SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Exploring the Mathematical Multiverse
A brief overview of Elementary Topoi and their Internal Language

av

Jonathan Osser

2023 - K7

Exploring the Mathematical Multiverse

A brief overview of Elementary Topoi and their Internal Language

Jonathan Osser

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Anders Mörtberg, Ivan Di Liberti

2023

Abstract

In this thesis we do two things; first we present the theory of elementary topoi, for which we first present the notions of subobjects and subobject classifiers, as well as cartesian closed categories. Then we show how to construct, for each elementary topos, a formal language which interprets into the topos, the internal language. Atop the formal language we the build a proof system, and show its soundness. This allows for reasoning about the topos from the "inside", and we provide examples of this form of reasoning, including a proof that every elementary topos has an image factorisation. We go on to show how natural numbers may be defined for elementary topoi, and show that for a topos which has an object of natural numbers, the induction principle is sound with respect to the proof system we defined earlier. Finally, we give two examples of topoi: the category of finite sets, which has no notion natural numbers, and presheaf topoi, which generally do not validate the law of excluded middle.

Contents

1 Introduction **2**

2 Categorical preliminaries **2**
2.1 Categories, functors, and natural transformations 2
2.2 Finite limits and colimits 5

3 Subobjects and the subobject classifier **8**
3.1 Subobjects 8
3.2 Membership of subobjects 10
3.3 Some properties of the collection of subobjects 11
3.4 Subobject classifiers 13

4 Cartesian closed categories **15**

5 Elementary topoi **20**

6 Internal language **25**
6.1 The term-language 25
6.2 A proof system for the internal language 28
6.3 Soundness of the proof system 32
6.4 Using the internal language 35

7 Natural numbers objects **38**

8 Examples of elementary topoi **41**
8.1 **FinSet** 41
8.2 Presheaf topoi 42

9 Conclusion **45**

1 Introduction

In 1969 Lawvere and Tierney introduced the notion of elementary topoi [MR11, p. 2], in what Freyd called the "most important event in the history of categorical logic" [Fre72, p. 1]. They not only produced a first-order axiomatisation of the notion of topoi used by Grothendieck in algebraic geometry and sheaf theory, but also connected the idea to higher-order logic and type theories [MR11, p. 2]. In fact, "they saw that the usual models of (...) mathematics known at that time as well as the forcing method of Cohen were specific cases of these toposes" [MR11, p. 33].

The idea of interpreting a logical theory in a topos appeared in a paper by William Mitchell, published in 1972 [MR11, p. 68]. He introduced explicitly a language $L(\mathcal{E})$ for a topos $\mathcal{E}$ and its interpretation into $\mathcal{E}$. This was what would later develop into the internal language of a topos, a variant of which is presented in this thesis, and as will be shown, can be used to reason about the logic internal to the topos [MR11, p. 68].

Before the definition of elementary topoi was given, Lawvere presented a categorical axiomatisation of the theory of sets, ETCS, [MR11, p. 17]. In this axiomatisation, the notion of a natural numbers object was given, which provides ETCS what the axiom of infinity provides ZFC [MR11, p. 18]. While ETCS was left without much further study, the definition of natural numbers is still as useful for elementary topoi, and allows us to carry out many of the constructions we are used to in their internal language.

The goal of this thesis is to present the theory of elementary topoi, as well as how we can internalise a simple logical language inside such objects. We then show how we may use the internal language to prove properties about the topos itself. We begin in section 2 by recalling the basic concepts of category theory we require. In section 3 we move on to generalising the notion of subsets to arbitrary categories, and similarly we generalise the idea of function-sets in section 4. In section 5 we combine the work in the previous two sections to give the definition of *elementary topoi*, and show how the collections of subobjects in elementary topoi have rich structure. Next, in section 6, we construct a language which interprets into elementary topoi, and then upon this a system for proofs. We show the proof system sound, and then use it to show several properties about elementary topoi themselves. Section 7 introduces further the notion of natural numbers objects, and we show that the induction-principle is sound in any elementary topos with such an object. We end the thesis in section 8 with some example of elementary topoi, specifically **FinSet**, which is an elementary topos without a natural numbers object, and presheaf categories, which are elementary topoi whose internal logic is often not boolean.

The main reference used throughout thesis are a set of lecture notes for a course in category theory and categorical logic by Streicher [Str04], as well as the book *Elementary categories, elementary toposes* by McLarty [McL92].

2 Categorical preliminaries

This section is meant to cover the categorical preliminaries required for the development of the rest of the thesis.

2.1 Categories, functors, and natural transformations

Definition 2.1 (Categories)**.** A *category* $\mathcal{C}$ consists of the following data:

- a collection of objects $\mathrm{Ob}(\mathcal{C})$,

- for each pair of objects $A, B \in \mathrm{Ob}(\mathcal{C})$ a collection $\mathrm{Hom}(A, B)$, the morphisms of $\mathcal{C}$,
- for each object $A \in \mathrm{Ob}(\mathcal{C})$ a morphism $\mathrm{id}_A \in \mathrm{Hom}(A, A)$.
- for each object $A, B, C \in \mathrm{Ob}(\mathcal{C})$, $f \in \mathrm{Hom}(B, C)$, and $g \in \mathrm{Hom}(A, B)$, a morphism $f \circ g \in \mathrm{Hom}(A, C)$

with the constraints that for all objects A, B, C, D and morphisms $f \in \mathrm{Hom}(A, B), g \in \mathrm{Hom}(B, C), h \in \mathrm{Hom}(C, D)$ the equations $f \circ \mathrm{id}_A = f = \mathrm{id}_B \circ f$ and $(h \circ g) \circ f = h \circ (g \circ h)$ hold true.

Notation. When the category is clear from context, we write $f : A \to B$ for $f \in \mathrm{Hom}(A, B)$. When dealing with several categories we may write $\mathcal{C}(A, B)$ or $\mathrm{Hom}_{\mathcal{C}}(A, B)$ for the collection of morphisms from A to B in the category $\mathcal{C}$.

Definition 2.2 (Small and locally small categories)**.** Usually the collections of morphisms of category $\mathcal{C}$ form a set, in which case we say that $\mathcal{C}$ is *locally small.* When furthermore the collection of objects $\mathrm{Ob}(\mathcal{C})$ also forms a set, we say the category is *small.*

Definition 2.3 (Opposite category)**.** Given a category $\mathcal{C}$, we define its opposite category, $\mathcal{C}^{\mathrm{op}}$, as having the same objects as $\mathcal{C}$, and as collections morphisms $\mathrm{Hom}(A, B)$ the collection $\mathcal{C}(B, A)$. That is, the opposite category of $\mathcal{C}$ is the same with the morphisms flipped.

The prototypical example of a category is the category of sets, **Set**, having sets as objects and functions between sets as morphisms. Another is **FinSet**, the category of finite sets and functions between them.

Remark. Starting with the next section, we will generally write composition by juxtaposition, so fg instead of $f \circ g$ in an arbitrary category. For specific categories, such as **Set**, we still write $f \circ g$, so that it is harder to confuse with application $f(x)$.

Definition 2.4 (Monomorphisms, epimorphisms and isomorphisms)**.** Let $\mathcal{C}$ be a category. A morphism $f : A \to B$ in $\mathcal{C}$ is said to be

- a *monomorphism*, or *monic*, if for every pair of morphisms $g, h : X \to A$ such that $f \circ g = f \circ h$ it follows that $g = h$,
- an *epimorphism*, or *epic*, if for every pair of morphisms $g, h : B \to Y$ such that $g \circ f = h \circ f$ it follows that $g = h$,
- an *isomorphism* if there exists a morphism $g : B \to A$ such that $f \circ g = \mathrm{id}_B$ and $g \circ f = \mathrm{id}_A$.

Every isomorphism is both monic and epic, but it is not necessarily the case that a morphism which is both monic and epic is an isomorphism. When two objects A, B are isomorphic, we write $A \cong B$. A monomorphism is denoted by an arrow with tail, that is, $f : A \rightarrowtail B$. Similarly, an epimorphism is denoted by $f : A \twoheadrightarrow B$.

Definition 2.5 (Functors)**.** Given two categories $\mathcal{C}, \mathcal{D}$, a *functor* F from $\mathcal{C}$ to $\mathcal{D}$ consists of a mapping F_0 from the objects of $\mathcal{C}$ to the objects of $\mathcal{D}$, and for each pair of objects A, B of $\mathcal{C}$, a mapping F_1 between the morphisms from $\mathcal{C}(A, B)$ to $\mathcal{C}(F_0(A), F_0(B))$. Furthermore, we require for all $A, B, C \in \mathrm{Ob}(\mathcal{C})$ and $f : B \to C$, $g : A \to B$ that $F_1(\mathrm{id}_A) = \mathrm{id}_{F_0(A)}$ and $F_1(f \circ g) = F_1(f) \circ F_1(g)$.

We will usually omit the subscripts on the functor, write both $F(A)$ for $F_0(A)$ and $F(f)$ for $F_1(f)$. When the mapping of morphisms is injective for all pairs of objects A, B, we say the functor is faithful, and when it is surjective we call it full. If it is bijective on morphisms we call it fully faithful.

For any category $\mathcal{C}$ there is an identity functor $\mathrm{id}_{\mathcal{C}}$, which maps every object and morphism to itself. Similarly, given functors $F : \mathcal{D} \to \mathcal{E}$ and $G : \mathcal{C} \to \mathcal{D}$, their composite $F \circ G$ is defined by composing the object and morphism mappings. Preservation of identity and composition is in both cases a trivial exercise to show. The identities also act as units for composition, and composition is associative.

Definition 2.6 (Natural transformations)**.** Given two functors $F, G : \mathcal{C} \to \mathcal{D}$, a *natural transformation* α from F to G consists of a family of morphisms $\alpha_A : F(A) \to G(A)$ for each object A of $\mathcal{C}$, such that for all $f \in \mathcal{C}(A, B)$ the following square, usually called the naturality square, commutes:

$$\begin{tikzcd} F(A) \arrow[r, "\alpha_A"] \arrow[d, "F(f)"'] & G(A) \arrow[d, "G(f)"] \\ F(B) \arrow[r, "\alpha_B"'] & G(B). \end{tikzcd}$$

As with functors we are able to define the notion of an identity and composite natural transformation. For any functors $F, G, H : \mathcal{C} \to \mathcal{D}$ and natural transformations $\alpha : G \to H$ and $\beta : F \to G$, the identity transformation id_F is given by taking $\mathrm{id}_{F(A)}$ at each $A \in \mathrm{Ob}(\mathcal{C})$. We define the composite $\alpha \circ \beta$ by composing object-wise; $(\alpha \circ \beta)_A = \alpha_A \circ \beta_A$ for all objects A of $\mathcal{C}$. Naturality holds in either case, as is easily inspected.

A natural isomorphism is a natural transformation with an inverse transformation, or equivalently, a natural transformation in which each component is an isomorphism. Similarly, it is monic precisely when every component is monic, and the same holds for being an epimorphism.

Proposition 2.1
Given small category $\mathcal{C}$ and a category $\mathcal{D}$, the collection of functors $\mathcal{C} \to \mathcal{D}$ and natural transformations between them forms a category. This category will generally be denoted by $[\mathcal{C}, \mathcal{D}]$.

Definition 2.7 (Preshaves)**.** A functor from $\mathcal{C}^{\mathrm{op}}$ to $\mathbf{Set}$ is called a presheaf over $\mathcal{C}$, and the category of presheaves over $\mathcal{C}$ is denoted by $\mathbf{Set}^{\mathcal{C}^{\mathrm{op}}}$ or $[\mathcal{C}^{\mathrm{op}}, \mathbf{Set}]$.

Definition 2.8 (Yoneda embedding)**.** Given a locally small category $\mathcal{C}$ and an object $A \in \mathcal{C}$, we define the *yoneda embedding* of A, written $よ(A)$, to be the presheaf defined by mapping objects $B \in \mathcal{C}$ to $\mathcal{C}(B, A)$ and morphisms $f : B \to C$ to the function taking $g : A \to B$ to $g \circ f : A \to C$.

In fact, the assignment of each object A to its yoneda embedding is also functorial. That is, $よ$ is a functor from $\mathcal{C}$ to $[\mathcal{C}^{\mathrm{op}}, \mathbf{Set}]$ mapping objects to their yoneda embeddings and morphisms $f \in \mathcal{C}(A, B)$ to natural transformations mapping morphisms g to $f \circ g$. Naturality is again trivial.

Lemma 2.2 (Yoneda lemma [Str04, p. 17-19])
For any presheaf F over a small category $\mathcal{C}$ and object A of $\mathcal{C}$, we have a natural bijection $[\mathcal{C}^{\mathrm{op}}, \mathbf{Set}](よ(A), F) \cong F(A)$. Furthermore, the yoneda embedding ($よ$) is fully faithful.

A presheaf is said to be *representable* if it is naturally isomorphic to the yoneda embedding of some object. That is, a presheaf $F : \mathcal{C}^{\mathrm{op}} \to \mathbf{Set}$ is representable when $F \cong \mathcal{C}(-, X)$ for some X.

Definition 2.9. Given two functors $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$, we say that F is *left adjoint* to G if $\mathcal{D}(F(A), B) \cong \mathcal{C}(A, G(B))$ naturally in $A \in \mathrm{Ob}(\mathcal{C})$ and $B \in \mathrm{Ob}(\mathcal{D})$. In this case we also say that G is *right adjoint* to F.

Definition 2.10 (Slice categories)**.** Given a category $\mathcal{C}$ and an object A of said category, we may construct a new category $\mathcal{C}/A$, the *slice* over A. The objects of this category are morphisms $B \to A$ in $\mathcal{C}$, and the morphisms between to objects $B \to A$ and $C \to A$ are morphisms $f : B \to C$ such that the following diagram commutes:

$$\begin{tikzcd}
B \arrow[rr, "f"] \arrow[dr] & & C \arrow[dl] \\
& A &
\end{tikzcd}$$

2.2 Finite limits and colimits

In this subsection we define certain constructions, all falling under the label of either limit, or dually, colimit. We fix a category $\mathcal{C}$ for this subsection.

Definition 2.11. A *terminal* object in $\mathcal{C}$ is an object 1, such that for any other A of $\mathcal{C}$ there exists a unique arrow from A to 1. Dually, an *initial* object $\mathcal{C}$ is an object 0 such that for any object A of $\mathcal{C}$ there exists a unique arrow from 0 to T.

