n+1}(m),$$

where the last equality holds because we know that firstly, the restriction $\rho_0 : \mathbb{N} \cup \{\tilde{n}\} \to \mathbb{N}$ is the identity if we restrict to $\mathbb{N} \setminus \{n\}$ and secondly, since $m \neq n$, we have $\alpha_{n+1}(m) \notin \{n, \tilde{n}\}$ (here we use injectivity of α_{n+1} and knowing that $\alpha_{n+1}(n, \tilde{n}) = \{n, \tilde{n}\}$). □

The previous example shows that an object can have an infinite subobject but not be infinite itself, in the case of boolean topoi this will not be the case:

Proposition 5. *Let $A \in \mathcal{E}$. If A contains a complemented infinite subobject, then is A infinite.*

Proof. Let $B \subseteq A$ be the complemented infinite subobject of A (with complement $A \setminus B$). Since B infinite, there exists a global element $b : 1 \to B$, a proper subobject $s : S \to B$ and an isomorphism $\sigma : B \to S$ such that $\vDash \neg(b \in S)$. Since $\vDash b \in B$, we have $\vDash \neg(b \in A \setminus B)$. So we have $\vDash \neg (b \in S \bigcup (A \setminus B))$. Thus $S \bigcup (A \setminus B)$ is a proper subobject of A. Since $s : B \to S$ is an isomorphism, we conclude that

$$A = B \bigcup (A \setminus B) \to S \bigcup (A \setminus B),$$

is an isomorphism from A to a proper subobject which shows the claim. □

Proposition 6. *If $A \in \mathcal{A}$ is an infinite object, then it contains subobject which is a natural number object.*

Proof. That A is infinite means that there is a subobject $s : S \to A$, a global element $a : \mathbf{1} \to A$ and isomorphism $\sigma : A \to S$ such that $\vDash \neg(a \in S)$. Let

$$\mathcal{P} := \{P | a \in P \wedge \forall b(b \in P \implies \sigma(b) \in P)\}.$$

and let $\mathbb{N}$ be its intersection, i.e.

$$\mathbb{N} := \bigcap \mathcal{P} = \{b | \forall P(P \in \mathcal{P} \implies b \in P)\}.$$

We clearly have that $\mathbb{N}$ is a subobject of A.
Also notice that $a \in \mathbb{N}$ (because $a \in P$ for every $P \in \mathcal{P}$). Thus $a : \mathbf{1} \to A$ factors through the inclusion $i : \mathbb{N} \to A$ (by definition of $\in$). This factorization we write as $0 : \mathbf{1} \to \mathbb{N}$.
That $\sigma : A \to A$ can be restricted to $\mathbb{N}$ as some morphism $s : \mathbb{N} \to \mathbb{N}$ follows from:

$$\vDash b \in \mathbb{N} \implies \forall P(P \in \mathcal{P} \implies b \in \mathcal{P}) \implies \forall P(P \in \mathcal{P} \implies \sigma(P)) \implies \sigma(b) \in \mathbb{N},$$

where the second implication hold by definition of $\mathcal{P}$.
So we now claim that $(\mathbb{N}, 0, s)$ is a model of Peano arithmetic (thus consequently a natural number object). To show $(P1) \vDash n = 0 \vee \exists m : n = s(m)$, define

$$Q := \{b | (b = a) \vee \exists c(c \in \mathbb{N} \wedge b = \sigma(c))\}.$$

To show that $(P1)$ holds, we thus have to show that $\vDash Q = \mathbb{N}$. We first show $\vDash Q \subseteq \mathbb{N}$. By $(T35) \vDash ((\phi \implies \delta) \wedge (\psi \implies \delta)) \implies (\phi \vee \psi \implies \delta)$ it suffices to notice the following:

$$\begin{array}{lrll} \vDash & (b = a) & \implies (b \in \mathbb{N}), & \text{since } a \in \mathbb{N} \\ \vDash & \exists c\,(c \in \mathbb{N} \wedge b = \sigma(c)) & \implies \exists c\,(\sigma(c) \in \mathbb{N} \wedge b = \sigma(c)), & \text{by definition } \mathcal{P} \\ & & \implies \exists c(b \in \mathbb{N}) \implies b \in \mathbb{N} & \end{array}$$

To show $\vDash \mathbb{N} \subseteq Q$, it suffices to show $\vDash Q \in \mathcal{P}$ (since $\mathbb{N} = \bigcap \mathcal{P}$). Thus we have to show

$$\vDash a \in Q \wedge (\forall b : b \in Q \implies \sigma(b) \in Q).$$

We clearly have $\vDash a \in Q$. From

$$\begin{array}{rll} \vDash b = a & \implies & a \in \mathbb{N} \wedge \sigma(b) = \sigma(a) \\ & \implies & \exists c(c \in \mathbb{N} \wedge \sigma(b) = \sigma(c)) \\ & \implies & \sigma(b) \in Q \\ \vDash c \in \mathbb{N} \wedge b = \sigma(c) & \implies & \sigma(c) \in \mathbb{N} \wedge \sigma(b) = (\sigma \circ \sigma)(c) \\ & \implies & \exists d(d \in \mathbb{N} \wedge \sigma(b) = \sigma(d)) \\ & \implies & \sigma(b) \in Q \end{array}$$

By $(T55)(\vDash \phi \implies \psi) \implies (\vDash \exists x\phi \implies \exists x\psi)$, we have

$$\vDash \exists c(c \in \mathbb{N} \wedge b = \sigma(c)) \implies \exists c(\sigma(b) \in Q).$$

And since c is not a free variable in $\sigma(b) \in Q$, we conclude by $(T50) x \notin FV(\phi) \implies \vDash ((\exists x\phi) \implies \phi)$,

$$\vDash \exists c(c \in \mathbb{N} \wedge b = \sigma(c)) \implies (\sigma(b) \in Q).$$

Combining this together with $\vDash b = a \implies \sigma(b) \in Q$, we conclude from

$$(T35) \vDash (((\phi \implies \theta) \wedge (\psi \implies \theta)) \implies ((\phi \vee \psi) \implies \theta)),$$

that

$$\vDash (b \in Q \implies \sigma(b) \in Q).$$

By $(T53)(\vDash \phi) \implies (\vDash \forall x \phi)$, we have

$$\forall b(b \in Q \implies \sigma(b) \in Q).$$

From this and $\vDash a \in Q$, we conclude

$$\vDash (a \in Q) \wedge \forall b(b \in Q \implies \sigma(b) \in Q),$$

which means precisely $\vDash Q \in \mathcal{P}$ which is exactly what we need to conclude $\vDash \mathbb{N} = Q$ and thus $(P1)$.
That $(P2) \vDash \neg(s(n) = 0)$ holds, follows by the following computation:

$$\begin{aligned}
\vDash s(n) = 0 \quad &\implies \quad \sigma(n) = 0, \quad \text{since } s = \sigma|_{\mathbb{N}} \\
&\implies \quad \sigma(n) = 0 \wedge \sigma(n) \in S, \quad \text{since } \sigma : A \to S \\
&\implies \quad 0 \in S \\
&\implies \quad \textbf{false}, \quad \text{since } a = i \circ 0 \text{ and } \vDash \neg(a \in S)
\end{aligned}$$

Since s is the restriction of the monomorphism σ, s is a monomorphism, thus $(P3)$ holds.
That $(P4)$ holds follows by the following computation:

$$\begin{aligned}
\vDash 0 \in P \wedge \forall n\,(n \in P \implies s(n) \in P) \quad &\implies \quad a \in P \wedge \forall n\,(n \in P \implies \sigma(n) \in P) \\
&\implies \quad P \in \mathcal{P} \quad \text{by definition } \mathcal{P} \\
&\implies \quad \mathbb{N} \subseteq P, \quad \text{since } \mathbb{N} = \bigcap \mathcal{P} \\
&\implies \quad \mathbb{N} = P, \quad \text{since } P \text{ of type } \Omega^{\mathbb{N}}
\end{aligned}$$

□

Corollary 6. *A topos has an infinite object if and only if it has a natural number object.*

2 Arithmetic in a topos

In this section, we fix a natural number object $(\mathbb{N}, 0, s)$ in a topos $\mathcal{E}$.