Proposition 2.3
If a terminal or initial object exists, then it is unique up to isomorphism.

Definition 2.12. Given two object A, B of $\mathcal{C}$, the *product* of A and B is an object P with morphisms $\pi_A : P \to A$ and $\pi_B : P \to B$, such that for any pair of morphisms $f : X \to A$ and $g : X \to B$, there exists a unique morphism $h : X \to P$ such that the following diagram commutes:

$$\begin{tikzcd}
& X \arrow[ddl, bend right, "f"'] \arrow[d, dashed, "\exists! h"] \arrow[ddr, bend left, "g"] & \\
& P \arrow[dl, "\pi_A"'] \arrow[dr, "\pi_B"] & \\
A & & B.
\end{tikzcd}$$

The product is, as with terminal and initial objects, unique up to isomorphism. Thus we usually speak of *the* product, and denote the product of A and B by $A \times B$.

Dually, we define the notion of coproduct by simply flipping all the morphisms in the definition of a product.

Definition 2.13. The *coproduct*, or *sum*, of two objects A and B is an object S with morphisms $i_A : A \to S$ and $i_B : B \to S$, such that for any pair of morphisms $f : A \to X$

and $g : B \to X$, there exists a unique morphism $h : S \to X$ such that the following diagram commutes:

$$\begin{tikzcd}
A \arrow[dr, "i_A"] \arrow[ddr, bend right, "f"'] & & B \arrow[dl, "i_B"'] \arrow[ddl, bend left, "g"] \\
& S \arrow[d, dashed, "\exists! h"'] & \\
& X &
\end{tikzcd}$$

Note that a coproduct in $\mathcal{C}$ is a product in the opposite category $\mathcal{C}^{\mathrm{op}}$, and vice versa. We say that the product is a limit and that the coproduct is a colimit. The coproduct will generally be denoted by $A + B$.

Definition 2.14. For a given pair of parallel morphisms $f, g : A \to B$, their *equaliser* is an object E together with a morphism $e : E \to A$, such that for any morphism $a : X \to A$ with $f \circ a = g \circ a$, there exists a unique morphism $h : X \to E$ such that $x = e \circ h$.

The equaliser can be thought of as the largest sub-"object" of A that makes f and g equal. This idea is made more precise in section 3. We denote the equaliser of f and g by $\mathrm{eq}(f; g)$.

Definition 2.15. The *coequaliser* of two parallel morphisms $f, g : A \to B$ is an object Q paired with a morphism $q : B \to Q$ such that for any object X with morphism $b : B \to X$ such that $b \circ f = b \circ g$, there exists a unique morphism $h : Q \to X$ with $b = h \circ q$.

Definition 2.16. Given morphisms $f : A \to C$ and $g : B \to C$, the *pullback* of f and g is an object P with morphisms $p : P \to A$ and $q : P \to B$ such that $f \circ p = g \circ q$. Furthermore, for any object X with morphisms $a : X \to A$ and $b : X \to B$ such that $f \circ a = g \circ b$ we require that there exists a unique morphism $h : X \to P$ such that $p \circ h = a$ and $q \circ h = b$. That is, we require that there exists a unique morphism h such that the diagram below commutes.

$$\begin{tikzcd}
X \arrow[dr, dashed, "\exists! h"] \arrow[drr, bend left, "b"] \arrow[ddr, bend right, "a"'] & & \\
& P \arrow[r, "q"] \arrow[d, "p"] & B \arrow[d, "g"] \\
& A \arrow[r, "f"] & C
\end{tikzcd}$$

Remark. We will often denote pulling back a morphism $g : B \to C$ along a morphism $f : A \to C$ by $f^*(B)$, with $f^*(g)$ denoting the projection from $f^*(B)$ to A.

Some useful properties of pullbacks include the following propositions, which tells us that pulling back along a composite is the same as pulling back twice.

Proposition 2.4 ([McL92, p. 45, Theorem 4.8])
Suppose the diagram below commutes, and that the right-hand square is a pullback (for j and g). Then the left-hand square is a pullback (for i and f) if and only if the outer

rectangle is a pullback (for j and gf):

$$\begin{tikzcd}
D \arrow[r, "k"] \arrow[d, "h"] & E \arrow[r, "m"] \arrow[d, "i"] & F \arrow[d, "j"] \\
A \arrow[r, "f"] & B \arrow[r, "g"] & C
\end{tikzcd}$$

Furthermore, pulling back a pullback square yields again a pullback, which is a consequence of the following proposition.

Proposition 2.5 ([McL92, p. 47, Theorem 4.10])
Suppose each of the following diagrams are pullbacks:

$$\begin{tikzcd}
E \arrow[r, "k"] \arrow[d, "h"] & D \arrow[d, "n"] \\
C \arrow[r, "m"] & B
\end{tikzcd}
\qquad
\begin{tikzcd}
F \arrow[r, "r"] \arrow[d, "q"] & C \arrow[d, "m"] \\
A \arrow[r, "f"] & B
\end{tikzcd}$$

$$\begin{tikzcd}
G \arrow[r, "t"] \arrow[d, "s"] & D \arrow[d, "n"] \\
A \arrow[r, "f"] & B
\end{tikzcd}
\qquad
\begin{tikzcd}
H \arrow[r, "x"] \arrow[d, "w"] & E \arrow[d, "z"] \\
A \arrow[r, "f"] & B
\end{tikzcd}$$

where $z = m \circ h$ (and, since the first square commutes, $z = n \circ k$). Then there are unique arrows u, v that make the following diagram commute:

$$\begin{tikzcd}
H \arrow[rr, dashed, "v"] \arrow[dr, "x"] \arrow[dd, dashed, "u"] & & G \arrow[dr, "t"] \arrow[dd, "s"] & \\
& E \arrow[rr, "k"] \arrow[dd, "h"] & & D \arrow[dd, "n"] \\
F \arrow[rr, "q"] \arrow[dr, "r"] & & A \arrow[dr, "f"] & \\
& C \arrow[rr, "m"] & & B
\end{tikzcd}$$

and every square in the diagram is a pullback. In particular, H, u, v is a pullback of s and q.

Proposition 2.6 (Streicher [Str04, p. 25, theorem 7.1])
Let $\mathcal{C}$ be a category with a terminal object 1. Then the following are equivalent

1. *$\mathcal{C}$ has all binary products and equalisers*

2. *$\mathcal{C}$ has all pullbacks.*

A category which has a terminal object, all binary products, and all equalisers, or equivalently a terminal object and all pullbacks, will be said to have all finite limits and be called *finitely complete*. Similarly, if a category has an initial object, all binary coproducts, and all coequalisers, we say it is has all finite colimits and is *finitely cocomplete*.

A useful property of adjunctions with respect to limits and colimits is that left adjoints preserve colimits and right adjoints preserve limits.

Proposition 2.7 (Streicher [Str04, p. 43, Theorem 8.4])
Let $\mathcal{C}$ and $\mathcal{D}$ be two categories, and $F \dashv G$ an adjunction. Then $F : \mathcal{C} \to \mathcal{D}$ preserves colimits and $G : \mathcal{D} \to \mathcal{C}$ preserves limits.

3 Subobjects and the subobject classifier

This section covers the notions of subobjects and the subobject classifier. Subobjects give a categorical formulation of the notion of substructures, such as subsets and subgroups, by way of specific types of morphisms. Similarly, subobject classifiers translate the notion of characteristic maps, so that each subobject corresponds to a characteristic morphism.

3.1 Subobjects

Oftentimes when we study particular mathematical structures we consider their substructures as well, such as subgroups of some group, or subsets of some set. These then come equipped with an inclusion into the set they are a subobject of, in general these are special monomorphisms. In fact, in the other direction we have that all inclusions give rise to a subobject by their image, such that this inclusion factor through an isomorphism. So when we try to consider subobjects in a general category $\mathcal{C}$, we might define a subobject simply as a monomorphism.

Definition 3.1 (Subobjects)**.** Given a category $\mathcal{C}$ and an object A of $\mathcal{C}$, a subobject u of A is simply a monomorphism $u : U \rightarrowtail A$.

It remains to see that this definition really fits with our idea of subobjects. For example, we would expect our collections of subobjects to be ordered by some form of inclusion. Looking again at sets and subsets, we see that if we have two subsets U and V of some set A such that $U \subseteq V$, then the inclusion of U into A factors through the inclusion of V. In fact, for any pair of injections f, g into A, we have $\mathrm{im}(f) \subseteq \mathrm{im}(g)$ precisely when f factors through g, since the domains of both f and g are in bijection with their respective images. This then hints at a correct definition for the ordering of subobjects.

Definition 3.2 (Ordering of subobjects)**.** Let $\mathcal{C}$ be some category and A and object of the category. If $u : U \rightarrowtail A$ and $v : V \rightarrowtail A$ are two subobjects of A, then we say $u \subseteq v$ precisely when u factors through v. That is, when there is a morphism $f : U \to V$ such that the diagram below commutes.

$$\begin{tikzcd} U \arrow[rr, "f"] \arrow[dr, tail, "u"'] & & V \arrow[dl, tail, "v"] \\ & A & \end{tikzcd}$$

A good first heuristic that this is a good definition, beyond the fact that it (essentially) corresponds to notions in categories we are familiar with, is that this relation forms a preorder.

Proposition 3.1
The $\subseteq$ relation is a preorder.

Proof. First note that for any subobject u, it is clear that $u \leq u$, since $u\,\mathrm{id}_U = u$ makes the triangle commute. Next we must show that the relation is transitive. Let u, v, w be any three subobjects of A such that $u \leq v$ and $v \leq w$. Then there are maps such that the diagram

$$\begin{tikzcd} U \arrow[r, "f"] \arrow[dr, tail, "u"'] & V \arrow[r, "g"] \arrow[d, tail, "v"] & W \arrow[dl, tail, "w"] \\ & A & \end{tikzcd}$$

commutes. Then we have that $wgf = vf = u$, so $gf : U \to W$ witnesses that $u \leq w$. $\square$

The morphisms given by the ordering relation are unique monomorphisms as well, and if two subobjects are both less than or equal to each other, that is $u \subseteq v$ and $v \subseteq u$, then they are isomorphic.

Proposition 3.2
Given subobjects $u : U \rightarrowtail A$ and $v : V \rightarrowtail A$, if $u \subseteq v$, then there exists a unique monomorphism $f : U \rightarrowtail V$ such that $u = vf$. If furthermore $v \subseteq u$, then f is an isomorphism.

Proof. Since $u \subseteq v$, there exists a morphism $f : U \to V$ such that $u = vf$. Suppose that there were another such morphism $g : U \to V$. Then $vf = u = vg$. But v is a monomorphism, so $f = g$. Since g was arbitrary, it follows that f is unique.

If furthermore $v \subseteq u$, so that there exists a unique morphism $g : V \to U$ with $v = ug$, then we have $v = ug = vfg$. But v is a monomorphism, so $fg = \mathrm{id}_V$. Similarly we can show that $gf = \mathrm{id}_U$. Hence f is an isomorphism with inverse g. $\square$

Thus we almost have antisymmetry for our objects as well, since if $u \leq v$ and $v \leq u$ we have $u \cong v$. However, note that this is not an equality. For example, in the category of sets, we can produce two equivalent subobjects which are not strictly equal; simply take the set $2 = \{\emptyset, \{\emptyset\}\}$ with subobjects $u : \{\emptyset\} \to 2; \emptyset \mapsto \emptyset$ and $v : \{\{\emptyset\}\} \to 2; \{\emptyset\} \mapsto \emptyset$. Clearly these are equivalent subobjects, since their images are the same, but the sets themselves are not the same.

We see then that our definition of subobjects is somewhat lacking. It is however quite easy to solve this issue; we simply define our subobjects not as specific monomorphisms, but as equivalence-classes of monomorphisms:

Definition 3.3 (Better subobjects)**.** A subobject U of A is an equivalence class of monomorphisms into A, given by the relation that two monomorphisms are equivalent when each factors through the other. That is, we simply quotient the collection of monomorphisms into A by the relation that $u \sim v$ if and only if $u \subseteq v$ and $v \subseteq u$ with the ordering for monomorphisms defined above.

Note that we can essentially keep the order-relation, changing it only slightly to make up for the fact that our subobjects are now equivalence-classes rather than humble monomorphisms:

Definition 3.4 (Ordering on better subobjects)**.** For subobjects U and V of A, we say that $U \subseteq V$ if there exist $u \in U$ and $v \in V$ such that u factors through v.

Remark. While this is the definition we will officially use throughout the thesis, we will generally conflate subobjects and monomorphisms, as monomorphisms are much easier to work with. This is fine in most cases as almost all constructions we use are unique up to isomorphism. However, when a construction is *not* clearly invariant under such isomorphism, we will make note of it and be more careful.

Since equivalent monomorphisms are isomorphic, we may easily recover the proof that it forms a preorder. Furthermore, since we made the definition of subobjects such that antisymmetry holds by design, we in fact have a poset of subobjects.

Proposition 3.3
For each object A of $\mathcal{C}$, and any two subobject $U \subseteq V$ of A, for any two representatives $u \in U$ and $v \in V$, we have that u factors through v. Furthermore the collection of subobjects $\mathrm{Sub}(A)$ *of A forms a partially ordered set.*

Proof. Let $u \in U$ and $v \in V$ be given. Since $U \subseteq V$, there exist $u' \in U$, $v' \in V$, and a morphism f such that $u' = v'f$. From $u \in U$ we have an isomorphism g between u' and u, and similarly h between v and v'. Thus $u = u'g = v'fg = vhfg$. So hfg is an morphism from u to v.

Thus the proof of proposition 3.1 that monomorphisms are pre-ordered carries over here. Antisymmetry holds by design, as mentioned before. Hence the subobjects are partially ordered. □

Remark. Technically, we might not have a set of subobjects, as there may be too many subobjects; they form a proper class rather than a set. When every object in a category does have a set of subobjects, we call it *well-powered* [Str04, p. 50]. In this thesis however, this distinction does not come up too much, since all examples we will have will be well-powered, and furthermore every locally small topos can be shown to be well-powered.

3.2 Membership of subobjects

When working with subsets, most concepts are defined in terms of membership. Sadly, since we are working with general categories, whose objects need not be sets, we don't have that notion as a primitive. However, we can define a similar notion, which for the category of sets essentially coincides with the notion of set theory.

For a set A, an element $x \in A$ may equivalently be framed as a function from a singleton set $1 = \{*\}$ to A, and vice versa. That is, the elements of A are in bijection with the functions from 1 to A. Since 1 is a terminal object of **Set**, we may generalise this notion to arbitrary categories a with terminal object. This gives us the definition of what we will call *global elements* of an object.

Definition 3.5 (Global elements)**.** Let $\mathcal{C}$ be a category with a terminal object. A *global element* of an object A of $\mathcal{C}$ is a morphism $1 \to A$.

However, while this definition works for categories with terminal objects, it does suffer from some deficiencies. For example, our categories may not have an equivalent of set-extensionality; we may have two very different objects whose sets of global elements are in bijection. Similarly, we may have morphisms which are equal at every global element but still distinct. For example, in the category of groups, the global elements are group homomorphisms from the trivial group. But for each group there exists only one such morphism, so all groups have isomorphic sets of global elements. Clearly there is not only one group, however; the notion of global elements is simply too strict in this case.

A better notion then for elements in a category is that of *generalised elements*.

Definition 3.6 (Generalised elements)**.** Let $\mathcal{C}$ be a category with T and A objects of it. A T-shaped generalised element of A is simply a morphism from T to A.

To say that $x : T \to A$ is a T-shaped generalised element of A, we write $x \in_T A$. Note that this is just a different framing of morphisms. Furthermore, if $\mathcal{C}$ has a terminal object 1, then global elements are simply 1-shaped generalised elements. This notion recovers several of the properties we would want. If two morphisms are equal at every generalised element, then they must be equal, since they are equal at identity as well.

With this notion at hand, we define membership of subobjects in the natural way.

Definition 3.7 (Membership of subobjects)**.** Let U be a subobject of A and x a T-shaped generalised element of A. Then we say $x \in_T U$ if x factors through any monomorphism in U.

Similarly to what we showed earlier with the ordering relation, if x factors through any monomorphism of a subobject U, then x factors through all monomorphisms of U. Furthermore, this notion of membership reinforces that our definition of subobjects is the right one, in that the following proposition holds.

Proposition 3.4
For any subobjects U, V of A, we have $U \subseteq V$ if and only if for all $x : T \to A$, if $x \in_T u$ then $x \in_T v$.

Proof. In the forward direction, suppose $U \subseteq V$ and $x \in_T U$. Then there are $u \in U$ and $v \in V$ such that $u = vf$ and $x = ug$ for some f and g, so $x = vfg$, i.e. x factors through v. Hence $x \in_T V$.

In the other direction, assume that for all $x : T \to A$, $x \in_T U$ implies $x \in_T V$. Then for some $u \in U$, we have that u factors through U by $u = u\,\mathrm{id}_U$, so $u \in_U U$, whereby $u \in_U V$. But then that is the same as $U \subseteq V$. ☐

3.3 Some properties of the collection of subobjects

Up until now, We have assumed very little of our category $\mathcal{C}$, and have despite this to some degree found a convincing notion of subobjects. However, for this definition to fully bloom, we will generally require that $\mathcal{C}$ has finite limits, in particular that it has pullbacks. That is because we then can construct a lot of the usual basic operations on subobjects that we would expect for subsets.

There is one lemma we need before we are able to continue further, however; that the pullback of a monomorphism is itself a monomorphism.

Lemma 3.5
Let X, Y, Z be objects of $\mathcal{C}$, and $f : X \to Z$, $g : Y \rightarrowtail Z$ be given, where g is a monomorphism. The pullback of g along f is also a monomorphism.

Proof. Let p, q be the projections from the pullback of f and g, such that the diagram

$$\begin{tikzcd} X \times_Z Y \arrow[r, "q"] \arrow[d, "p"'] \arrow[dr, phantom, "\lrcorner", very near start] & Y \arrow[d, tail, "g"] \\ X \arrow[r, "f"] & Z \end{tikzcd}$$

commutes. Let $r, s : W \to X \times_Z Y$ be given such that $pr = ps$. Then we have that $gqr = fpr = fps = gqs$, and since g is mono, it follows that $qr = qs$. By the universal property of pullbacks, if there is a morphism $h : W \to X \times_Z Y$ such that $fph = gqh$, then it is unique. But $fpr = gqr$ and $fps = gqs$, so we must conclude that $r = h = s$. ☐

We may prove with this lemma that when $\mathcal{C}$ has pullbacks (of monomorphisms), then the collections of subobjects have intersections; that is, we have for any pair of subobjects of the same object another subobject representing their intersection.

Proposition 3.6
Let U and V be subobjects of A in some category $\mathcal{C}$. Then the pullback of one representative of each equivalence-class is a representative of the intersection of U and V.

Proof. Since pullbacks are unique up to isomorphism, it suffices to show that the pullback of a pair of monomorphisms is the meet in the preorder of monomorphisms. This then translates to the level of subobjects.

Let $u : U \rightarrowtail A$ and $v : V \rightarrowtail A$ be any given pair of monomorphisms. Then the pullback of u and v is the meet of them. Specifically, we have for any other monomorphism $w : W \rightarrowtail A$ that $w \subseteq u \times_A v$ if and only if $w \subseteq u$ and $w \subseteq v$, which follows from the universal property of pullbacks together with the fact that the ordering of monomorphisms is a preorder. Hence $u \times_A v$ is the meet of u and v, so it is a representative of the meet of U and V. □

This subobject then also satisfies the expected property that $x \in_T U \cap V$ if and only if $x \in_T U$ and $x \in_T V$, which follows from the universal property of pullbacks.

Pullbacks give more beyond just intersections, however; they give us a notion of preimages. Namely, given a morphism $f : A \to B$, pulling back equivalent monomorphisms into B along f give again equivalent monomorphisms into A; this follows from the universal property of pullbacks. We can thus extend the notion of pullbacks of monomorphisms to pullbacks of subobjects. This extended notion is then something akin to the notion of preimages of functions in **Set**.

Proposition 3.7 (McLarty [McL92, p. 44, Theorem 4.7])
Let $f : B \to A$ and U a subobject of A be given. Then for any $x : T \to B$ we have $fx \in_T U$ if and only if $x \in_T f^*(U)$.

Proof. Let u be any representative of U. Then $fx \in_T U$ is equivalent to $fx = uy$ for some y and $x \in_T f^*(U)$ is equivalent to $x = f^*(u)x'$ for some x'. We have from the universal property of pullbacks that $x = f^*(u)x'$ if and only if $fx = uy$ for some y. The desired result immediately follows. □

Moreover, taking these preimages is functorial, though contravariant; the preimage of a subobject under an identity morphism is the same subobject, and the preimage of a subobject under a composite is the preimage of the preimage of the subobject under first the right factor, then the left. This gives us the following proposition.

Proposition 3.8
For $\mathcal{C}$ a well-powered category with pullbacks, there exists have a functor $\mathrm{Sub} : \mathcal{C}^{\mathrm{op}} \to \mathbf{Set}$ *which assigns to each object A its poset of subobjects, and each morphism $f : B \to A$ we assign the function f^* taking each subobject of A to its preimage subobject of B.*

Proof. Let $f : B \to A$ be given. We must show that pulling back f along

- identity is trivial, and
- a composite is equivalent to pulling back twice.

For the former, it suffices to show that B is the pullback of f along id_A. But for any object X with morphisms $x_1 : X \to A$ and $x_2 : X \to B$, such that $\mathrm{id}_A x_1 = f x_2$, then both factor through B with x_1, as required by pullbacks. So B is the pullback of f along id_A.

Composition follows directly from proposition 2.4. $\square$

Furthermore, we have as with sets that taking the preimage preserves the ordering of subobjects and their intersections.

Proposition 3.9
Let $f : B \to A$ be a morphism of $\mathcal{C}$. Then for any subobjects U, V of A, we have that if $U \subseteq V$, then $f^*(U) \subseteq f^*(V)$. Similarly, we have that $f^*(U \cap V) = f^*(U) \cap f^*(V)$.

Proof. It suffices to show that the pullback preserves intersections, as then we have $U \subseteq V$ if and only if $U \cap V = U$, for any subobjects U and V. If f^* preserves intersections and $U \subseteq V$, then

$$f^*(U) = f^*(U \cap V) = f^*(U) \cap f^*(V),$$

so $f^*(U) \subseteq f^*(V)$.

Thus we show that taking the preimage preserves intersections. Let u, v be any representatives of subobjects U and V respectively. Their intersection is then represented as by their pullback, so that we have the following commutative diagram, pulling back each morphism into A of the pullback square of u and v along f:

$$\begin{tikzcd}
f^*(U \cap V) \arrow[rr, tail, dashed] \arrow[dr, "\exists! g"] \arrow[dd, tail, dashed] & & f^*(V) \arrow[dr] \arrow[dd, tail] & \\
& U \cap V \arrow[rr, tail] \arrow[dd, tail] & & V \arrow[dd, tail, "v"] \\
f^*(U) \arrow[rr, tail] \arrow[dr] & & B \arrow[dr, "f"] & \\
& U \arrow[rr, tail, "u"] & & A.
\end{tikzcd}$$

By proposition 2.5 we then have that every square in the cube is a pullback. In particular, $f^*(U \cap V)$ is the pullback of $f^*(U)$ and $f^*(V)$, so it represents the intersection of them. Hence the intersection is preserved by pullbacks, and so also the ordering. $\square$

3.4 Subobject classifiers

As with reasoning about elements of sets, another useful tool in set theory is the fact that every subset of some set A is exactly represented by a function from A to the set $\{0, 1\}$ by the characteristic function. More precisely, we can represent a subset $U \subseteq A$ by a function $\chi_U : A \to \{0, 1\}$, such that $\chi_U(x) = 1$ if and only if $x \in U$. In other words, the powerset of A is in bijection with the set of functions from A to $\{0, 1\}$. Let us call the latter Ω. This property, then, can be simply phrased in terms of preimages, saying that U is the preimage of $\{1\}$ under χ_U. We can then also say that Ω *classifies* subsets.

Thus we can say that in **Set**, there exists a set Ω with an element $t \in \Omega$, such that every subset U of A is the preimage of $\{t\}$ under some (unique) function $\chi_U : A \to \Omega$. Since we have already generalised all of these notions earlier, we may simply adapt this idea as given above to any category with finite limits.

Definition 3.8 (Subobject classifier)**.** Let $\mathcal{C}$ be a category with all finite limits. A *subobject classifier* is an object Ω together with a global element $t : 1 \to \Omega$, with the property that for each object A and subobject U of A, there exists a unique morphism $\chi_u : A \to \Omega$ such that U is the preimage of t under χ_U. In other words, such that the following square is a pullback:

$$\begin{tikzcd} U \arrow[r] \arrow[d, "u"] & 1 \arrow[d, "t"] \\ A \arrow[r, "\chi_u"] & \Omega. \end{tikzcd}$$

Remark. We say that the morphism $t : 1 \to \Omega$ is the *generic subobject*, since it gives rise to all others. Since it is a morphism from the terminal object, it is also monic. This follows from the uniqueness of terminal objects.

Remark. It will be common that we compose the generic subobject with the unique terminal arrow from some object X, i.e. that we write $t!_X : X \to \Omega$. Thus we will often simply write the object subscript to t, as $t_X : X \to \Omega$ instead.

Note that we have several equivalent properties to those for sets. For example, we have $x \in_T U$ if and only if $\chi_U x = t_T$ for all generalised elements x, which follows from the universal property of pullbacks. Similarly, we have the property that the set of subobjects $\mathrm{Sub}(A)$ of A is in bijection with the set of morphisms $\mathrm{Hom}(A, \Omega)$. In fact, this bijection is natural in A, which means that (for a well-powered category), the Sub-functor is representable.

Proposition 3.10 (Streicher [Str04, p. 80, lemma 12.1])
Let $\mathcal{C}$ be a (well-powered) category with pullbacks. Then $\mathcal{C}$ has a subobject classifier if and only if $\mathrm{Sub}_{\mathcal{C}} : \mathcal{C}^{\mathrm{op}} \to \mathbf{Set}$ *is a representable presheaf.*

Proof. In the forward direction, assume $\mathcal{C}$ has a subobject classifier. Then we may define a natural isomorphism ι between $\mathrm{Sub}_{\mathcal{C}}$ and $よ(\Omega)$ by

$$\iota_A(u : U \rightarrowtail A) = \chi_u \in \mathrm{Hom}(A, \Omega),$$

with inverse $\iota_A^{-1}(\varphi) = \varphi^*(t)$. That they are inverses comes fact that by definition u is the pullback of t along χ_u, so u is isomorphic to $\chi_u^*(t)$, and similarly φ would be the characteristic morphism of $\varphi^*(t)$. Naturality then follows from observing that for any $f : A \to B$, we have that $\mathrm{Sub}(f)(u) = f^*(u)$, so the following squares commute and are pullbacks squares:

$$\begin{tikzcd} f^*(U) \arrow[r] \arrow[d, tail, "f^*(u)"] & U \arrow[r, tail, "t"] \arrow[d, tail, "u"] & 1 \arrow[d] \\ B \arrow[r, "f"] & A \arrow[r, "\chi_u"] & \Omega \end{tikzcd}$$

Hence it follows that $\chi_{f^*(u)} = \chi_u f$, that is, $\iota_B \circ \mathrm{Sub}(f) = よ(\Omega)(f) \circ \iota_A$, which is exactly naturality for ι. Hence $\mathrm{Sub} \cong よ(\Omega)$.

In the other direction, we must show that given a natural isomorphism $\iota : よ(\Omega) \to \mathrm{Sub}_{\mathcal{C}}$ for some Ω, we have that Ω is a subobject classifier. Let $t : T \rightarrowtail \Omega$ denote $\iota_\Omega(\mathrm{id}_\Omega)$. Then from naturality follows that for any $\varphi : A \to \Omega$ we have

$$\iota_A(\varphi) = \iota_A(よ(\varphi)(\mathrm{id}_\Omega)) = Sub(\varphi)(\iota_\Omega(\mathrm{id}_\omega)) = \varphi^*(t).$$

Specifically we then have for any subobject $u : U \rightarrowtail A$ that

$$u = \iota_A(\iota_A^{-1}(u)) = \chi_u^*(t),$$

where $\chi_u = \iota_A^{-1}(u)$, meaning every subobject is the pullback of $t : T \rightarrowtail \Omega$ along its characteristic morphism. Finally we must show that T is a terminal object. Note that $\mathrm{id}_A : A \rightarrowtail A$ is always a subobject, and so the following is a pullback

$$\begin{tikzcd}
A \arrow[r] \arrow[d, "\mathrm{id}_A"] & T \arrow[d, "t"] \\
A \arrow[r] & \Omega
\end{tikzcd}$$

Hence there exists a morphism $!_A$ from A to T. $\square$

Since the morphisms into the subobject classifier represent subobjects, we may transfer the order on subobjects to morphisms into the subobject classifier, as follows.