Proposition 7. *There exists an* ***addition*** *morphism*

$$+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N},$$

such that for variables $m, n : \mathbb{N}$, we have

$$\vDash n + 0 = n, \quad \vDash n + s(m) = s(n + m).$$

Proof. Consider the following diagrams:

$$\begin{array}{ccc}
\mathbf{1} & \xrightarrow{0} & \mathbb{N} \\
& \searrow^{i} & \downarrow \oplus \\
& & \mathbb{N}^{\mathbb{N}}
\end{array}, \qquad
\begin{array}{ccc}
\mathbb{N} & \xrightarrow{s} & \mathbb{N} \\
\downarrow \oplus & & \downarrow \oplus \\
\mathbb{N}^{\mathbb{N}} & \xrightarrow{s^{\mathbb{N}}} & \mathbb{N}^{\mathbb{N}}
\end{array}$$

where i corresponds by cartesian closedness by $Id_{\mathbb{N}}$ and $s^{\mathbb{N}}$ correspond with $Id_{\mathbb{N}} \times s$ under the isomorphisms

$$\mathcal{E}(\mathbb{N}^{\mathbb{N}}, \mathbb{N}^{\mathbb{N}}) \cong \mathcal{E}(\mathbb{N}^{\mathbb{N}} \times \mathbb{N}, \mathbb{N}) \cong \mathcal{E}(\mathbb{N} \times \mathbb{N}, \mathbb{N} \times \mathbb{N}),$$

and $\oplus$ is the unique morphism induced by the universal property of the *n.n.o.* $\mathbb{N}$ which, by cartesian closedness, corresponds with a (unique) morphism $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. We now claim

$$Id_{\mathbb{N}} = + \circ (Id_{\mathbb{N}} \times 0), \quad s \circ + = + \circ (Id_{\mathbb{N}} \times s).$$

By naturality of the adjunction we have that the following diagram commute:

$$\begin{array}{ccc} \mathcal{E}(\mathbb{N},\mathbb{N}^{\mathbb{N}}) & \xrightarrow{\phi} & \mathcal{E}(\mathbb{N}\times\mathbb{N},\mathbb{N}) \\ \downarrow{\scriptstyle \circ -0} & & \downarrow{\scriptstyle \circ -(Id_{\mathbb{N}}\times 0)} \\ \mathcal{E}(\mathbf{1},\mathbb{N}^{\mathbb{N}}) & \xrightarrow{\phi} & \mathcal{E}(\mathbb{N}\times\mathbf{1},\mathbb{N}) \end{array}$$

So applying this to $\oplus$, we conclude:

$$Id_{\mathbb{N}} = \phi(i) = \phi(\oplus \circ 0) = \phi(\oplus) \circ (Id_{\mathbb{N}} \times 0) = + \circ (Id_{\mathbb{N}} \times 0),$$

which shows the first equality. For the second equality, consider the following commutative diagrams:

$$\begin{array}{ccc} \mathcal{E}(\mathbb{N},\mathbb{N}^{\mathbb{N}}) & \xrightarrow{\phi} & \mathcal{E}(\mathbb{N}\times\mathbb{N},\mathbb{N}) \\ \downarrow{\scriptstyle -\circ s} & & \downarrow{\scriptstyle \circ -(Id_{\mathbb{N}}\times s)} \\ \mathcal{E}(\mathbb{N},\mathbb{N}^{\mathbb{N}}) & \xrightarrow{\phi} & \mathcal{E}(\mathbb{N}\times\mathbb{N},\mathbb{N}) \end{array} \qquad \begin{array}{ccc} \mathcal{E}(\mathbb{N},\mathbb{N}^{\mathbb{N}}) & \xrightarrow{\phi} & \mathcal{E}(\mathbb{N}\times\mathbb{N},\mathbb{N}) \\ \downarrow{\scriptstyle -\circ s} & & \downarrow{\scriptstyle s\circ -} \\ \mathcal{E}(\mathbb{N},\mathbb{N}^{\mathbb{N}}) & \xrightarrow{\phi} & \mathcal{E}(\mathbb{N}\times\mathbb{N},\mathbb{N}) \end{array}$$

From the left diagram we conclude:

$$+ \circ (Id_{\mathbb{N}} \times s) = \phi(\oplus) \circ (Id_{\mathbb{N}} \times s) = \phi(\oplus \circ s).$$

And from the second diagram we conclude:

$$\phi(\oplus \circ s) = s \circ \phi(\oplus) = s \circ +.$$

Which combined shows $+ \circ (Id_{\mathbb{N}} \times s) = s \circ +$.
That the equalities hold (in the internal logic) means precisely that those diagrams commute which shows the proposition. □

Let us write $1 := s(0)$, we then have in particular:

$$s(n) = s(n + 0) = n + s(0) = n + 1.$$

We will use this notation to use induction.

Proposition 8. *Let $l, m, n : \mathbb{N}$ be variables. Then*

1. $\vDash l + (m + n) = (l + m) + n$.
2. $\vDash m + n = n + m$.
3. $\vDash (m + l = n + l) \implies (m = n)$.
4. $\vDash (m + n = 0) \implies (m = 0 \wedge n = 0)$.

Proof. All four statements are proven by the principle of induction.
We show the first equation (i.e. associativity) by induction on n. That the base case $n = 0$ holds follows because $\vDash m + 0 = m$, indeed:

$$\vDash l + (m + 0) = l + m = (l + m) + 0.$$

We now show the induction step. First notice:

$$\vDash i + (j + 1) = i + s(j) = s(i + j) = (i + j) + 1.$$

This implies

$$\begin{array}{lrcll} \vDash l + (m + n) = (l + m) + n \implies l + (m + (n + 1)) & = & l + ((m + n) + 1), & \text{by } i = m, j = n \\ & = & (l + (m + n)) + 1, & \text{by } i = l, j = m + n \\ & = & ((l + m) + n) + 1, & \text{by induction hypothesis} \\ & = & (l + m) + (n + 1), & \text{by i=l+m, j=n} \end{array}$$

To show the second equation (i.e. commutativity), we also do induction on n. So we first have to show the base case $\vDash m + 0 = 0 + m$. We show this by induction on m. The base case $\vDash 0 + 0 = 0 + 0$ is clear. So $\vDash m + 0 = 0 + m$ now follows because:

$$\vDash m + 0 = 0 + m \implies (m + 1) + 0 = m + 1 = (m + 0) + 1 = (0 + m) + 1 = 0 + (m + 1),$$

where the 3^{th} equality holds by the base case $\vDash m + 0 = 0 + m$ and the 4^{th} equation holds by associativity. Before showing the induction step of commutativity, we first show $\vDash i + 1 = 1 + i$ by induction on i as follows:

$$\begin{aligned} &\vDash 0 + 1 = 0 + s(0) = s(0 + 0) = s(0) = s(0) + 0 = 1 + 0 \\ &\vDash i + 1 = 1 + i \implies (i + 1) + 1 = (1 + i) + 1 = 1 + (i + 1) \end{aligned}$$

where the last equality holds because of associativity. So we are now ready to show commutativity by the induction step:

$$\begin{aligned} \vDash m + n = n + m \implies m + (n + 1) &= (m + n) + 1, && \text{by associativity} \\ &= (n + m) + 1, && \text{by induction hypothesis } m + n = n + m \\ &= n + (m + 1), && \text{by associativity} \\ &= n + (1 + m), && \text{by } i = m \\ &= (n + 1) + m, && \text{by associativity} \end{aligned}$$

We show the 3^{th} equation $\vDash m + l = n + l \implies m = n$ by induction on l. The base holds by:

$$\vDash (m + 0 = n + 0) \implies m = m + 0 = n + 0 = n.$$

The induction step is as follows:

$$\begin{aligned} &\vDash \quad (m + l = n + l \implies m = n) \\ \implies &\quad m + (l + 1) = n + (l + 1) \quad \implies s(m + l) = s(n + l), \quad \text{by associativity} \\ &\qquad\qquad\qquad\quad \implies m + l = n + l, \quad \text{by } (P3) \\ &\qquad\qquad\qquad\quad \implies m = n, \quad \text{by induction} \end{aligned}$$

We now show the 4^{th} equation $\vDash (m + n = 0) \implies (m = 0 \wedge n = 0)$. We show this by giving a direct proof (instead of induction). We show

$$\vDash m + n = 0 \implies n = 0,$$

as follows:

$$\begin{aligned} \vDash m + n = 0 &\implies [(m + n = 0) \wedge (n = 0 \vee \exists l : (n = s(l)))], \quad \text{by } (P1) \\ &\implies (n = 0) \vee (m + n = 0 \wedge \exists l\, (m + n = m + s(l) = s(m + l))), \\ &\implies (n = 0) \vee \mathbf{false}, \quad \text{by } (P2) :\vDash \neg(s(n) = 0) \\ &\implies n = 0 \end{aligned}$$