Definition 3.9 (Ordering on characteristic morphisms)**.** For any morphisms $\varphi, \psi : A \to \Omega$, we say that $\varphi \leq \psi$ when $\varphi^*(t) \subseteq \psi^*(t)$.

However, an equivalent characterisation of the ordering can be given as well, similar to proposition 3.4. This then also corresponds to the pointwise ordering of functions A to $\{0, 1\}$ for sets.

Proposition 3.11
Let $\varphi, \psi : A \to \Omega$ be given. Then $\varphi \leq \psi$ precisely when for each $x : X \to A$, $\varphi x = t_X$ implies $\psi x = t_X$.

Proof. By proposition 3.4 we have that $x \in_X \varphi^*(t)$ implies $x \in_X \psi^*(t)$ for all $x : X \to A$ precisely when $\varphi^*(t) \subseteq \psi^*(t)$, i.e. when $\varphi \leq \psi$. But from the definition of the subobject classifier and pullbacks, we have $x \in_X \varphi^*(t)$ precisely when $\varphi^*(x) = t_X$, and the same holds for ψ. $\square$

4 Cartesian closed categories

This section covers the definition of *cartesian closed categories*, as well as some of their properties. The idea of these special categories is to generalise the notion of function-sets to the more general categorical setting, having for each pair of objects A, B an object representing the set of morphisms from A to B.

More concretely, we often in **Set** consider for two sets the set of function from one to the other. This can be can be characterised as having for each pair of sets A, B a set B^A, the set of functions, together with a function $\mathrm{ev} : B^A \times A \to B$ given by $\mathrm{ev}(f, x) = f(x)$. This tells us that if we have a function and a value, we may apply the function to it.

While this gives us an idea for how we may generalise the notion of how to apply a function, it does not give us the details of how we may construct one. The most naive answer would come from noting that every function appears as a global point of the function set. Thus we have a correspondence between $\mathbf{Set}(A, B)$ and $\mathbf{Set}(1, B^A)$. However, this does not take into account the surrounding *context* we may have.

For example, when considering group actions of a group G on some set X, we may want to look at the permutation representation of it; assigning to each element $g \in G$ the action of multiplying by g, itself a function on X. In this case, the context is the element g of the group.

Really then, when we want to construct functions, taking a context C into account, we say that given a function $f : C \times A \to B$, we can construct a function $\overline{f} : C \to B^A$. This function is given by $\overline{f}(c)(x) = f(c, x)$, as would be expected.

These considerations together then lead naturally to a categorical formulation, and thus also generalisation, of the notion of function-sets.

Definition 4.1 (Cartesian Closed Categories)**.** A category $\mathcal{C}$ is *cartesian closed* if it has all finite products, and for each pair of objects $A, B \in \mathrm{Ob}(\mathcal{C})$ there exists an object B^A, called the exponential object of A and B, and a morphism $\mathrm{ev}_{A,B} : B^A \times A \to A$, the evaluation morphism, such that for any $f : X \times A \to B$ there is a unique $\overline{f} : X \to B^A$, which we will call the *transpose* of f, for which the following diagram commutes:

$$\begin{tikzcd}
X \times A \arrow[d, "\overline{f} \times A"'] \arrow[dr, "f"] & \\
B^A \times A \arrow[r, "\mathrm{ev}"'] & B.
\end{tikzcd}$$

Remark. Oftentimes the subscripts of the evaluation morphism will be clear from context, in which case we will omit them.

With our definition at hand, we now wish to show that these, at least to a certain degree, correspond with the notion of function-sets we are used to. To that end, we fix a cartesian closed category $\mathcal{C}$ for the remainder of the section.

First we wish to see some relatively basic facts. For example, composing a transposed morphism with any other morphism should correspond, in analogy with **Set**, to changing only the context, leaving the dependent variable unchanged. That is, in **Set**, if we have functions $f : C \times A \to B$ and $g : C' \to C$, then we should have

$$(\overline{f} \circ g)(c)(x) = f(g(c))(x) = \overline{f \circ (g \times A)}(c)(x).$$

This in fact holds in any cartesian closed category.

Lemma 4.1 ([Str04, p. 64, lemma 11.1])
For any $f : X \times A \to B$ and $g : Y \to X$, we have

$$\overline{f} \circ g = \overline{f \circ (g \times A)}.$$

Proof. Note that for any morphism $h : Y \times A \to B$, its transpose $\overline{h}$ uniquely determined by $\mathrm{ev}(\overline{h} \times A) = h$. Thus we have

$$\mathrm{ev}((\overline{f}\ g) \times A) = \mathrm{ev}(\overline{f} \times A)(g \times A) = f(g \times A) = \mathrm{ev}(\overline{f(g \times A)} \times A).$$

Then $\overline{f(g \times A)} = \overline{f}\ g$ by uniqueness of the transpose. $\square$

Similarly, we may look at **Set** to see that the transpose of an evaluation morphism, which is of the right form to take the transpose of, should satisfy the equation $\overline{\mathrm{ev}_{A,B}}(f)(x) = f(x)$, so $\overline{\mathrm{ev}_{A,B}}(f) = f$. Hence the transpose of evaluation should be identity.

Lemma 4.2
The transpose of $\mathrm{ev}_{A,B}$ *is the identity morphism* id_{B^A}.

Proof. Notice that the diagram

$$\begin{tikzcd}
B^A \times A \arrow[d, "\mathrm{id}_{B^A} \times A"'] \arrow[dr, "\mathrm{ev}"] & \\
B^A \times A \arrow[r, "\mathrm{ev}"'] & B
\end{tikzcd}$$

commutes, so by the definition of transposes, $\overline{\mathrm{ev}_{A,B}} = \mathrm{id}_{B^A}$. □

With these properties at hand, we can in fact show that not only does every morphism from a product give rise to a morphism into the exponential, but also the converse.

Proposition 4.3
For any morphism $f : C \to B^A$ *there exists a unique morphism* g *such that* $f = \overline{g}$.

Proof. Let $g = \mathrm{ev}(f \times A)$. Then $\overline{g} = \overline{\mathrm{ev}(f \times A)} = \overline{\mathrm{ev}}\, f$ by lemma 4.1. But $\overline{\mathrm{ev}} = \mathrm{id}_{B^A}$, so $\overline{g} = f$. For any morphism $g' : C \times A \to B$ for which $\overline{g'} = f$, we have

$$g = \mathrm{ev}\overline{g} \times A = \mathrm{ev} f \times A = \mathrm{ev}\overline{g'} \times A = g',$$

showing uniqueness. □

A simple consequence of this is then that exponentials can be probed for equality by evaluating them, in analogy to how functions may be probed for equality by checking them pointwise.

Corollary 4.4
For any pair of morphisms $f, g : C \to B^A$, *if* $\mathrm{ev}(f \times A) = \mathrm{ev}(g \times A)$, *then* $f = g$.

Proof. Since $\mathrm{ev}(f \times A) = \mathrm{ev}(g \times A)$ we have $f = \overline{\mathrm{ev}(g \times A)}$ by the previous corollary. But then $f = g$ by the uniqueness of transposes, since also $g = \overline{\mathrm{ev}(g \times A)}$. □

Looking back at the motivation for the definition of cartesian closed categories, we should expect every morphism $f : A \to B$ to correspond to a point in the exponential object B^A.

Definition 4.2 (Name of a morphism)**.** The *name* of a morphism $f : A \to B$, $\ulcorner f \urcorner$, is defined as the transpose of $f\pi_A : 1 \times A \to B$, where $\pi_A : 1 \times A \to A$ is the obvious projection.

This definition will be especially useful later for internalising logic, for which the following expected proposition also will be required.

Proposition 4.5
For any morphism $f : A \to B$ *and* $g : X \to A$, *we have* $\mathrm{ev}\langle \ulcorner f \urcorner !_X, g \rangle = fg$.

Proof. Calculation, with heavy use of the definition of transposes, yields

$$\mathrm{ev}\langle \ulcorner f \urcorner !_X, g \rangle = \mathrm{ev}\langle \overline{f\pi_A} !_X, g \rangle = \mathrm{ev}(\overline{f\pi_A} \times A)\langle !_X, g \rangle = f\pi_A\langle !_x, g \rangle = fg. \qquad \square$$

Thus we have showed at least some similarity with function-sets. Another common operation on functions we care about is composition. Since points in the exponential object are supposed to represent morphisms in some sense, we should expect that we may post-compose the morphisms to produce new points in another exponential object. In other words, we should have an equivalent to the function $g^A : B^A \to B'^A$ given by $g^A(f) = g \circ f$ for each given $g : B \to B'$, post-composing g to the result of each function. This equivalent is in fact given by a functor for each object A.

Proposition 4.6 ([Fre72, p. 3])
For any fixed $A \in \mathrm{Ob}(\mathcal{C})$, the mapping $(-)^A$ is a functor $\mathcal{C} \to \mathcal{C}$.

Proof. We first show how this functor is to act on morphisms. Given any $f : B \to B'$, take f^A to be the unique adjunct to the composite

$$B^A \times A \underset{\mathrm{ev}}{\xrightarrow{B}} \underset{f}{\xrightarrow{B'}} .$$

That is, $f^A : B^A \to B'^A$ with $f^A = \overline{f\,\mathrm{ev}}$.

Next, we show functoriality. For identity, note that $(\mathrm{id}_B)^A = \overline{\mathrm{ev}} = \mathrm{id}_{B^A}$ by lemma 4.2, as required. To show preservation of composition, first let $g : B' \to B''$ be given. Then

$$g^A f^A = \overline{g\,\mathrm{ev}}\,\overline{f\,\mathrm{ev}} = \overline{g\,\mathrm{ev}(\overline{f\,\mathrm{ev}} \times A)} = \overline{gf\,\mathrm{ev}} = (gf)^A.$$

Hence the action is functorial. □

Symmetrically, we should have an equivalent of pre-composing, taking the function $g : A' \to A$ to the function $B^g(f) = f \circ g$ for each function $f \in B^A$.

Proposition 4.7
For any fixed $B \in \mathrm{Ob}(\mathcal{C})$, the mapping $B^{(-)}$ is a functor $\mathcal{C}^{\mathrm{op}} \to \mathcal{C}$.

Proof. Let $f : A' \to A$ be given. We define B^f as the transpose of the composite

$$B^A \times A' \xrightarrow{B^A \times f} B^A \times A \xrightarrow{\mathrm{ev}} B,$$

i.e. $B^f = \overline{\mathrm{ev}(B^A \times f)}$.

Then $B^{\mathrm{id}_A} = \overline{\mathrm{ev}(B^A \times \mathrm{id}_A)} = \overline{\mathrm{ev}} = \mathrm{id}_{B^A}$, as before.

For composition, let $g : A'' \to A'$ be given. Then $B^{fg} = \overline{\mathrm{ev}(B^A \times fg)}$ and $B^g B^f = \overline{\mathrm{ev}(B^{A'} \times g)}\,\overline{\mathrm{ev}(B^A \times f)}$. Thus

$$\begin{aligned}
\mathrm{ev}((B^g B^f) \times A'') &= \mathrm{ev}(B^g \times A'')(B^f \times A'') \\
&= \mathrm{ev}(B^A \times g)(B^f \times A'') \\
&= \mathrm{ev}(B^f \times A')(B^A \times g) \\
&= (B^A \times f)(B^A \times g) \\
&= B^A \times (fg) \\
&= \mathrm{ev}(B^{fg} \times A'').
\end{aligned}$$

By corollary 4.4, we thus have $B^g B^f = B^{fg}$, i.e. $B^{(-)}$ acts contravariantly on morphisms. Hence $B^{(-)}$ is a functor from $\mathcal{C}^{\mathrm{op}}$ to $\mathcal{C}$. □

Combining these two propositions, we should even expect a bifunctor, taking each pair of objects to its exponential object, and morphisms to the composite of the two above functors.

Proposition 4.8
The mapping $(-)^{(-)}$ *taking each pair of objects* (B, A) *to* B^A *yields a functor* $C^{\mathrm{op}} \times C \to C$*.*

Proof. It suffices to show that $B'^f g^A = g^{A'} B^f$ for any $f : A' \to A$ and $g : B \to B'$, as we may then define $f^g = B^f g^A$. Functorality then follows:

$$id_A^{id_B} = B^{id_A}(id_B)^A = id_{B^A}$$

and

$$(f_1 f_2)^{(g_1 g_2)} = B^{(f_1 f_2)}(g_1 g_2)^A = B^{f_1} B^{f_2} g_1^A g_2^B = B^{f_1} g_1^A B^{f_2} g_2^B = g_1^{f_1} g_2^{f_2}.$$

So we need to show that $B'^f g^A = g^{A'} B^f$. Note that

$$\begin{aligned}
B'^f g^A &= \overline{\mathrm{ev}(B'^A \times f)}\,\overline{g\,\mathrm{ev}} \\
&= \overline{\mathrm{ev}(B'^A \times f)(\overline{g\,\mathrm{ev}} \times A')} \\
&= \overline{\mathrm{ev}(\overline{g\,\mathrm{ev}} \times A)(B^A \times f)} \\
&= \overline{g\,\mathrm{ev}(B^A \times f)} \\
&= \overline{g\,\mathrm{ev}(\overline{\mathrm{ev}(B^A \times f)} \times A')} \\
&= \overline{g\,\mathrm{ev}}\,\overline{\mathrm{ev}(B^A) \times f)} \\
&= g^{A'} B^f,
\end{aligned}$$

so we are done. ☐

Furthermore, we in fact have an adjunction with the functors $(-)^A$ and $(-) \times A$, which should not be too surprising, given that we took as motivation for the definition that we can for each morphism $f : C \times A \to B$ construct a morphism $C \to B^A$, and as shown above, vice versa.

To show this, however, we first need the following lemma, whose similarity to lemma 4.1 should be noted.

Lemma 4.9
For any $f : X \times A \to B$ *and* $g : B \to B'$*, we have* $\overline{gf} = g^A \overline{f}$*.*

Proof. The following series of equalities hold:

$$g^A \overline{f} = \overline{g\,\mathrm{ev}}\,\overline{f} = \overline{g\,\mathrm{ev}(\overline{f} \times A)} = \overline{gf}$$

☐

Finally, we have the expected proposition.

Proposition 4.10
For each $A \in \mathrm{Ob}(\mathcal{C})$*, the functor* $(-) \times A$ *is left adjoint to the functor* $(-)^A$*.*

Proof. We need to show that $\mathcal{C}(B \times A, C) \cong \mathcal{C}(B, C^A)$ naturally in B, C. First note that for any $f \in \mathcal{C}(B \times A, C)$ its transpose is in $\mathcal{C}(B, C^A)$, and vice versa by corollary 4.3, and that these uniquely determine each other. Thus, we have a bijection between the sets. All that remains then is to prove naturality in B, C. Let $f : B' \to B$ and $g : C \to C'$ be given. Then we need to show that the square

$$\begin{tikzcd}
\mathcal{C}(B \times A, C) \arrow[r, "\overline{(-)}"] \arrow[d, "\mathcal{C}(f \times A, g)"'] & \mathcal{C}(B, C^A) \arrow[d, "\mathcal{C}(f, g^A)"] \\
\mathcal{C}(B' \times A, C') \arrow[r, "\overline{(-)}"] & \mathcal{C}(B', A^{C'})
\end{tikzcd}$$

commutes, i.e. that for any $a \in \mathcal{C}(B \times A, C)$, we have $\overline{ga(f \times A)} = g^A \overline{a} f$. But this holds by lemma 4.1 and the previous lemma. $\square$

We have a similar adjunction for the other functor, $C^{(-)} : \mathcal{C}^{\text{op}} \to \mathcal{C}$. However, in this case the functor is adjoint to itself.

Proposition 4.11
For fixed C, The functor $C^{(-)} : \mathcal{C}^{\text{op}} \to \mathcal{C}$ is its own left (and thus also right) adjoint.

Proof. We have the following composition of natural isomorphisms:

$$\mathcal{C}^{\text{op}}(C^B, A) \cong \mathcal{C}(A, C^B) \cong \mathcal{C}(A \times B, C) \cong \mathcal{C}(B \times A, C) \cong \mathcal{C}(B, C^A). \square$$

With both of these adjunctions at hand, we can prove several preservation properties of both functors, which also then motivate the name of "exponential", since it behaves much like exponents in arithmetic would. Similarly products behave much like products of natural numbers with respect to both sums and exponentials.

Corollary 4.12
For any $A, B, C \in \mathcal{C}$, the following hold:

- $A^1 \cong A$
- $(A \times B)^C \cong A^C \times B^C$
- $(A^B)^C \cong A^{B \times C}$,

and assuming $\mathcal{C}$ has coproducts and initial object

- $0 \times A \cong 0$
- $(A + B) \times C \cong A \times C + B \times C$
- $A^{B+C} \cong A^B \times A^C$.

Proof. These all follow from proposition 2.7, proposition 4.10, and proposition 4.11. $\square$

5 Elementary topoi

The previous two sections both generalised different aspects of the category of sets, first the notion of subsets and characteristic maps, and then the notion of the set of functions between two sets. But this then begs the question; if we have a subobject classifier and exponentials, can we not have *objects* representing the collection of subobjects, rather than just a set? That is, can we *internalise* the idea of subobjects, with ordering, intersections, and all?

The goal of this section is to show that it is, in fact, possible to do just that. We begin by defining *elementary topoi*, which are precisely cartesian closed categories with all finite limits and a subobject classifier. Then we show how in this setting, we may relate the properties we wish to show to mere equality of certain morphisms. The goal of the next section is then to show how we may make use of these internalised notions to make reasoning about subobjects purely by way of only morphisms possible, and so make possible to wholly reason internally.

We begin by collecting the concepts we introduced earlier under one name [Tie11].

Definition 5.1 (Elementary Topoi)**.** A category $\mathcal{E}$ is an *elementary topos* if it

- has all finite limits,
- is cartesian closed, and
- has a subobject classifier.

The most obvious example of such a category is the category **Set** of sets and functions, which we used as a motivating example for both the notion of subobject classifiers and exponential objects. Thus there is no surprise that this category is in fact also an elementary topos. Another example, which we show later in section 8, is that the category of finite sets is also an elementary topos, although it obviously lacks certain features that the category of all sets has.

For the remainder of this section, we fix an elementary topos $\mathcal{E}$. The plan now is to somehow "internalise" the logic of truth-values, viewing the subobject classifier as the object of such, and relating this to the algebra of subobjects we gave in section 3; much in the same way that the set of truth-values in **Set** also describes the algebra of subsets.

We first show that conjunction of truth-values has an internal analogue, and how it corresponds to intersections of subobjects.

Proposition 5.1
Any elementary topos $\mathcal{E}$ has a morphism $\wedge : \Omega \times \Omega \to \Omega$ such that for two subobjects U, V of $A \in \mathrm{Ob}(\mathcal{E})$, the meet $U \cap V$ is precisely classified by $\wedge\langle \chi_U, \chi_V \rangle$.

Proof. Take $\wedge : \Omega \times \Omega \to \Omega$ be the classifier for $\langle t, t\rangle : 1 \to \Omega \times \Omega$, i.e. take $\wedge$ such that

$$\begin{tikzcd}
1 \arrow[r] \arrow[d, tail, "\langle t,t\rangle"'] & 1 \arrow[d, "t"] \\
\Omega \times \Omega \arrow[r, "\wedge"] & \Omega
\end{tikzcd}$$

is a pullback square.

Now we must show that for any subobjects U, V of A, the intersection $U \cap V$ is classified by $\wedge\langle \chi_U, \chi_V\rangle$. Remember that $U \cap V$ is characterised by the fact that for any generalised element $x : T \to A$, we have $x \in_T U \cap V$ if and only if $x \in_T U$ and $x \in_T V$, and that $x \in_T W$ if and only if $\chi_W x = t_T$ for any subobject W.

Thus if $\wedge\langle \chi_U, \chi_V\rangle x = t_T$ if and only if $\chi_U x = t_T$ and $\chi_V x = t_T$, then $\wedge\langle \chi_U, \chi_V\rangle$ must be the characteristic morphism of $U \cap V$, as such morphisms are unique. But by the universal property of pullbacks, we have $\wedge\langle \chi_U, \chi_V\rangle x = t_T$ if and only if $\langle \chi_U, \chi_V\rangle x = \langle t, t\rangle !_T$, i.e. when $\chi_U x = t_T$ and $\chi_V x = t_T$.

Since $x : T \to A$ was chosen arbitrarily, it must follow that $\wedge\langle \chi_U, \chi_V\rangle = \chi_{U\cap V}$. $\square$

Remark. Since $\wedge\langle \varphi, \psi\rangle$ is often cumbersome to write, we will generally write $\wedge$ infix instead. So we write $\varphi \wedge \psi$ to mean $\wedge\langle \varphi, \psi\rangle$.

One way to view proposition 5.1 is as saying that Ω has an internal operation for conjunctions, and that the intersection subobjects, viewed as morphisms into Ω, can be viewed as taking the conjunction pointwise. Note that in the category of sets, this analogy is precise; the intersection of subsets is precisely the pointwise meet of truth-values when the subsets are viewed as functions.

With conjunctions internalised we move on to the next target, internalising equality. We start by looking at the usual constructions with sets, and generalise from there. Given a set A, a relation on A should be a subset $R \subseteq A \times A$, and the equality relation should be exactly the subset $R = \{(a, a) \mid a \in A\}$. In other words, R is the image of the diagonal map $\delta_A(a) = (a, a)$. Then R is classified by the function $\mathrm{eq}_A : A \times A \to \Omega$ which gives t on the diagonal, and false otherwise.

Note now that we already have categorical formulations of all of the required concepts to state this categorically. The equality relation E_A can be seen as a subobject of $A \times A$ given by the diagonal. Furthermore, the diagonal morphism $\delta_A = \langle \mathrm{id}_A, \mathrm{id}_A \rangle : A \to A \times A$ is a monomorphism, so this relation can be represented precisely by the map δ_A. Finally then, the morphism $\mathrm{eq}_A : A \times A \to \Omega$ which checks if two values are equal should then be the characteristic morphism of δ_A.

Proposition 5.2
For each object A of $\mathcal{E}$, there is a morphism $\mathrm{eq}_A : A \times A \to \Omega$ such that for any two generalised elements $a, b : X \to A$, we have $a = b$ if and only if $\mathrm{eq}_A\langle a, b\rangle = t_X$.

Proof. Take eq_A to be the classifying morphism of $\delta_A : A \rightarrowtail A \times A$, the diagonal at A. We show that this morphism satisfies the expected property. Let $a, b : X \to A$ be some arbitrary morphisms. We want to show that $a = b$ if and only if $\mathrm{eq}_A\langle a, b\rangle = t_X$. The forward direction is trivial, so we examine the other. Suppose $\mathrm{eq}_A\langle a, b\rangle = t_X$. Then $\langle a, b\rangle : X \to A \times A$ factors uniquely through $\delta_A : A \rightarrowtail A \times A$, since eq_A classifies δ_A, so $\langle a, b\rangle = \delta_A c$ for some $c : X \to A$, i.e. $\langle a, b\rangle = \langle c, c\rangle$. But then $a = c$ and $b = c$, i.e. $a = b$. □

Furthermore, we in fact have that the subobject classified by $\mathrm{eq}_B\langle f, g\rangle$ is precisely the equaliser of arbitrary parallel morphisms $f, g : A \to B$, which is analogous to how in **Set** the equaliser is exactly the set $\mathrm{eq}(f; g) = \{a \in A \mid f(a) = g(a)\}$, or equivalently, the preimage of the diagonal subset of $B \times B$ under $\langle f, g\rangle$.

Corollary 5.3
Given any pair of morphisms $f, g : A \to B$, the subobject classified by $\mathrm{eq}_B\langle f, g\rangle$ is exactly the equaliser of f and g.

Proof. Let E denote the subobject classified by $\mathrm{eq}_B\langle f, g\rangle$. Thus the diagram below commutes:

$$\begin{tikzcd}
E \arrow[r] \arrow[d, tail, "e"] & B \arrow[r] \arrow[d, tail, "\delta_B"] & 1 \arrow[d, tail, "t"] \\
A \arrow[r, "\langle f,g\rangle"] & B \times B \arrow[r, "\mathrm{eq}_B"] & \Omega
\end{tikzcd}$$

Since the outer and right squares are both pullbacks, it follows that the left square is also a pullback. From proposition 2.6 then follows that $E \xrightarrow{e} A$ is the equaliser of f and g. □

Now that we have internal forms of both conjunction and equality, we can may mirror the ordering as well by making use of the equivalence $u \leq v \iff u \wedge v = u$. In other words, we construct a morphism $\Rightarrow : \Omega \times \Omega \to \Omega$ such that $\varphi \Rightarrow \psi$ corresponds to the truth-value of the statement that ψ follows from φ. If this is true, then we should also have that $\varphi \leq \psi$. Then we extend this pointwise to hold over characteristic morphisms for some object A, and so for general subobjects of A.

Proposition 5.4
There exists an morphism $\Rightarrow : \Omega \times \Omega \to \Omega$ such that for any subobjects U, V of A, it holds that $U \subseteq V$ if and only if $\Rightarrow \langle \chi_U, \chi_V\rangle = t_A$.

Proof. Note that $U \subseteq V$ precisely when $U \cap V = U$, i.e. when $\chi_U \wedge \chi_V = \chi_U$. The latter is then equivalent to $\mathrm{eq}_A\langle \chi_u \wedge \chi_v, \chi_u\rangle = t_A$ by proposition 5.2. Further rewriting then yields

$\mathrm{eq}_\Omega(\wedge \times \pi_1)\langle \chi_U, \chi_V \rangle = t_A$, where $\mathrm{eq}_\Omega(\wedge \times \pi_1)$ is independent of A, U, and V. Taking $\Rightarrow = \mathrm{eq}_\Omega(\wedge \times \pi_1)$ then gives the desired result for the characteristic morphisms of U and V. Since A, U and V were all independent of $\Rightarrow$ and arbitrary, we note that the statement holds for any choice of those values, from which the desired conclusion follows. □

Remark. As with the internalised conjunctions, we write internal implication infix. That is, we write $\Rightarrow \langle \varphi, \psi \rangle$ infix as $\varphi \Rightarrow \psi$. We will also write $U \Rightarrow V$ for the subobject classified by $\chi_U \Rightarrow \chi_V$, for any subobjects U, V of A some object.

It will be helpful to give a characterisation of membership of the implicate $U \Rightarrow V$ of subobjects U and V of A, both to give an intuition for how it behaves, and to soon prove that the implicate acts as an exponential object in the poset of subobjects.

Corollary 5.5
Given subobjects U, V of A, we have for any generalised element $x : T \to A$ that $x \in_T U \Rightarrow V$ if and only if $x \in_T U$ implies $x \in_T V$.

Proof. This follows from the fact that $U \subseteq V$ if and only if $x \in_T U$ implies $x \in_T V$ (proposition 3.4), as well as the fact that $U \Rightarrow V$ is characterised by $\chi_U \Rightarrow \chi_V$.

We have the following chain of equivalences:

$$\begin{array}{ll} x \in_T U \Rightarrow V & \text{iff} \\ (\chi_U \Rightarrow \chi_V)x = t_T & \text{iff} \\ \mathrm{eq}_\Omega\langle \chi_U \wedge \chi_V, \chi_U \rangle x = t_T & \text{iff} \\ (\chi_U \wedge \chi_V)x = \chi_U x & \text{iff} \\ x \in_T U \cap V \text{ exactly when } x \in_T U & \end{array}$$

So if $x \in_T U \Rightarrow V$ and $x \in_T U$, then $x \in_T U \cap V$, and so also $x \in_T V$. In other words, if $x \in_T U \Rightarrow V$, then $x \in_T U$ implies $x \in_T V$.