From this we can conclude $\vDash (m + n = 0) \implies (m = 0 \wedge n = 0)$ in multiple ways. We could just add into this calculation $\exists k : (m = s(k))$ and do the exact same calculation, but we can also conclude the result by commutativity because we then have $\vDash (m + n = 0) \implies (m = 0)$ and then by the rule $\vDash ((\phi \implies \psi) \wedge (\phi \implies \theta)) \implies (\phi \implies (\psi \wedge \theta))$ (proposition 6.7.5 (T31)), together with the Modus Ponens rule (proposition 6.7.1 (T11))

$$\text{if } \vDash \phi \text{ and } \vDash (\phi \implies \psi), \text{ then } \vDash \psi,$$

we conclude the result. □

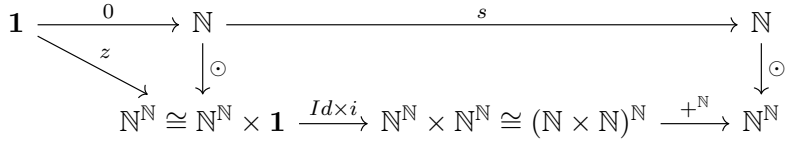
Proposition 9. *There exists a* ***multiplication*** *morphism*

$$\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N},$$

such that for variables $m, n : \mathbb{N}$*, we have*

$$\vDash n \cdot 0 = 0, \quad \vDash n \cdot (m+1) = (n \cdot m) + n.$$

Proof. Consider the following diagram:



where i, z and $+^{\mathbb{N}}$ correspond by cartesian closedness with $Id_{\mathbb{N}}$, $\mathbb{N} \to \mathbf{1} \xrightarrow{0} \mathbb{N}$ and $Id_{\mathbb{N}} \times +$. Moreover, $\odot$ is the unique morphism given by the universal property of the n.n.o. $(\mathbb{N}, 0, s)$. By cartesian closedness, $\odot$ correspond with some $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ and that it satisfies the necessairy conditions is the same proof as for the addition morphism. □

Proposition 10. *Let* $l, m, n : \mathbb{N}$ *be variables. Then*

1. $\vDash m \cdot 1 = m$.
2. $\vDash l \cdot (m+n) = (l \cdot m) + (l \cdot n)$.
3. $\vDash l \cdot (m \cdot n) = (l \cdot m) \cdot n$.
4. $\vDash m \cdot n = n \cdot m$.
5. $\vDash (m \cdot l = 0) \implies (m = 0 \vee l = 0)$.
6. $\vDash (m \cdot l = n \cdot l) \implies (m = n \vee l = 0)$.

Proof. That $\vDash m \cdot 1 = m$ holds follows from:

$$\vDash m \cdot 1 = m \cdot (0+1) = (m \cdot 0) + m = 0 + m = m.$$

We show the distributivity by induction on n. The base case is proven as follows:

$$\vDash l \cdot (m+0) = l \cdot (m) = (l \cdot m) + (l \cdot 0).$$

The induction step now follows:

$$\begin{aligned}
\vDash l \cdot (m+n) = (l \cdot m) + (l \cdot n) \implies l \cdot (m + (n+1)) &= l \cdot ((m+n)+1), && \text{by associativity addition} \\
&= l \cdot (m+n) + l \\
&= ((l \cdot m) + (l \cdot n)) + l, && \text{by induction hypothesis} \\
&= (l \cdot m) + ((l \cdot n) + l), && \text{by associativity addition} \\
&= (l \cdot m) + l \cdot (n+1).
\end{aligned}$$

We now show associativity (also by induction on n). The base case is shown as:

$$\vDash l \cdot (m \cdot 0) = l \cdot 0 = 0 = (l \cdot m) \cdot 0.$$

The induction step is now shown as:

$$\begin{aligned}
\vDash l \cdot (m \cdot n) = (l \cdot m) \cdot n \implies l \cdot (m \cdot (n+1)) &= l \cdot (m \cdot n + m) \\
&= (l \cdot (m \cdot n)) + (l \cdot m), && \text{by distributivity} \\
&= (l \cdot m) \cdot n + (l \cdot m), && \text{by induction hypothesis} \\
&= (l \cdot m)(n+1)
\end{aligned}$$

We now show commutativity $\vDash m \cdot n = n \cdot m$ by induction on m. Before showing the base case, we first show $\vDash 0 \cdot i = 0$ by induction on i:

$$\vDash 0 \cdot 0 = 0, \quad \vDash 0 \cdot i = 0 \implies 0 \cdot (i+1) = (0 \cdot i) + 0 = 0 + 0 = 0.$$

The base case for the commutativity follows now immediate $\vDash 0 \cdot n = 0 = n \cdot 0$ (where the first equality is just proven and the second equality holds by definition of the multiplication). Before proving the induction step, we first show $\vDash 1 \cdot i = i$ by induction on i:

$$\vDash 1 \cdot 0 = 0, \quad 1 \cdot i = i \implies 1 \cdot (i+1) = (1 \cdot i) + 1 = i + 1.$$

The induction step now goes as follows:

$$\begin{aligned} \vDash n \cdot m = m \cdot n \implies n \cdot (m+1) &= (n \cdot m) + n \\ &= (m \cdot n) + n, \quad \text{by induction hypothesis} \\ &= (m \cdot n) + (1 \cdot n), \quad \text{by } i = n \\ &= (m+1) \cdot n, \quad \text{by distributivity} \end{aligned}$$

We now show $\vDash (m \cdot l = 0) \implies (m = 0 \vee l = 0)$ by induction on l. The base case

$$\vDash (m \cdot 0 = 0) \implies (m = 0) \vee (0 = 0),$$

clearly holds since $\vDash 0 = 0$. The induction step goes as follows:

$$\begin{aligned} \vDash ((m \cdot l = 0) \implies (m = 0) \vee (l = 0)) \implies [m \cdot (l+1) = 0 &\implies (m \cdot l) + m = 0 \\ &\implies (m \cdot l = 0) \wedge (m = 0) \\ &\implies (m = 0) \\ &\implies (m = 0) \vee (l + 1 = 0)] \end{aligned}$$

We now show $\vDash (m \cdot l = n \cdot l) \implies (m = n) \vee (l = 0)$ by induction on n. The base case is precisely equation (5). The induction step

$$\vDash [(m \cdot l = n \cdot l) \implies (m = n) \vee (l = 0)] \implies [(m \cdot l = (n+1) \cdot l) \implies (l = 0) \vee (m = n+1)],$$

will be shown via the principle of localization, i.e. from

$$\vDash (m \cdot l = n \cdot l) \implies (m = n) \vee (l = 0),$$

we will conclude

$$\vDash (m \cdot l = (n+1) \cdot l) \implies (l = 0) \vee (m = n+1).$$

Indeed:

$$\begin{aligned} \vDash m \cdot l &= (n+1) \cdot l \\ &\implies (m \cdot l = (n \cdot l) + l) \wedge (m = 0 \vee \exists k (m = k+1)) \\ &\implies (0 \cdot l = (n \cdot l) + l) \vee \exists k \left((k+1) \cdot l = (n \cdot l) + l \wedge m = k+1\right), \quad \text{by } (T26) \\ &\implies (0 = (n \cdot l) + l) \vee \exists k \left((k+1) \cdot l = (n \cdot l) + l \wedge m = k+1\right) \\ &\implies ((n \cdot l) = 0 \wedge l = 0) \vee \exists k \left((k \cdot l) + l = (n \cdot l) + l \wedge m = k+1\right) \\ &\implies (l = 0) \vee \exists k \left(k \cdot l = n \cdot l \wedge m = k+1\right) \\ &\implies (l = 0) \vee \exists k \left((k = n \vee l = 0) \wedge m = k+1\right), \quad \text{by hypothesis} \\ &\implies (l = 0) \vee \exists k \left(m = n+1 \vee l = 0\right) \\ &\implies (l = 0) \vee (m = n+1) \end{aligned}$$

So we can now indeed conclude the proposition because we have shown that this holds for all topoi, thus in particular in the slice categories from which we conclude the proposition by the principle of localization. $\square$