In the other direction, suppose $x \in_T U$ implies $x \in_T V$. Then we have from that from intersections that $x \in_T U \cap V$ if and only if $x \in_T U$ and $x \in_T V$. From the assumption we then have $x \in_T U \cap V$ if and only if $x \in_T U$, whence $x \in_T U \Rightarrow V$. □

With this corollary at hand, we can easily show that implicates are right adjoint to conjunctions, in the sense of cartesian closedness.

Proposition 5.6
For all U, V, W subobjects of $A \in \mathrm{Ob}(\mathcal{E})$, we have $U \subseteq V \Rightarrow W$ if and only if $U \cap V \subseteq W$.

Proof. Note that $U \subseteq V \Rightarrow W$ if and only if for all $x : T \to A$, it holds that if $x \in_T U$, then $x \in_T V \Rightarrow W$. But from the last corollary, $x \in_T V \Rightarrow W$ exactly if $x \in_V$ implies $x \in_T W$.

Plainly, $x \in_T U$ implies $x \in_T V$ implies $x \in_T W$. But this is equivalent to having that $x \in_T U$ and $x \in_T V$ implies $x \in_T W$. From the membership-characterisation of intersections we then equivalently have $x \in_T U \cap V$ implies $x \in_T W$ for all $x : T \to A$. Thus $U \cap V \subseteq W$ if and only if $U \subseteq V \Rightarrow W$. □

Up until now, we've only considered the propositional parts of the algebra of subobjects, and also ignored the cartesian closed structure of the topos. However, with the exponential objects, we really unlock a very powerful language. Namely, the existence of the subobject classifier Ω tells us that subobjects of an object A are equivalently morphisms from A to Ω. Add to this the fact that exponential objects represent sets morphisms, we then have that the object Ω^A should represent the collection of subobjects of A; the *power object* of A, in analogy with power sets.

Then we may at least try to construct a morphism $\forall_A : \Omega^A \to \Omega$, which would give true when the input subobject is the maximal subobject. Alternatively, viewing subobjects as formulas, which is commonly done with sets, the morphism $\forall_A$ would tell us if the formula is true everywhere, functioning as a universal quantifier in a sense.

Definition 5.2 (Universal quantifier)**.** Let A be any object of $\mathcal{E}$. The *universal quantifier* $\forall_A : \Omega^A \to A$ at A is the classifier of the morphism $\ulcorner t_A \urcorner$, where $t_A : A \to \Omega$ denotes the characteristic morphism of the maximal subobject.

Alternatively, in the vein of internalising quantification, we could look at relations $R \subseteq B \times A$ of B and A. Universally quantifying over A in this relation should give a subobject S of B such that for every $U \subseteq B$, we have $U \subseteq S$ precisely when $U \times A \subseteq R$; essentially, it is the subobject S of B such that whatever we pair an element of S with, we have a subobject of R.

Definition 5.3 (Universal quantification of relations [McL92, p. 121])**.** Given a relation $R \subseteq B \times A$, we define the *universal quantification* of R over A, written $\forall a.R$, as the pullback of the subobject represented by $\ulcorner t_A \urcorner : 1 \rightarrowtail \Omega^A$ along the transpose of $\chi_R : B \times A \to \Omega$:

$$\begin{tikzcd}
\forall a.R \arrow[r] \arrow[d, tail] \arrow[dr, phantom, "\lrcorner", very near start] & 1 \arrow[d, tail, "\ulcorner t_A \urcorner"] \\
B \arrow[r, "\overline{\chi_R}"] & \Omega^A
\end{tikzcd}$$

Note that since $\forall a.R$ is defined by pulling back along $\overline{\chi_R}$, its classifying morphism is given by the composite $\forall_A \overline{\chi_R}$, where $\forall_A : \Omega^A \to \Omega$ is the universal quantifier for A as defined above.

The desired property for the universal quantification of relations, as motivated above, follows immediately.

Proposition 5.7 ([McL92, thm. 13.8])
Let $S \subseteq B$ and $R \subseteq B \times A$ be any given subobjects. Then $S \subseteq \forall a.R$ if and only if $S \times A \subseteq R$.

Proof. Let s be a representative of S, overloading S to also mean the domain of s, and similarly for some $r \in R$. Then $S \subseteq \forall a.R$ holds by definition exactly when $\overline{\chi_R} s = \ulcorner t_A \urcorner !_S$. Transposing both sides then yields $\chi_R(s \times A) = t_{S \times A}$, hence $s \times A \subseteq r$, i.e. $S \times A \subseteq R$. $\square$

Finally, just as we have characterised membership of implicates, it will prove useful to give a similar result for the universal quantifier.

Proposition 5.8 ([McL92, p. 122, Theorem 13.9])
Let $R \subseteq B \times A$ be some relation. Then for any generalised element $x : T \to B$, we have $x \in_T \forall a.R$ if and only if $x \times A \in_{T \times A} R$.

Proof. Let $r \in R$ be some representative, again writing R also for the domain of r.

In the forward direction, suppose $x \in_X \forall a.R$. Then there is a morphism $x' : X \to \forall a.R$ such that the diagram

$$\begin{tikzcd}
X \arrow[r, "x'"] \arrow[dr, bend right, "x"'] & \forall a.R \arrow[r] \arrow[d, tail, "\forall a.r"'] & 1 \arrow[d, "\ulcorner t \urcorner_A"] \\
& B \arrow[r, "\overline{\chi_R}"'] & \Omega^A
\end{tikzcd}$$

commutes, where the right square is a pullback. Hence $\overline{\chi_R}x = \ulcorner t_A \urcorner$. But $\overline{\chi_R}x = \overline{\chi_R(x \times A)} = \ulcorner t_A \urcorner !_X$, so transposing both sides we have $\chi_R(x \times A) = t_{X \times A}$. Hence $x \times A \in_{X \times A} R$.

In the other direction, we have a morphism $x : X \to B$ such that $x \times A \in_{X \times A} R$. Then $\chi_R(x \times A) = t_{X \times A}$, so transposing both sides we have $\overline{\chi_R}x = \overline{\chi_R(x \times A)} = \ulcorner t_A \urcorner !_X$. Thus there exists by the definition of pullbacks a morphism $x' : X \to \forall a.R$ such that $x = (\forall a.R)x'$, so $x \in_X \forall a.R$. □

6 Internal language

This section introduces the internal language of a topos. The broad idea of the internal language is to, in a sense, replicate the reasoning on elements we use in set theory. The solution for allowing such reasoning we gave in section 3 was through *generalised elements*, and while the concept is useful, we can take it further. Furthermore, it is not enough to simply provide a method construct generalised elements; we also want to find a structured method for reason about subobjects through these elements. That is what the internal language provides.

We begin this section with constructing a language of terms and types, together with a way of interpreting these syntactic objects as generalised elements and objects respectively. Then we make use of the fact that generalised elements of the subobject classifier, as simply morphisms into it, correspond to subobjects of their domain. Hence we can use this fact to reason about subobjects simply as terms with the subobject classifier as type. With this fact in mind, we construct a system for proofs about formulas in the style of natural deduction. We prove that this system is sound, in the sense that any valid proof of a statement implies that the statement holds internally. Finally we use this proof system, together with some axioms which we prove hold in the internal logic of all internal topoi, to show several properties about the topoi themselves. For example, we show that every morphism factors as a monomorphism composed with an epimorphism, and that any monic epimorphism is an isomorphism.

For the whole section, we fix an elementary topos $\mathcal{E}$.

6.1 The term-language

The idea of the term language is to allow easy construction of generalised elements of objects. One perspective on such elements would be as terms in a context: the morphism itself is the term, the domain gives the context, and the codomain the type. We think of the context as containing all variables our term may make use of, so the context should be seen as a list of variables with their types, which can be interpreted as a product of objects of the topos.

Remark. In the presentation of the internal language we use the language and notation of *type theory*. Geuvers [Geu09] provides a good introduction for those uninitiated.

Since we interpret the types of our language simply as objects of $\mathcal{E}$, we need only concern ourselves with contexts and terms. We will generate these inductively, to make reasoning about the terms easier.

Terms will always be given inside a context. Before any other terms are given, we will require a countable supply of variables. Then we define contexts, as the name suggests, as simply a list of distinct variables with an some type assigned, we write this as $x : A$. A context Γ is thus of the form $x_1 : A_1, \ldots, x_n \; : \; A_n$.

A well-typed term t of type A in a context Γ will be written as $\Gamma \vdash t : A$. The remaining terms, beyond just variables, are then given by the following inference rules:

$$\frac{(x : A \in \Gamma)}{\Gamma \vdash x : A} \qquad \frac{}{\Gamma \vdash * : 1}$$

$$\frac{\Gamma \vdash a : A \qquad \Gamma \vdash b : B}{\langle a, b \rangle : A \times B} \qquad \frac{\Gamma \vdash t : A \times B}{\Gamma \vdash \mathrm{fst}(t) : A} \qquad \frac{\Gamma \vdash t : A \times B}{\Gamma \vdash \mathrm{snd}(t) : B}$$

$$\frac{\Gamma, x : A \vdash b : B}{\Gamma \vdash \lambda x : A.\, b : A \to B} \qquad \frac{\Gamma \vdash t : A \to B \qquad \Gamma \vdash u : A}{\Gamma \vdash t\, u : B}$$

$$\frac{(A, B \in \mathrm{Ob}(\mathcal{E})) \qquad (f \in \mathcal{E}(A, B))}{\Gamma \vdash f : A \to B} \qquad \frac{(A \in \mathrm{Ob}(\mathcal{E})) \qquad (c \in \mathcal{E}(1, a))}{\Gamma \vdash c : A,}$$

where we use certain suggestive notation for some types; exponentials are written with arrows, so $A \to B$, and products are written as usual.

Remark. This presentation is really a simply typed λ-calculus. More about this presentation, with a focus on interpretation into general cartesian closed categories is given in [Str04].

When types are clear from context, we will omit them. Next we show how to interpret the types, contexts, and terms inside the topos $\mathcal{E}$. We define interpretation of each by structural recursion, starting with interpreting contexts as simply the product of each variables type: $[\![x_1 : A_1, \ldots, x_n : A_n]\!] = \prod_{i=1,\ldots n} [\![A_i]\!]$.

Terms are then interpreted as follows:

$$\begin{array}{lcll}
[\![\Gamma \vdash x : A]\!] & = & \pi_i & \text{(where } i \text{ is the index of } x : A \text{ in } \Gamma) \\
[\![\Gamma \vdash * : 1]\!] & = & !_{[\![\Gamma]\!]} & \\
[\![\Gamma \vdash c : A]\!] & = & c\, !_{[\![\Gamma]\!]} & (A \in \mathrm{Ob}(\mathcal{E}) \text{ and } c \in \mathcal{E}(1, A)) \\
[\![\Gamma \vdash f : A \to B]\!] & = & \ulcorner f \urcorner\, !_{[\![\Gamma]\!]} & (A, B \in \mathrm{Ob}(\mathcal{E}) \text{ and } f \in \mathcal{E}(A, B)) \\
[\![\Gamma \vdash \langle a, b \rangle : A \times B]\!] & = & \langle [\![\Gamma \vdash a]\!], [\![\Gamma \vdash b]\!] \rangle & \\
[\![\Gamma \vdash \mathrm{fst}(t) : A]\!] & = & \pi_1 [\![\Gamma \vdash t : A \times B]\!] & \\
[\![\Gamma \vdash \mathrm{snd}(t) : B]\!] & = & \pi_2 [\![\Gamma \vdash t : A \times B]\!] & \\
[\![\Gamma \vdash \lambda x : A.\, t : A \to B]\!] & = & \overline{[\![\Gamma, x : A \vdash t : B]\!]} & \\
[\![\Gamma \vdash t\, u : B]\!] & = & \mathrm{ev} \langle [\![\Gamma \vdash t : A \to B]\!], [\![\Gamma \vdash u : A]\!] \rangle &
\end{array}$$

We also have some equational rules that we would expect to hold. For example, we would expect a pair equal the pair of each projection; that is, $\langle \mathrm{fst}(p), \mathrm{snd}(p) \rangle = p$. Similarly, we would expect $\mathrm{fst}\langle a, b \rangle = a$ and $\mathrm{snd}\langle a, b \rangle = b$. We would also expect the only term of 1 to be $*$, since 1 is terminal and plays the role of the singleton set. Simple calculation shows that these rules are consistent with the interpretation; from the axioms of cartesian closed categories, these equations hold in the interpretation. Hence it would not be weird to include these rules.

Furthermore, since exponentials play the role of function-objects, we'd expect similar rules for these; The λ-terms are to be interpreted as constructing a function with a variable, and application is meant to replace a variable with the applied to term. Thus we would want $(\lambda x : A.\ t)\, u = t[u/x]$, where the right-hand side is the term t with every (free) occurrence of x replaced by u. For this to make sense, we require a notion of substitutions to begin with.

Definition 6.1. Given a pair of contexts Γ, Δ, as *substitution* from Γ to Δ is map from the variables $x : A$ of Δ to terms $\Gamma \vdash t : A$.

We may apply a substitution $\sigma : \Gamma \to \Delta$ to a term $\Delta \vdash t : A$, written $t[\sigma]$, to produce a term of the same type in context Γ. The method of substitution is capture-avoiding substitution, similar to how Streicher [Str04] handles the situation.

With substitutions at hand, we may state all the equations we expect the terms of our calculus to obey. We write $\Gamma \vdash t \equiv u : A$ when t and u both have type A in context Γ, and they are supposed to be equivalent.

$$\frac{\Gamma \vdash t : A \qquad \Gamma \vdash u : B}{\Gamma \vdash \mathrm{fst}\langle t, u\rangle \equiv t : A} \qquad \frac{\Gamma \vdash t : A \qquad \Gamma \vdash u : B}{\Gamma \vdash \mathrm{snd}\langle t, u\rangle \equiv u : B} \qquad \frac{\Gamma \vdash t : A \times B}{\Gamma \vdash t \equiv \langle \mathrm{fst}(t), \mathrm{snd}(t)\rangle : A \times B}$$

$$\frac{\Gamma, x : A \vdash t : B \qquad \Gamma \vdash u : A}{\Gamma \vdash (\lambda x : A.\, t)\, u \equiv t[u/x]} \qquad \frac{\Gamma \vdash t : A \to B}{\Gamma \vdash (\lambda x : A.\, t\, x) \equiv t : A \to B} \qquad \frac{\Gamma \vdash t : 1}{\Gamma \vdash t \equiv * : 1}$$

$$\frac{\Gamma \vdash t \equiv u : A \qquad \Gamma \vdash s \equiv t : A}{\Gamma \vdash s \equiv u : A} \qquad \frac{\Gamma \vdash t : A}{\Gamma \vdash t \equiv t : A} \qquad \frac{\Gamma \vdash t \equiv u : A}{\Gamma \vdash u \equiv t : A}$$

$$\frac{\Gamma \vdash t \equiv t' : A \qquad \Gamma \vdash u \equiv u' : B}{\Gamma \vdash \langle t, u\rangle \equiv \langle t', u'\rangle : A \times B} \qquad \frac{\Gamma \vdash t \equiv t' : A \times B}{\Gamma \vdash \mathrm{fst}(t) \equiv \mathrm{fst}(t') : A \times B}$$

$$\frac{\Gamma \vdash t \equiv t' : A \times B}{\Gamma \vdash \mathrm{snd}(t) \equiv \mathrm{snd}(t') : A \times B} \qquad \frac{\Gamma, x : A \vdash t \equiv t' : A}{\Gamma \vdash (\lambda x : A.\, t) \equiv (\lambda x : A.\, t') : A \to B}$$

$$\frac{\Gamma \vdash t \equiv t' : A \to B \qquad \Gamma \vdash u \equiv u' : A}{\Gamma \vdash t\, u \equiv t'\, u' : B}$$

The proposition we then expect is that, if $\Gamma \vdash t \equiv u : A$, then $[\![\Gamma \vdash t]\!] = [\![\Gamma \vdash u]\!]$. The proof of this is simply by structural induction on the equation-rules and the relevant properties of cartesian closedness of the elementary topos. However, one small problem with proving that these rules hold comes from the interpretation of terms with substitutions. To show that substitutions behave well under interpretation, we require a few more things.

First of all, we require a way to interpret substitutions inside the topos. But this is really quite simple; since a substitution is a list of terms, all in the same context, we may simply interpret them as a product of the interpretation of each term; the interpretation of a substitution $\sigma : \Gamma \to \Delta$ is just the morphism

$$\langle [\![\Gamma \vdash \sigma(x_i) : A_i]\!] \mid x_i : A_i \in \Delta\rangle : [\![\Gamma]\!] \to [\![\Delta]\!].$$

Furthermore, we should expect substitutions to behave nicely with interpretation of terms. Specifically, since substitutions are interpreted as morphisms between contexts, we want to say that applying a substitution to a term, and then interpreting the result, is really the same as composing the interpretations of each:

Lemma 6.1 (Substitution Lemma [Str04, Lemma 11.2])
Whenever $\Gamma \vdash t : A$ and $\sigma : \Delta \to \Gamma$ is a substitution, then

$$[\![\Delta \vdash t[\sigma] : A]\!] = [\![\Gamma \vdash t : A]\!] \circ [\![\sigma]\!].$$

Proof. A proof for an analogous result is given by Streicher [Str04], and the same proof applies here. $\square$

With the substitution lemma at hand, we may prove that the equation-rules on terms given above turn into equality in the interpretation.

Proposition 6.2
Suppose Γ is a context and $\Gamma \vdash t \equiv u : A$ for some terms t and u, both of type A in context Γ. Then $[\![\Gamma \vdash t : A]\!] = [\![\Gamma \vdash u : A]\!]$.

Proof. Proceed by induction on the equivalence rules. Most rules follow either immediately from the induction hypothesis or the fact that equality is an equivalence relation. The only cases which require further scrutiny are the specific rules regarding products, exponentials, and the terminal object. But these cases all follow from the universal properties of the respective kind of object. □

Further expectations on the interpretation of terms is with regards to applying a function-constant to some term. Specifically, we would expect that this is simply pre-composing the morphism with the interpretation of the argument.

Lemma 6.3
For any function constant $f \in \mathcal{E}(A, B)$ and term $\Gamma \vdash t : A$, we have

$$[\![\Gamma \vdash ft : B]\!] = f[\![\Gamma \vdash t : A]\!].$$

Proof. By definition of the interpretation of terms and proposition 4.5 we have

$$[\![\Gamma \vdash ft : B]\!] = \mathrm{ev}\langle \ulcorner f \urcorner !_{[\![\Gamma]\!]}, [\![\Gamma \vdash t : A]\!]\rangle = f[\![\Gamma \vdash t : A]\!].$$ □

6.2 A proof system for the internal language

Since the term-language is interpreted as morphisms in $\mathcal{E}$, we may reason about sub-objects of (the interpretation of) a context by simply looking at terms of type Ω in that context. These terms may also be viewed as formulas in the context, which is partially motivated from section 5, where we obtained terms corresponding to the logical connectives of conjunction and implication. By similar reasoning we also have a notion of universal quantification, by way of the morphism $\forall_A : \Omega^A \to \Omega$.

Remark. As we did for the connectives $\wedge$ and $\to$, we will make use of certain additional syntactic sugar for universal quantifiers: $\forall x : A.\ \varphi$ rather than $\forall_A(\lambda x : A.\ \varphi)$.

Thus, we may make these ideas more formal; we may construct a system for reasoning with these connectives in a syntax similar to that of natural deduction. We will write $\Gamma \mid \Phi \vdash \varphi$ (borrowing the notation from Streicher [Str04]) to mean that there is a deduction, as will be given shortly, with assumptions in a list of formulas Φ concluding a formula φ, all with free variables in the context Γ. A list of formulas $\Phi = \varphi_1, \ldots, \varphi_n$ will be called a *propositional* context, distinguishing from the *variable* context Γ.

Structural rules

Before we get to the logical rules, we of course need certain structural rules.

$$\frac{(\Gamma \vdash \varphi : \Omega)}{\Gamma \mid \Phi, \varphi \vdash \varphi}\ \textsc{Ax} \qquad \frac{\Gamma \mid \Phi \vdash \varphi}{\Gamma \mid \Phi, \psi \vdash \varphi}\ \textsc{Weak} \qquad \frac{\Gamma \mid \Phi, \varphi, \varphi \vdash \psi}{\Gamma \mid \Phi, \psi \vdash \psi}\ \textsc{Contr}$$

$$\frac{\Gamma \mid \Phi_1, \varphi, \psi, \Phi_2 \vdash \rho}{\Gamma \mid \Phi_1, \psi, \varphi, \Phi_2 \vdash \rho}\ \textsc{Exch} \qquad \frac{\Gamma \mid \Phi \vdash \varphi \qquad (\sigma : \Gamma' \to \Gamma)}{\Gamma' \mid \Phi[\sigma] \vdash \varphi[\sigma]}\ \textsc{Subst}$$

$$\frac{\Gamma \mid \Phi, \psi \vdash \varphi \qquad \Gamma \mid \Phi \vdash \psi}{\Gamma \mid \Phi \vdash \varphi}\ \textsc{Cut}$$

where $\sigma : \Gamma' \to \Gamma$ is a substitution and Φ, φ are lists of formulas and formulas in context Γ.

Remark. Weakening of the variable context can be achieved with the substitution rule; in the one-variable case, for example, simply let $\sigma = (\Gamma, y : A)$, with Γ the original context. Then the substitution rule simply adjoins a single variable $y : A$ to each of the formulas; it weakens them.

Logical rules

$$\frac{}{\Gamma \mid \Phi \vdash \top}\ \top \qquad \frac{\Gamma \mid \Phi \vdash \varphi \qquad \Gamma \mid \Phi \vdash \psi}{\Gamma \mid \Phi \vdash \varphi \wedge \psi}\ \wedge \qquad \frac{\Gamma \mid \Phi, \varphi \vdash \psi}{\Gamma \mid \Phi \vdash \varphi \to \psi}\ \to$$

$$\frac{\Gamma, y : A \mid \Phi \vdash \varphi}{\Gamma \mid \Phi \vdash \forall y : A.\ \varphi}\ \forall$$

where $y : A$ does not appear in Γ nor free in Φ.

We will also make use of several *derived* rules; certain rules, which while not part of the collection of actual rules, may be derived from them. These are useful when reasoning within the language, but do not add any difficulties when it comes to reasoning about the system itself.

Theorem 6.4
For any variable context Γ*, al context* Φ*, and formulas* φ, ψ*, the rules*

$$\frac{\Gamma \mid \Phi \vdash \varphi \to \psi \qquad \Gamma \mid \Phi \vdash \varphi}{\Gamma \mid \Phi \vdash \psi}\ \mathit{MP} \qquad \frac{\Gamma \mid \Phi \vdash \varphi}{\Gamma \mid \Phi, \varphi \to \psi \vdash \psi}\ {\to}\mathit{INST}$$

$$\frac{\Gamma \mid \Phi, \varphi[t/y] \vdash \psi}{\Gamma \mid \Phi, \forall y : A.\ \varphi \vdash \psi}\ \forall\mathit{INST}$$

are derivable.

Proof. Taking Φ, φ, and ψ to be in context Γ, the first rule holds:

$$\frac{\dfrac{\Gamma \mid \Phi \vdash \varphi \to \psi}{\Gamma \mid \Phi, \varphi \vdash \psi}\ \to \qquad \Gamma \mid \Phi \vdash \varphi}{\Gamma \mid \Phi \vdash \psi}\ \text{Cut}$$

The second rule can be given the following derivation tree:

$$\dfrac{\dfrac{}{\Gamma \mid \Phi, \varphi \to \psi \vdash \varphi \to \psi}\ \text{Ax} \qquad \dfrac{\Gamma \mid \Phi \vdash \varphi}{\Gamma \mid \Phi, \varphi \to \psi \vdash \varphi}\ \text{Weak}}{\Gamma \mid \Phi, \varphi \to \psi \vdash \psi}\ {\to}\text{E}$$

With Φ and ψ in context Γ,φ in context $\Gamma, y : A$, and $\Gamma \vdash t : A$, we may derive the third rule by

$$\dfrac{\dfrac{\Gamma \mid \Phi, \varphi[t/y] \vdash \psi}{\Gamma \mid \Phi, \forall y : A.\ \varphi, \varphi[t/y] \vdash \psi}\ \text{Weak} \qquad \dfrac{\dfrac{\dfrac{}{\Gamma \mid \Phi, \forall y : A.\ \varphi \vdash \forall y : A.\ \varphi}\ \text{Ax}}{\Gamma, y : A \mid \Phi, \forall y : A.\ \varphi \vdash \varphi}\ \forall\text{E}}{\Gamma \mid \Phi, \forall y : A.\ \varphi \vdash \varphi[t/y]}\ \text{Subst } t/y}{\Gamma \mid \Phi, \forall y : A.\ \varphi \vdash \psi}\ \text{Cut}$$

□

Note that we don't have rules, or even symbols, for falsehood, disjunction, nor existential quantifiers. That is because we can encode the connectives and derive associated rules by clever use of universal quantifiers [Str04].

We are in fact able to derive formulas for each of falsehood, disjunction, and existential quantification by reasoning about their expected elimination rules.

- We expect falsehood $\bot$ to be a term of type Ω such that the rule

  $$\dfrac{\Gamma \vdash \varphi : \Omega}{\Gamma \mid \Phi, \bot \vdash \varphi}$$

  holds for any context Γ, and formulas Φ and φ. If we define $\bot = \forall \varphi : \Omega.\ \varphi$, we may derive the expected rule:

  $$\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma \mid \Phi, (\forall \varphi : \Omega.\ \varphi) \vdash \forall x : \Omega.\ x}\ \text{Ax}}{\Gamma, x : \Omega \mid \Phi, (\forall \varphi : \Omega.\ \varphi) \vdash x}\ \forall}{\Gamma \mid \Phi, (\forall \varphi : \Omega.\ \varphi) \vdash \varphi}\ \textsc{Subst}}{\Gamma \mid \Phi, \bot \vdash \varphi}$$

- For two formulas $\varphi : \Omega$ and $\psi : \Omega$, define $\varphi \vee \psi$ by

  $$\varphi \vee \psi := \forall \rho : \Omega.\ (\varphi \Rightarrow \rho) \wedge (\psi \Rightarrow \rho) \Rightarrow \rho$$

  with ρ not free in φ nor ψ.