Proposition 11. *There exists a* ***exponential*** *morphism*

$$exp : \mathbb{N} \times \mathbb{N} \to \mathbb{N},$$

such that for variables $m, n : \mathbb{N}$*, we have*

$$\vDash n^0 = 1, \quad \vDash n^{(m+1)} = (n^m) \cdot n.$$

Proof. Consider the following diagram:

$$\begin{array}{ccccccc} \mathbf{1} & \xrightarrow{0} & \mathbb{N} & & \xrightarrow{\quad\quad s \quad\quad} & & \mathbb{N} \\ & \searrow^{zs} & \downarrow{\scriptstyle \underline{exp}} & & & & \downarrow{\scriptstyle \underline{exp}} \\ & & \mathbb{N}^{\mathbb{N}} \cong \mathbb{N}^{\mathbb{N}} \times \mathbf{1} & \xrightarrow{Id \times i} & \mathbb{N}^{\mathbb{N}} \times \mathbb{N}^{\mathbb{N}} \cong (\mathbb{N} \times \mathbb{N})^{\mathbb{N}} & \xrightarrow{\cdot^{\mathbb{N}}} & \mathbb{N}^{\mathbb{N}} \end{array}$$

where i, zs and $\cdot^{\mathbb{N}}$ correspond by cartesian closedness with $Id_{\mathbb{N}}$, $\mathbb{N} \to \mathbf{1} \xrightarrow{0} \mathbb{N} \xrightarrow{s} \mathbb{N}$ and $Id_{\mathbb{N}} \times \cdot$. Moreover, $\underline{exp}$ is the unique morphism given by the universal property of the n.n.o. $(\mathbb{N}, 0, s)$. By cartesian closedness, $\underline{exp}$ correspond with some $exp : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ and that it satisfies the necessary conditions is the same proof as for the addition morphism. □

Just as with the addition and multiplication, it satisfies the basic properties which one expects. We do not use further on these properties, but to give an illustration, we can for example show $\vDash l^m \cdot l^n = l^{m+n}$ by induction on n as follows:

$$\begin{aligned} l^m \cdot l^0 = l^m \cdot 1 = l^m = l^{m+0}, \\ l^m \cdot l^{n+1} = l^m \cdot (l^n \cdot l^1) = (l^m \cdot l^n) \cdot l^1 = l^{m+n} \cdot l^1 = l^{m+n} \cdot l = l^{m+n+1}. \end{aligned}$$

3 The trichotomy

We again let $(\mathbb{N}, 0, s)$ be a natural number object in a topos $\mathcal{E}$.

Proposition 12. *The subobject*

$$\{(n, m) | \exists l : n + l = m\} \subseteq \mathbb{N} \times \mathbb{N},$$

defines a partial order on $\mathbb{N}$*, i.e. if we write* $\vDash n \leq m$ *to indicate* $\vDash \exists l : n + l = m$*, then we have*

- *Reflexivity:* $\vDash n \leq n$.
- *Transitivity:* $\vDash (n \leq m \wedge m \leq l) \implies (n \leq l)$.
- *Anti-symmetry:* $\vDash (n \leq m \wedge m \leq n) \implies (m = n)$.

Proof. By

$$(T52) \vDash \phi(t) \implies (\exists \phi), \quad \text{where } t \text{ term not containing any bound variables,}$$

we have $\vDash n + 0 = n \implies \exists l : n + l = n$. And since $\vDash n + 0 = n$ is valid, we conclude by the modus ponus rule $\vDash \exists l : n + l = n$ which shows reflexivity.
That transitivity holds follows from the following computation:

$$\begin{aligned} \vDash n \leq m \wedge m \leq l &\implies (\exists k : n + k = m) \wedge (\exists j : m + j = l) \\ &\implies \exists k \exists j : (n + k = m \wedge m + j = l) \\ &\implies \exists k \exists j : (n + k + j = m + j = l) \\ &\implies \exists k \exists j \exists i : (n + i = l) \\ &\implies n \leq l \end{aligned}$$

where the second implication holds by

$$(T77) \vDash (\phi \wedge \exists \psi) \implies \exists x(\phi \wedge \psi),$$

and the fifth implication holds by

$$(T50) \vDash (\exists \phi) \implies \phi, \quad \text{if } x \text{ not a free variable in } \phi.$$

The anti-symmetry is proven in the same way as transitivity, the only difference is that we use $\vDash (n+l+k = n) \implies (l+k=0) \implies (l=0 \wedge k=0)$. □

Proposition 13. *Let l, m, n be variables of type $\mathbb{N}$. The following are equivalent:*

1. $\vDash (n \leq m) \wedge \neg(n = m)$.
2. $\vDash \exists l : n + l + 1 = m$.

If these conditions are fulfilled, we write $\vDash n < m$.

Proof. That (1) implies (2) follows by the following computation:

$$\begin{aligned}
\vDash n \leq m \implies \exists l : n + l = m \quad &\implies \quad \exists l : (n + l = m \wedge (l = 0 \vee \exists k : l = k + 1)) \\
&\implies \quad \exists l : (n + 0 = m \vee \exists k : n + k + 1 = m) \\
&\implies \quad (n = m) \vee \exists k : (n + k + 1 = m) \\
&\implies \quad \textbf{false} \vee \exists k : (n + k + 1 = m), \quad \text{since } \vDash \neg(n = m) \\
&\implies \quad \exists k : n + k + 1 = m
\end{aligned}$$

Note that we used $(\vDash \phi \wedge \psi)$ if and only $\vDash \phi$ and $\vDash \psi$.
To show (2) $\implies$ (1), it suffices to show

$$\vDash (\exists l : n + l + 1 = m) \implies (\exists k : n + k = m), \quad ((\exists l : n + l + 1 = m) \wedge (n = m)) \implies \textbf{false}.$$

The first formula is immediately and the second equation follows in a straightforward way where we use $n + l + 1 = n \implies s(l) = l + 1 = 0 \implies \textbf{false}$. □

Proposition 14. *("Law of trichotomy") Let m, n be variables of type $\mathbb{N}$, then:*

1. $\vDash (n < m) \vee (n = m) \vee (n > m)$
2. $\vDash \neg((n < m) \wedge (n = m))$
3. $\vDash \neg((n = m) \wedge (n > m))$
4. $\vDash \neg((n < m) \wedge (n > m))$

Proof. The first formula is proven by induction on m. The base case follows from $(P1)$ as follows:

$$\begin{aligned}
\vDash (m = 0) \vee \exists k(m = s(k)) \quad &\implies \quad (m = 0) \vee \exists k : (m = k + 0 + 1) \\
&\implies \quad (m = 0) \vee (0 < m) \\
&\implies \quad (m = 0 \vee 0 < m \vee 0 > m)
\end{aligned}$$

For the induction step, it suffices to show

$$\vDash n < m \implies n < m + 1, \quad \vDash n = m \implies n < m + 1, \quad \vDash m < n \implies n = m + 1 \vee n > m + 1,$$

because then we conclude the induction step from

$$(T35) \vDash ((\phi \implies \delta) \wedge (\psi \implies \delta)) \implies (\phi \vee \psi \implies \delta).$$

The first two are immediate, the third formula follows again from $(P1)$:

$$\begin{aligned} \vDash n > m &\implies \exists l : m + l + 1 = n \\ &\implies \exists l : (m + l + 1 = n \wedge (l = 0 \vee \exists k : l = k + 1)) \\ &\implies (m + 0 + 1 = n) \vee \exists k : (m + k + 1 + 1 = n) \\ &\implies (n = m + 1) \vee (n > m + 1) \end{aligned}$$

The formulas (2) and (3) are immediate because $\vDash n < m \implies \neg(n = m)$.
Formula (4) is shown as follows:

$$\begin{aligned} ((n < m) \wedge (n > m)) &\implies (\exists k : n + k + 1 = m) \wedge (\exists l : m + l + 1 = n) \\ &\implies \exists k \exists l : (n + k + 1 = m \wedge m + l + 1 = n) \\ &\implies \exists k \exists l : (m + l + 1 + k + 1 = m) \\ &\implies \exists k \exists l : (l + 1 + k + 1 = 0) \\ &\implies \exists k \exists l : \textbf{false}, \quad \text{by } (P2) \vDash \neg(s(n) = 0) \text{ since } l + 1 + k + 1 = s(l + 1 + k) \\ &\implies \textbf{false} \end{aligned}$$

□

Proposition 15. *Let l, m, n be variables of type $\mathbb{N}$. Then*

1. $\vDash 0 \leq n$,
2. $\vDash 0 < n + 1$,
3. $\vDash n \leq m \iff n + l \leq m + l$,
4. $\vDash n < m \iff n + l < m + l$,
5. $\vDash n \leq m \implies n \cdot l \leq m \cdot l$,
6. $\vDash n \cdot l \leq m \cdot l \implies (l = 0) \vee (n \leq m)$,
7. $\vDash n \cdot l < m \cdot l \implies n < m$.

Proof. That formulas 1 and 2 are valid follows from $\vDash n = n + 0$. To show formula 3, we show the two implications. From left to right we have:

$$\vDash n \leq m \implies \exists k : n + k = m \implies \exists k : n + l + k = n + k + l = m + l \implies n + l \leq m$$

. From right to left, we have

$$\vDash n + l \leq m + l \implies \exists k : n + k + l = n + l + k = m + l \implies \exists k : n + k = m \implies n \leq m.$$

Formula 4 is proven in the same way as formula 3. We show 5 by induction on m. The base case follows from the following computation:

$$\begin{aligned} \vDash n \leq 0 &\implies \exists k : n + k = 0 \implies n = 0 \\ &\implies n \cdot l = 0 \cdot l \implies (n \cdot l) + 0 = 0 \cdot l \\ &\implies \exists k : n \cdot l + k = l \implies n \cdot l \leq 0 \cdot l \end{aligned}$$

The induction step follows from:

$$\begin{aligned} n \leq m + 1 &\implies \exists k : n + k = m + 1 \\ &\implies \exists k : (n + k) \cdot l = (m + 1) \cdot l \\ &\implies \exists k : n \cdot l + k \cdot l = (m + 1) \cdot l \\ &\implies \exists j : n \cdot l + j = (m + 1) \cdot l \\ &\implies n \cdot l \leq (m + 1) \cdot l \end{aligned}$$

Formula 6 is shown by induction on m. How the base case is proven, we have already done previously by concluding that $\vDash n \cdot l \leq 0 \cdot l = 0 \implies n = 0 \vee l = 0 \implies (n \leq 0) \vee (l = 0)$.
The induction step is proven using the localization principle, so we assume

$$\vDash n \cdot l \leq m \cdot l \implies (l = 0 \vee n \leq m)$$

and we have to show

$$\vDash n \cdot l \leq (m+1) \cdot l \implies (l = 0 \vee n \leq (m+1))\,.$$

The latter indeed holds (under the assumption) by the following computation:

$$\begin{aligned}
\vDash (n \cdot l \leq (m+1) \cdot l) \quad &\implies \quad (n \cdot l \leq (m+1) \cdot l) \wedge (n = 0 \vee \exists k : n = k+1)) \\
&\implies \quad (0 \leq (m+1) \cdot l) \wedge (n \cdot l \leq (m+1) \cdot l \wedge n = k+1) \\
&\implies \quad \mathbf{true} \wedge ((k+1) \cdot l \leq (m+1) \cdot l \wedge n = k+1) \\
&\implies \quad k \cdot l + l \leq m \cdot l + l \wedge (n = k+1) \\
&\implies \quad k \cdot l \leq m \cdot l \wedge (n = k+1), \quad \text{by formula 3} \\
&\implies \quad ((l = 0) \vee (k \leq m)) \wedge (n = k+1), \quad \text{by assumption} \\
&\implies \quad ((l = 0) \vee (k+1 \leq m+1)) \wedge (n = k+1) \\
&\implies \quad ((l = 0) \vee (n \leq m+1))
\end{aligned}$$

Formula 7 is shown in the same way as 6. □

Proposition 16. *("**Euclidean division**") Let a, b, q, r be variables of type $\mathbb{N}$. Then*

$$\vDash \neg(b = 0) \implies (\exists!(q, r) : a = b \cdot q + r \wedge r < b)\,.$$

Proof. Fix some variable b and define

$$P_b := \{a | \exists q : b \cdot q \leq a < b \cdot (q+1)\}\,.$$

We claim that $\vDash \neg(b =) \implies P_b = \mathbb{N}$. By $(P4)$, it suffices to show $\vDash \neg(b = 0) \implies 0 \in P_b$ and $\vDash \neg(b = 0) \implies (a \in P_b \implies (a+1) \in P_b)$. These indeed are valid because:

$$\begin{aligned}
\vDash \neg(b = 0) \quad &\implies \quad b \cdot 0 = 0 \leq 0 < b + 1 = b \cdot (0+1) \\
\vDash \neg(b = 0) \quad &\implies \quad a \in P_b \\
&\implies \quad \exists q : b \cdot q \leq a < b \cdot (q+1) \\
&\implies \quad \exists q : b \cdot q \leq a \wedge a + 1 \leq b \cdot (q+1) \\
&\implies \quad \exists q : b \cdot q \leq a \wedge (a + 1 = b \cdot (q+1) \vee a + 1 < (q+1)) \\
&\implies \quad \exists q : b \cdot q \leq a \wedge (a + 1 < b \cdot (q+2) \vee a + 1 < (q+1)) \\
&\implies \quad \exists q : b \cdot q \leq a + 1 < b \cdot (q+2) \wedge b \cdot q \leq a + 1 < (q+1)
\end{aligned}$$

□

4 Examples

Example 4. *Let X be a discrete topological space and consider the (grothendieck) topos $\mathcal{E} := Sh(X)$ of sheaves over X. Let $\tilde{\mathbb{N}}$ be the natural number object in $\mathcal{E}$ and let $m : \mathbf{1} \to \tilde{\mathbb{N}}$ be a global element. Then we have*

$$\vDash \{n | m \leq n \leq m+1\} = \{m\} \cup \{m+1\}.$$

Moreover, if X is infinite, then contains this object uncountably many global elements.

Proof. First notice that since X is discrete and if F is a sheaf, we have for each open $U \subseteq X$ that $F(U) = \bigsqcup_{x \in U} F(\{x\})$. So we have that $\mathcal{E}$ is $\mathbf{Set}^X$, i.e. an object is a collection of sets indexed by the elements of X and a morphism from $(A_x)_{x \in X}$ to $(B_x)_{x \in X}$ is a collection of morphisms $(f_x : A_x \to B_x)_{x \in X}$. All the structures are given object wise as in **Set** as in the following sense:
The terminal object is a collection of singletons $(\{\star\})_{x \in X}$, the subobject classifier is given by a collection two-element sets $(\{0,1\})_{x \in X}$ and the morphism true consists of the morphisms $\{\star\} \to \{0,1\} : \star \mapsto 1$. The natural number object is given by $(\mathbb{N})_{x \in X}$ with successor morphism (resp. zero morphism) the collection of successor morphisms $(\mathbb{N} \to \mathbb{N} : n \mapsto n+1)_{x \in X}$ (resp. zero morphisms $(\{\star\} \mapsto \mathbb{N} : \star \mapsto 0)_{x \in X}$.
A global element of $\mathbb{N}$ is given as a collection of natural numbers $n := (n_x)_{x \in X}$ (with $n_x \in \mathbb{N}$) and (considered as subobject of the n.n.o), it has characteristic morphism given by taking the characteristic morphism at each *level*, more precisely: The characteristic morphism of $n := (n_x)_x$ is given by

$$\chi_n : (\mathbb{N})_{x \in X} \to (\{0,1\})_{x \in X} : (m_x)_x \mapsto (\chi_{n_x}(m_x))_x,$$

where χ_{n_x} is the characteristic morphism of $\{n_x\} \subseteq \mathbb{N}$ in **Set**, i.e. $\chi_{n_x}(m_x) = 1 \iff m_x = n_x$. The supremum morphism is given by

$$(\{0,1\})_{x \in X} \times (\{0,1\})_{x \in X} \to (\{0,1\})_{x \in X} : ((a_x)_x, (b_x)_x) \mapsto (a_x \vee b_x)_x.$$

Consider the object $\{m\} \cup \{m+1\} = \{n | m = n \vee m+1 = n\}$. The characteristic morphism of this object is given by $\vee \circ (\chi_m, \chi_{m+1})$. So a global element $n := (n_x)_{x \in X}$ belongs to this object (in the sense that $\vDash n \in \{m\} \cup \{m+1\}$ is indeed valid) precisely when $\vee \circ (\chi_m(n), \chi_{m+1}(n)) = (1)_x$. This is equivalent with saying:

$$\forall x : n_x = m_x \vee n_x = m_x + 1.$$

Since $n_x, m_x \in \mathbb{N}$, this is equivalent with

$$\forall x : m_x \leq n_x \leq m_x + 1.$$

This means precisely $\vDash m \leq n \leq m+1$, so we conclude

$$\vDash \forall n : n \in \{m\} \cup \{m+1\} \iff n \in \{k | m \leq k \leq m+1\},$$

which shows the claim by $(T92)$ **the axiom of extensionality**.
The global elements of $\{m\} \cup \{m+1\}$ are thus given by elements $(n_x)_{x \in X}$ with $n_x \in \{m_x, m_x + 1\}$, so the number of global elements is thus given by $2^{|X|}$. So if X is infinite, the number of global elements is indeed uncountable. □

If we consider the previous example with X a 2-element set, we can conclude that that although the n.n.o is *internally* totally ordered, we do not have this *externally*:

Example 5. *Let $n, m : \mathbf{1} \to \mathbb{N}$ be global elements. The Law of trichotomy allows us to conclude $\vDash (n \leq m) \vee (m \leq n)$, but we do not have*

$$\vDash n \leq m \text{ or } \vDash m \leq n,$$

in general.

Proof. Consider $\mathcal{E}$ the topos of sheaves over the discrete space with 2 elements, i.e. $\mathcal{E} = \mathbf{Set} \times \mathbf{Set}$. Consider the global elements $(0,1)$ and $(1,0)$ of $\mathbb{N}$. Neither of them are smaller then the other. □

Just as in the case of infinite objects, not being boolean can sometimes leads to unexpected behaviour, for example:

Example 6. *Call a global element $p : \mathbf{1} \to \mathbb{N}$ **prime** if*

$$\vDash p = a \cdot b \implies (p = a \vee p = b).$$

Now consider again the topos $\mathcal{E} = \mathbf{Set} \times \mathbf{Set}$ *as in the previous example. The global element* $(3,3)$ *can be written as the product* $(3,1) \cdot (1,3)$*. But we can actually conclude that* $(3,3)$ *is prime, indeed: We have* $\vDash (m,n) \in \{(a,b)\} \cup \{(c,d)\}$ *if and only if*

$$(a = m \text{ or } c = a) \text{ and } (n = b \text{ or } c = d),$$

this is the same reasoning to show $\vDash \{n | m \leq n \leq m+1\} = \{m\} \cup \{m+1\}$*. So we have* $(3,3) \in \{(3,1)\} \cup \{(1,3)\} = \{p | p = (3,1) \vee p = (1,3)\}$*.*

In **Set**, the global elements of the natural number object are precisely the natural numbers, but in general we can have more global elements:

Example 7. *Let* $\mathcal{E}$ *be the category whose objects are sequences of sets* $\{A_n\}_{n\in\mathbb{N}}$ *up to the equivalence defined by:*

$$\{A_n\}_{n\in\mathbb{N}} \sim \{B_n\}_{n\in\mathbb{N}} : \iff \exists n_0 : \forall n \geq n_0 : A_n = B_n.$$

A morphism between sequences is a sequence of morphisms which also coincide starting from a certain index. Since there is no relation between objects/morphisms of different indices and because equivalent sequences are the same after a certain index, all constructions are computed at each index. So the terminal object is the sequence consisting of the terminal object in **Set** *(i.e. singleton sets), the subobject classifier is the sequence consisting of the subobject classifier in* **Set** *(i.e. a two-element set) and the characteristic morphism of a subsequence (a sequence of functions which from a certain index only consists of injections) is given by taking the characteristic morphism at each level, and so on.*
The natural number object is represented by $\{\mathbb{N}\}_{n\in\mathbb{N}}$ *with zero (resp. successor) morphism given by the morphism mapping the sequence of singleton sets to the sequence of singleton sets* $\{\{0\}_n\}$ *(resp.* $\{\mathbb{N} \xrightarrow{s} \mathbb{N}\}_{n\in\mathbb{N}}$*). So we have* $1 := s(0)$ *is given by the constant sequence of singletons* $\{1\}$*, more generally* $n := s(n-1)$ *is given by the sequence of singletons* $\{n\}$*. The morphism* $\{\{\star\} \to \mathbb{N} : \star \mapsto n\}_{n\in\mathbb{N}}$ *is injective at each level, hence a monomorphism in* $\mathcal{E}$*, thus this is a subobject of the natural number object. Since the addition is computed at each index, i.e.* $\{\{i_n\}\}_{n\in\mathbb{N}} + \{\{j_n\}\}_{n\in\mathbb{N}} = \{\{i_n + j_n\}\}_{n\in\mathbb{N}}$ *(with* $i_n, j_n \in \mathbb{N}$*), we also have that* $\leq$ *is computed at each index, thus for each* $m \in \mathbb{N}$*, we have* $\{\{m\}\}_{n\in\mathbb{N}} < \{\{n\}\}_{n\in\mathbb{N}}$*.*
Notice that this global element is not maximal (w.r.t. the order) because it is smaller then $\{\{n+k\}\}_{n\in\mathbb{N}}$ *for any natural number* k*.*

5 Finite objects in a topos

In this section we introduce two notions of when an object is finite. The first notion is that of Kuratowski finiteness, these are objects which (in the internal logic) can be build as a finite union of singletons and the second notion is that of finite cardinals which are objects which are *downsets* of global elements of the natural number object.

5.1 Kuratowski finite objects

Definition 5. *An object* A *of a topos is* ***Kuratowski finite*** *if the following holds:*

$$\vDash \forall \mathcal{P} : \begin{cases} (\emptyset \in \mathcal{P}) \wedge (\forall a : \{a\} \in \mathcal{P}) \\ \wedge\, (\forall B \forall C : B \in \mathcal{P} \wedge C \in \mathcal{P} \implies B \cup C \in \mathcal{P}) \end{cases} \implies (A \in \mathcal{P}),$$

where $a \in Var(A), B, C \in Var(\Omega^A), \mathcal{P} \in Var(\Omega^{\Omega^A})$ *and* $\emptyset$ *is the constant (of type* Ω^A*) representing the initial subobject* $\mathbf{0} \to A$*.*

Example 8. *In* **Set**, $\mathbf{Set}_G$ *(with* G *a group), the Kuratowski finite objects are the* G*-sets with finitely many elements.*

Proof. If A is a set (or G-set) which is Kuratowski finite, then we can consider

$$\mathcal{P} := \{B \subseteq A | B \text{ finite } \}.$$

It clearly contains the empty set, all singletons and is closed under the union, so by Kuratowski-finiteness we have $A \in \mathcal{P}$, thus A is finite. That a finite set is Kuratowski-finite is immediate because if any singleton is in $\mathcal{P}$, we can take there union (since there are only finitely many) and this lies again in $\mathcal{P}$, but this is the complete set. □

Proposition 17. *Let A be a Kuratowski finite object. Every complemented subobject of A is Kuratowski finite.*

Proof. Let $S \subseteq A$ be a complemented subobject. In order to show that S is Kuratowski finite, it suffices by $(T53)$ the principle of localization that for each $\mathcal{P} \in \Omega^A$,

$$\vDash (\emptyset \in \mathcal{P}) \wedge (\forall a : \{a\} \in \mathcal{P}) \wedge (\forall B \forall C : B \in \mathcal{P} \wedge C \in \mathcal{P} \implies B \cup C \in \mathcal{P})$$

implies $\vDash S \in \mathcal{P}$. Since $A \cap S = S$, we have shown the statement if we can conclude $A \in Q := \{D | D \cap S \in \mathcal{P}\}$. So using that A is Kuratowski finite, it suffices to show the following three cases:

1. Since $\emptyset \cap S = \emptyset$, $\vDash \emptyset \in Q$.
2. Let $a \in Var(a)$. Since S is complemented (with complement $\mathcal{C}S$) we have $\vDash (a \in S) \vee \neg(a \in S)$ because
$$A = S \cup \mathcal{C}S = \{b | b \in S \vee b \in \mathcal{C}S\}.$$
So $\{a\} \in Q$ now follows by the following computation:
$$\begin{aligned} \vDash (a \in S) \vee \neg(a \in S) &\implies (\{a\} \cap S = \{a\}) \wedge (\{a\} \cap S = \emptyset) \\ &\implies \{a\} \cap S \in \mathcal{P}, \quad \text{by hypothesis } \mathcal{P} \\ &\implies \{a\} \in Q \end{aligned}$$
3. Let $B, C \in Var(\Omega^A)$ such that $\vDash B \in Q \wedge C \in Q$

So we indeed can conclude from the Kuratowski finiteness of A, that $\vDash A \in Q$ and thus $\vDash S = A \cap S \in \mathcal{P}$, then

$$\begin{aligned} \vDash S = A \cap S \in \mathcal{P} &\implies B \cap S \in \mathcal{P} \wedge C \cap S \in \mathcal{P} \\ &\implies (B \cap S) \cup (C \cap S) \in \mathcal{P}, \quad \text{by hypothesis } \mathcal{P} \\ &\implies (B \cup C) \cap S \in \mathcal{P} \\ &\implies B \cup C \in Q \end{aligned}$$

□

The following example shows that the previous proposition does not hold for general (i.e. non-complemented) subobjects:

Example 9. *Let $X = \{x, y\}$ be the sierpinski space, with only 1 open point y. A presheaf thus assigns sets to $\emptyset, \{y\}$ and $\{x, y\}$ and morphisms into the opposite direction. A sheaf must map $\emptyset$ to $\emptyset$, thus a sheaf F is specified by the data $F(\{x, y\}) \to F(\{y\})$. A morphism is a natural transformation, thus a morphism between such sheaves $F \to G$ is given by a commutative diagram:*

$$\begin{array}{ccc} F(\{x,y\}) & \longrightarrow & F(\{y\}) \\ \downarrow & & \downarrow \\ G(\{x,y\}) & \longrightarrow & G(\{y\}) \end{array}$$

So we have that the topos $\mathcal{E}$ of sheaves on X is given by the arrow category of **Set**, *i.e. objects are functions and morphisms are commuting squares between the functions.*
We now claim that the Kuratowski finite objects are the surjective functions between finite sets.
The powerobject of $\alpha : A_1 \to A_2$ is given by the function:

$$\mathbb{P}(\alpha)_1 := \{\beta : B_1 \to B_2 | B_1 \subseteq A_1, B_2 \subseteq A_2, \beta = \alpha|_{B_1} : B_1 \to \alpha(B_1) \subseteq B_2\} \to \mathbb{P}(\alpha)_2 := \{B | B \subseteq A_2\},$$

which maps $\beta : B_1 \to B_2$ to B_2.
A subobject $\mathcal{P}$ consists of the powerobject is given by a function $\mathcal{P}_1 \to \mathcal{P}_2$ which still sends a function to its codomain and where $\mathcal{P}_1 \subseteq \mathbb{P}(\alpha)_1$ and $\mathcal{P}_2 \subseteq \mathbb{P}(\alpha)_2$ with the extra condition that the codomain of every function in $\mathcal{P}_1$ lies in $\mathcal{P}_2$.
The initial subobject is given by $\{\emptyset \to \emptyset\} \to \emptyset$, a singleton a of A is given by $\{\{a\} \to \{\alpha(a)\}\} \to \{\alpha(a)\}$ and the union of $(\beta : B_1 \to B_2) \to B_2$ with $(\gamma : C_1 \to C_2) \to C_2$ is given by

$$(\beta \cup \gamma : (B_1 \cup C_1) \to (B_2 \cup C_2)) \to (B_2 \cup C_2).$$

Assume $\alpha : A_1 \to A_2$ is Kuratowski finite. Define $\mathcal{P}$ as:

$$\mathcal{P}_1 := \{\beta : B_1 \to B_2 | B_1, B_2 \text{ finite}, \beta = \alpha|_{B_1} \text{ and is surjective } \},$$

and $\mathcal{P}_2 = \{B | B \subseteq A_2\}$. Clearly we have that the initial subobject, singletons are in $\mathcal{P}$ and it is closed under the union, thus by Kuratowski-finiteness, we have α is also in $\mathcal{P}_1$ (and A_2 in $\mathcal{P}_2$). So α is then by definition of $\mathcal{P}_1$ a surjective function between finite sets.
Conversely let $\alpha : A_1 \to A_2$ be a surjection between finite sets. We now show that α is Kuratowski finite, so consider a subobject $\mathcal{P} := \mathcal{P}_1 \to \mathcal{P}_2$ of $\mathbb{P}(\alpha)$ which satisfy the conditions, so it closed under all singletons and finite unions. So in particular we have that the union of all $\alpha|_{\{a\}} : \{a\} \to \{\alpha(a)\}$ is in $\mathcal{P}_1$, but A_1 is finite, thus it is a finite union of its singletons, thus $\alpha|_{A_1} : A_1 \to \alpha(A_1) \in \mathcal{P}_1$, but α is surjective, this $\alpha = \alpha|_{A_1} : A_1 \to A_2 \in \mathcal{P}_1$ from which we conclude $\alpha \in \mathcal{P}$ which shows that α is Kuratowski finite.

5.2 Finite cardinals

Definition 6. *In a topos with a natural number object $(\mathbb{N}, 0, s)$, a* ***finite cardinal*** *is an object of the form*

$$[n] := \{m | m < n\},$$

where $m \in Var(\mathbb{N})$ is a variable and $n : \mathbf{1} \to \mathbb{N}$ is a global element.

Proposition 18. *The finite cardinal associated to the global element 0 (resp. 1) is the initial object (resp. terminal object) and for each global element $n : \mathbf{1} \to \mathbb{N}$ we have*

$$\vDash \{m | m < n + 1\} = \{m | m < n\} \cup \{n\}.$$

Proof. By $(P3) \vDash \neg(s(n) = 0)$, we have

$$\vDash m < 0 \implies \exists k : m + k + 1 = 0 \implies \exists k : (s(m + k) + 1 = 0) \implies \textbf{false}.$$

So $[0] = \{n |$ **false** $\}$. This shows the claim because the initial object is the unique object A such that $\vDash \neg(\exists x : x \in A)$ (with x a variable of type A), see for example proposition 6.10.4 in [1].
Since $\vDash m < 1 \implies \exists k : m + k + 1 = 1 \implies \exists k : m + k = 0 \implies m = 0$, we have $[1] = \{n | n = 0\}$. But, again by proposition 6.10.4, we have that the terminal object is the unique object A such that $\vDash \exists! x (x \in A)$, which shows that [1] is indeed the terminal object.
We now show $\vDash \{m | m < n + 1\} = \{m | m < n\} \cup \{n\}$. This follows by the following computation

$$\begin{aligned}
\vDash m < n + 1 &\implies \exists k : m + k + 1 = n + 1 \\
&\implies \exists k : m + k = n \\
&\implies m \leq n \\
&\implies m < n \vee m = n \\
\vDash (m < n \vee m = n) &\implies (m < n + 1 \vee m + 0 + 1 = m + 1 = n + 1) \\
&\implies (m < n + 1) \vee (m < n + 1) \\
&\implies m < n + 1
\end{aligned}$$

Notice that this indeed shows the claim because $\{m|m<n\}\cup\{n\}=\{m|m<n\vee m=n\}$. □

Corollary 7. *Every finite cardinal (in a topos with a n.n.o.) is Kuratowski finite.*

Proof. For an object A, define the object $K(A)$ as

$$K(A)=\left\{S|\forall\mathcal{P}:\begin{cases}(\emptyset\in\mathcal{P})\wedge(\forall a:\{a\}\in\mathcal{P})\\ \wedge(\forall B\forall C:B\subseteq S\wedge C\subseteq S\wedge B\in\mathcal{P}\wedge C\in\mathcal{P}\implies B\cup C\in\mathcal{P})\end{cases}\implies(S\in\mathcal{P})\right\}$$

A subobject $S\subseteq A$ is Kuratowski finite if and only if $\vDash S\in K(A)$. So we have to show

$$\vDash\{m|m<n\}\in K(\mathbb{N}),$$

for $m,n\in Var(\mathbb{N})$. We show this by induction on n, i.e. we have to show

$$\begin{aligned}&\vDash\{m|m<0\}\in K(\mathbb{N})\\ \vDash\{m|m<n\}\in K(\mathbb{N})\implies&\{m|m<n+1\}\in K(\mathbb{N})\end{aligned}$$

Since $\{m|m<0\}$ is the initial object, we clearly have that it lies in $K(\mathbb{N})$ (by the condition $\emptyset\in\mathcal{P}$). The induction step follows because

$$\vDash\{m|m<n\}\cup\{n\}=\{m|m<n+1\},$$

indeed

$$\begin{aligned}\vDash\{m|m<n\}\in K(\mathbb{N})\quad&\implies\quad\{m|m<n\}\in K(\mathbb{N})\wedge\{n\}\in K(\mathbb{N})\\ &\implies\quad\{m|m<n\}\cup\{n\}\in K(\mathbb{N})\\ &\implies\quad\{m|m<n+1\}\in K(\mathbb{N}).\end{aligned}$$

□

So any finite cardinal is Kuratowski finite, but the converse does in general not hold:

Example 10. *Consider the Sierpinski topos, i.e. the arrow category of* **Set**. *The Kuratowski finite objects are the surjective functions between finite sets, but an arrow is (isomorphic to) a finite cardinal if and only if it is a bijection between finite sets, indeed: Since the terminal object is $\{\star\}\to\{\star\}$, so a subobject of the natural number object is given by a commutative diagram:*

$$\begin{array}{ccc}\{\star\}&\xrightarrow{Id}&\{\star\}\\ \downarrow&&\downarrow\\ \mathbb{N}&\xrightarrow{Id}&\mathbb{N}\end{array}$$

Thus the global elements correspond with the (ordinary) natural numbers, thus a finite cardinal $[n]$ is given by the function:

$$\{m|m<n\}\xrightarrow{Id}\{m|m<n\}.$$

So an isomorphic object to a finite cardinal is given by a function $f:A\to B$ such that there are bijections $\{m|m<n\}\to A$ and $\{m|m<n\}\to B$ (thus A,B are both finite) and since Id is a bijection, f should also be a bijection.

Proposition 19. *("**Cardinal arithmetic**") Let m,n be global elements of the natural number object. Then*

1. $[m+n]\cong[m]\coprod[n]$;
2. $[m\cdot n]\cong[m]\times[n]$;

Proof. In both cases we use proposition 6.10.9 in [1] which says: Let $\phi : A \times B \to \Omega$ be a formula, if $\vDash \exists! b \phi$, then there exists a unique morphism $f : A \to B$ such that $\vDash \phi(a, f(a))$.
We first prove (1). The proposition allows us the define morphisms

$$f_n : [n] \to [m+n] : k \mapsto k, \quad f_m : [m] \to [m+n] : k \mapsto n+k.$$

So by the universal property of the coproduct, there exists a (unique) morphism $f : [m] \coprod [n] \to [m+n]$ such that $f_n = f \circ i_n, f_m = f \circ i_m$ (with i_n, i_m the morphisms from $[n], [m]$ into the coproduct). We now show that ϕ is an isomorphism, so we have to show that is both mono and epi and thus we have to show that it is injective and surjective in the internal logic. That it is surjective follows from:

$$\begin{aligned}
\forall k : k < m+n \quad &\implies \quad (k < n \vee k \geq n) \implies (k < n \vee \exists i : k = n+i)\,, \\
&\implies \quad (k = \phi_n(k) = \phi \circ i_n(k) \vee \exists i : k = n+i = \phi_m(i) = \phi(i_n(i)))\,, \\
&\implies \quad \exists j_1 : k = \phi(j_1) \vee \exists j_2 : k = \phi(j_2), \\
&\implies \quad \exists j : k = \phi(i).
\end{aligned}$$

We now show injectivity: Let i, j be global elements of $[m] \coprod [n]$, such that $\phi(i) = \phi(j)$. Since $[m] \coprod [n]$ is the coproduct, it satisfies (in the internal logic)

$$\begin{aligned}
\vDash \quad & \exists x_i : i = i_n(x_i) \vee \exists y_i : i = i_m(y_i) \\
\vDash \quad & \neg\left(\exists x_i : i = i_n(x_i) \wedge \exists y_i : i = i_m(y_i)\right)
\end{aligned}$$

with x_i a variable of type $[m]$ and y_i of type $[n]$. So from this we can conclude

$$\vDash \phi(i) = \phi(j) \quad \implies \quad (\exists x_i : i = i_n(x_i) \vee \exists y_i : i = i_m(y_i)) \wedge (\exists x_j : j = i_n(x_j) \vee \exists y_j : i = i_m(y_j)) \wedge \phi(i) = \phi(j)$$

In the internal logic, this implies

$$\begin{aligned}
\exists x_i : i = i_n(x_i) \wedge \exists x_j : j = i_n(x_j) \wedge \phi_n(x_i) = \phi(i_n(x_i)) = \phi(i) = \phi(j)\phi(i_n(x_j)) = \phi_n(x_j), \\
\exists y_i : i = i_m(y_i) \wedge \exists y_j : j = i_m(y_j) \wedge \phi_m(y_i) = \phi(i_m(y_i)) = \phi(i) = \phi(j)\phi(i_m(y_j)) = \phi_m(y_j), \\
\exists x_i : i = i_n(x_i) \wedge \exists y_j : j = i_m(y_j) \wedge \phi_n(x_i) = \phi(i_n(x_i)) = \phi(i) = \phi(j)\phi(i_m(y_j)) = \phi_m(y_j),
\end{aligned}$$

But ϕ_n and ϕ_m are monomorphisms, hence injective in the internal logic, thus in the internal, the first two equations imply $x_i = x_j$ resp. $y_i = y_j$ from which we conclude (in the internal logic) $i = i_n(x_i) = i_n(x_j) = j$ resp. $i = i_m(y_i) = i_m(y_j) = j$. The thirth equation implies $x_i = \phi_n(x_i) = \phi_m(y_j) = n + y_j$ which implies **false** because $x_i < n$ and $n + y_j > n$. The fourth equation also implies **false**, thus this indeed implies injectiveness in the internal logic, thus ϕ is a monomorphism which shows that ϕ is an isomorphism.
We now show $[m] \times [n] \cong [m \cdot n]$. We assume $m \neq 0$, otherwise the statement is immediate since $[m]$ is then the initial object.
Define a morphism ϕ as:

$$\phi : [m] \times [n] \to [m \cdot n] : (u, v) \mapsto v \cdot m + u.$$

That this is an isomorphism follows from the euclidean division. We first show it is an epimorphism: Let k be a global element of $[m \cdot n]$, then:

$$\vDash m \neq 0 \quad \implies \quad (k < m \cdot n) \wedge \exists!(q, r)\,(k = (q \cdot m + r) \wedge (r < m))\,.$$

So from this we would like to conclude $\vDash m \neq 0 \implies \exists(q, r) : \phi(r, q) = q \cdot m + r = k$, which shows surjectivity. Since $r < m$, it only remains to argue $q < n$ which follows from the following computation:

$$\begin{aligned}
\vDash m \neq 0 \quad &\implies \quad (k < m \cdot n) \wedge \exists!(q, r)\,(k = (q \cdot m + r) \wedge (r < m)) \\
&\implies \quad (k < m \cdot n) \wedge \exists!(q, r)\,(k = (q \cdot m + r) \wedge (\exists i : r + i = m)) \\
&\implies \quad \exists!(q, r)\,((\exists i : q \cdot (r+i) + r = q \cdot m + r = k < m \cdot n = (r+i) \cdot n = r \cdot n + i \cdot n)) \\
&\implies \quad \exists!(q, r)\,((\exists i : q \cdot (r+i) + r = q \cdot m + r = k < m \cdot n = (r+i) \cdot n = r \cdot n + i \cdot n)) \\
&\implies \quad \exists!(q, r)\,((\exists i : (q+1) \cdot r + q \cdot i < n \cdot (r+i))) \\
&\implies \quad \exists!(q, r)\,((\exists i : q \cdot (r+i) = q \cdot r + q \cdot i < n \cdot (r+i))) \\
&\implies \quad \exists!(q, r) : \exists i : q < n
\end{aligned}$$

So we indeed can conclude surjectivity of ϕ. That ϕ is a mono (i.e. injective in the internal logic), follows immediate since (q, r) is unique. So ϕ is an isomorphism which shows the statement. □

Remark 2. *The previous proposition tells us that the full subcategory of finite cardinals is closed under finite products (and finite coproducts). One can even show that it is closed under exponentials and closed under pullbacks. Then we have that* $[2] = [s(s(0))]$ *forms a subobject classifier which makes this subcategory a topos. The details of this can be found in [2].*

References

[1] Francis Borceaux. *Handbook of Categorical Algebra 3: Categories of Sheaves.* Cambridge University Press, 1994.

[2] Peter T. Johnstone *Sketches of an Elephant: A Topos Theory Compendium. Volume* 1. Clarendon Press Oxford, 2002.