  Then we can derive the characteristic rules

  $$\dfrac{\Gamma \mid \Phi \vdash \varphi \vee \psi \qquad \Gamma \mid \Phi, \varphi \vdash \rho \qquad \Gamma \mid \Phi, \psi \vdash \rho}{\Gamma \mid \Phi \vdash \rho}$$

  $$\dfrac{\Gamma \mid \Phi \vdash \varphi}{\Gamma \mid \Phi \vdash \varphi \vee \psi} \qquad\qquad \dfrac{\Gamma \mid \Phi \vdash \psi}{\Gamma \mid \Phi \vdash \varphi \vee \psi}$$

First we give a derivation for the first rule, assuming the top row and proving the bottom one:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Gamma \mid \Phi \vdash \varphi \vee \psi}{\Gamma \mid \Phi \vdash \forall x : \Omega.\ (\varphi \Rightarrow x) \wedge (\psi \Rightarrow x) \Rightarrow x}}{\Gamma, x : \Omega \mid \Phi \vdash (\varphi \Rightarrow x) \wedge (\psi \Rightarrow x) \Rightarrow x}\,\forall\mathrm{I}}{\Gamma \mid \Phi \vdash (\varphi \Rightarrow \rho) \wedge (\psi \Rightarrow \rho) \Rightarrow \rho}\,\mathrm{Subst}}{\Gamma \mid \Phi, (\varphi \Rightarrow \rho) \wedge (\psi \Rightarrow \rho) \vdash \rho}\,{\to}\mathrm{E} \qquad \dfrac{\dfrac{\dfrac{\Gamma \mid \Phi, \varphi \vdash \varphi \Rightarrow \rho}{\Gamma \mid \Phi \vdash \varphi \Rightarrow \rho}\,{\to}\mathrm{I}}{\Gamma \mid \Phi \vdash \varphi \Rightarrow \rho}\,\mathrm{Weak} \quad \dfrac{\dfrac{\Gamma \mid \Phi, \psi \vdash \psi \Rightarrow \rho}{\Gamma \mid \Phi \vdash \psi \Rightarrow \rho}\,{\to}\mathrm{I}}{\Gamma \mid \Phi \vdash \psi \Rightarrow \rho}\,\mathrm{Weak}}{\Gamma \mid \Phi \vdash (\varphi \Rightarrow \rho) \wedge (\psi \Rightarrow \rho)}\,\wedge\mathrm{I}}{\Gamma \mid \Phi \vdash \rho}\,\mathrm{Cut}$$

Next we construct a derivation for $\Gamma \mid \Phi \vdash \varphi \vee \psi$ assuming that we have a derivation $\Gamma \mid \Phi \vdash \varphi$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma, x : \Omega \mid \Phi, (\varphi \Rightarrow x) \wedge (\psi \Rightarrow x) \vdash (\varphi \Rightarrow x) \wedge (\psi \Rightarrow x)}\,\mathrm{Ax}}{\Gamma, x : \Omega \mid \Phi, (\varphi \Rightarrow x) \wedge (\psi \Rightarrow x) \vdash \varphi \Rightarrow x}\,\wedge\mathrm{E}}{\Gamma, x : \Omega \mid \Phi, (\varphi \Rightarrow x) \wedge (\psi \Rightarrow x), \varphi \vdash x}\,{\Rightarrow}\mathrm{E} \qquad \dfrac{\Gamma, x : \Omega \mid \Phi \vdash \varphi}{\Gamma, x : \Omega \mid \Phi, (\varphi \Rightarrow x) \wedge (\psi \Rightarrow x) \vdash \varphi}\,\mathrm{Weak}}{\Gamma, x : \Omega \mid \Phi, (\varphi \Rightarrow x) \wedge (\psi \Rightarrow x) \vdash x}\,\mathrm{Cut}}{\Gamma, x : \Omega \mid \Phi \vdash (\varphi \Rightarrow x) \wedge (\psi \Rightarrow x) \Rightarrow x}\,{\Rightarrow}\mathrm{I}}{\Gamma \mid \Phi \vdash \varphi \vee \psi}\,\forall\mathrm{I}$$

The derivation of $\Gamma \mid \Phi \vdash \varphi \vee \psi$ from $\Gamma \mid \Phi \vdash \psi$ is the same with φ replaced by ψ in several places.

- Similarly we may define $\exists x : A.\ \varphi := \forall \rho : \Omega.\ (\forall x : A.\ \varphi \Rightarrow \rho) \Rightarrow \rho$ with ρ not free in φ, and the corresponding bidirectional rule

$$\begin{array}{c} \Gamma, y : A \mid \Phi, \varphi \vdash \psi \\ \hline\hline \Gamma \mid \Phi, \exists y : A.\ \varphi \vdash \psi \end{array}$$

holds for this definition [Str04, p. 94].

For the forward direction, with the assumption of a derivation for $\Gamma, y : A \mid \Phi, \varphi \vdash \psi$, we use the derivation tree

$$\dfrac{\dfrac{\dfrac{\dfrac{\Gamma, y : A \mid \Phi, \varphi \vdash \psi}{\Gamma, y : A \mid \Phi \vdash \varphi \to \psi}\,{\to}}{\Gamma \mid \Phi \vdash \forall y : A.\ \varphi \to \psi}\,\forall}{\Gamma \mid \Phi, (\forall y : A.\ \varphi \to \psi) \to \psi \vdash \psi}\,{\to}\mathrm{inst}}{\Gamma \mid \Phi, \exists y : A.\ \varphi \vdash \psi}\,\forall\mathrm{inst}$$

In the other direction, we will need the following derivation of $\Gamma, y : A \mid \Phi, \varphi \vdash \exists y : A.\ \varphi$:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma, y : A, \rho : \Omega \mid \Phi, \varphi \vdash \varphi}\,\mathrm{Ax}}{\Gamma, y : A, \rho : \Omega \mid \Phi, \varphi, \varphi \to \rho \vdash \rho}\,{\to}\mathrm{inst}}{\Gamma, y : A, \rho : \Omega \mid \Phi, \varphi \vdash (\forall y : A.\ \varphi \to \rho) \to \rho}\,{\to}}{\Gamma, y : A \mid \Phi, \varphi \vdash \exists y : A.\ \varphi}\,\forall$$

which we then use in the backward direction

$$\dfrac{\dfrac{\dfrac{\Gamma \mid \Phi, \exists y : A.\, \varphi \vdash \psi}{\Gamma, y : A \mid \Phi, \exists y : A.\, \varphi \vdash \psi}\,\text{Subst}}{\Gamma, y : A \mid \Phi, \varphi, \exists y : A.\, \varphi \vdash \psi}\,\text{Weak} \qquad \Gamma, y : A \mid \Phi, \varphi \vdash \exists y : A.\, \varphi}{\Gamma, y : A \mid \Phi, \varphi \vdash \psi}\,\text{Cut}$$

6.3 Soundness of the proof system

A useful property, in fact, an essential property, of proof systems is their *soundness*. This property states that any proof in the system is in fact true. Traditionally, this says that whenever we have a derivation tree $\Gamma \mid \Phi \vdash \varphi$, then the formula φ is true whenever the formulas Φ are also true. In our case, however, we have no predefined notion of truth; we will need to begin with defining that, before we are able to continue.

Definition 6.2 (Truth of a formula)**.** Let $\Gamma \vdash \varphi : \Omega$ be some formula in context Γ. We say φ is *true* when for any generalised element $x : T \to [\![\Gamma]\!]$, we have $[\![\Gamma \vdash \varphi]\!]x = t_T$.

Equivalently, we could present this by viewing φ as cutting out a subobject of $[\![\Gamma]\!]$. Then φ is true whenever it cuts out the maximal subobject. For this, however, we require a more precise meaning of "cutting out" a subobject of $[\![\Gamma]\!]$.

Definition 6.3 (Extensions)**.** For a given context Γ and a formula $\Gamma \vdash \varphi : \Omega$, the *extension* of φ, written $[\Gamma \mid \varphi]$, is the subobject of $[\![\Gamma]\!]$ classified by $[\![\Gamma \vdash \varphi]\!]$.

Remark. For a list of formulas Φ with formulas in context Γ, we write $[\Gamma \mid \Phi]$ for $\bigcap_{\varphi \in \Phi} [\Gamma \mid \varphi]$.

With this definition, we have that a formula $\Gamma \vdash \varphi : \Omega$ is true whenever $[\Gamma \mid \varphi]$ is the maximal subobject, by the definition of the subobject classifier.

Now that we have an idea of what it means for a formula to be true, we can move on to show that the proof system we devised in the previous subsection is sound with respect to this definition.

Definition 6.4 (Soundness of a rule)**.** We say that a deduction rule

$$\frac{\Gamma_1 \mid \Phi_1 \vdash \varphi_1 \qquad \cdots \qquad \Gamma_n \mid \Phi_n \vdash \psi_n}{\Gamma_{n+1} \mid \Phi_{n+1} \vdash \varphi_{n+1}}$$

is *sound*, if, whenever $[\Gamma_i \mid \Phi_i] \subseteq [\Gamma_i \mid \varphi_i]$ for all $1 \leq i \leq n$, it also holds that $[\Gamma_{n+1} \mid \Phi_{n+1}] \subseteq [\Gamma_{n+1} \mid \varphi_{n+1}]$.

Remark. An equivalent formulation of soundness goes as follows: A rule as above is sound, if, whenever $[\![\Gamma_i \vdash \Phi_i]\!] \leq [\![\Gamma_i \vdash \varphi_i]\!]$ for all $1 \leq i \leq n$, it follows that $[\![\Gamma_{n+1} \vdash \Phi_{n+1}]\!] \leq [\![\Gamma_{n+1} \vdash \varphi_{n+1}]\!]$.

The remainder of the section will show that all the structural and logical rules we defined are sound. Furthermore, it is easy to see that a derived rule is sound if all rules used to derive it are sound themselves. Thus all our derived rules will be sound, too.

We start with the structural rules.

Lemma 6.5
The structural rules are sound.

Proof. That the structural rules are sound follows immediately from the definition of binary meets:

- from commutativity follows that the exchange rule is sound,
- from idempotence follows that the contraction rule is sound, and
- from monotonicity, i.e. that if for any u, v, w subobjects of $[\![\Gamma]\!]$ with $u \leq v$ we have $u \cap w \leq v \cap w$, follows that weakening is sound.

This leaves the rules for cut and substitution.

For cut, we use that for any subobjects u, v, w, if $u \cap v \subseteq w$ and $u \subseteq v$, then $u \subseteq w$, since $u = u \cap v$. Thus if $[\Gamma \mid \Phi] \subseteq [\Gamma \mid \Psi]$ and $[\Gamma \mid \Phi, \psi] \subseteq [\Gamma \mid \varphi]$, then

$$[\Gamma \mid \Phi] = [\Gamma \mid \Phi] \cap [\Gamma \mid \psi] = [\Gamma \mid \Phi, \psi] \subseteq [\Gamma \mid \varphi],$$

so the cut rule is sound.

Finally, for substitution, we assume $\sigma : \Delta \to \Gamma$ is a substitution, and that $[\Gamma \mid \Phi] \subseteq [\Gamma \mid \varphi]$. Thus we need to show that $[\Delta \mid \Phi[\sigma]] \subseteq [\Delta \mid \varphi[\sigma]]$. But by the substitution-lemma and the fact that the subobject classifier represents the functor Sub, this is equivalent to showing that

$$[\![\sigma]\!]^*[\Gamma \mid \Phi] \subseteq [\![\sigma]\!]^*[\Gamma \mid \varphi].$$

But pullbacks preserve the ordering and $[\Gamma \mid \Phi] \subseteq [\Gamma \mid \varphi]$, so we may conclude the desired result. Hence the substitution rule is sound. □

Next we show that the logical rules are sound.

Lemma 6.6
The logical rules are sound.

Proof. We show that each rule is sound.

- For the rule for truth, we have that $[\Gamma \mid \top]$ is classified by $t_{[\![\Gamma]\!]}$, and so is the maximum element of the poset. Hence for any Φ, $[\Gamma \mid \Phi] \leq [\Gamma \mid \top]$.
- For conjunction, note that $[\Gamma \mid \varphi \wedge \psi] = [\Gamma \mid \varphi] \wedge [\Gamma \mid \varphi]$ by proposition 4.5, and $[\Gamma \mid \Phi] \leq [\Gamma \mid \varphi] \wedge [\Gamma \mid \psi]$ if and only if $[\Gamma \mid \Phi]$ is less than both. Hence the conjunction rule holds in both directions.
- Implication is right adjoint to conjunction, so $[\Gamma \mid \Phi, \varphi] \leq [\Gamma \mid \psi]$ if and only if $[\Gamma \mid \Phi] \leq [\Gamma \mid \varphi] \Rightarrow [\Gamma \mid \psi] = [\Gamma \mid \varphi \Rightarrow \psi]$, so the implication rule holds.
- Let Γ be a context, $y : A$ a variable of type A, Φ a list of formulas in context Γ, and φ a formula in context $\Gamma, y : A$.

  Then there is a substitution $\pi_\Gamma : \Gamma, y : A \to \Gamma$ which simply forgets $y : A$. Since y does not appear in Φ, we have that $\Phi[\pi_\Gamma] = \Phi$. Hence

  $$[\Gamma, y : A \mid \Phi] = [\Gamma, y \mid \Phi[\pi_\Gamma]] = [\![\pi_\Gamma]\!]^*[\Gamma \mid \Phi] = \pi^*_{[\![\Gamma]\!]}[\Gamma \mid \Phi].$$

  From proposition 5.7 pulling back along the projection is left adjoint to universal quantification inside $\mathcal{E}$ as defined in section 5. Thus

  $$[\Gamma, y : A \mid \Phi] = \pi^*_\Gamma[\Gamma \mid \Phi] \leq [\Gamma, y : A \mid \varphi]$$

if and only if

$$[\Gamma \mid \Phi] \leq \forall a.\ [\Gamma, y : A \mid \varphi].$$

Thus we need only show that $[\Gamma \mid \forall y : A.\ \varphi] = \forall a.\ [\Gamma, y : A \mid \varphi]$. Remember that $\forall a.\ u$ is precisely the subobject classified by $\forall_A \overline{\chi_u}$, so it suffices to show that $[\![\Gamma \vdash \forall y : A.\ \varphi]\!] = \forall_A \overline{[\![\Gamma, y : A \vdash \varphi]\!]}$. But this follows from lemma 6.3 and the definition of the interpretation.

Hence it must be the case that the rules for universal quantification are sound, so we are done. □

With these lemmas, we may prove the soundness theorem we expect.

Theorem 6.7
The proof-system presented is sound, in the sense that for any context Γ*, and propositional context* Φ *and formula* φ *in the context* Γ *such that* $\Gamma \mid \Phi \vdash \varphi$*, then* $[\Gamma \mid \Phi] \subseteq [\Gamma \mid \varphi]$*.*

Proof. The proof is by induction on deductions, using the soundness lemmas above. □

Since we derived the rules for falsity, disjunction, and existential quantification from sound rules, they must also be sound. We may use the soundness of these formulas to show that the posets of subobjects actually form lattices, and that the finite joins are preserved under pullbacks.

Theorem 6.8 ([Str04, p. 94, theorem 13.5])
For all elementary topoi $\mathcal{E}$

1. *the posets* $\mathrm{Sub}_{\mathcal{E}}(A)$ *contain least elements* $\perp_A$ *that are preserved by* f^* *for arbitrary* $f : B \to A$ *in* $\mathcal{E}$*.*

2. *the posets* $\mathrm{Sub}_{\mathcal{E}}(A)$ *contain joins that are preserved by* f^* *for arbitrary* $f : B \to A$ *in* $\mathcal{E}$*.*

3. *for all subobjects* $R \subseteq C \times A$ *there exists a subobject* $\exists a.\ R \subseteq C$ *such that for all subobjects* $P \subseteq C$ *it holds that*

$$\exists a.\ R \subseteq P \qquad \textit{iff} \qquad R \subseteq \pi_C^*(M),$$

where $\pi_A : C \times A \to C$ *is the first projection and, moreover, for all morphisms* $f : D \to C$ *in* $\mathcal{E}$ *it holds that* $f^*(\exists a.\ R) = \exists a.\ (f \times \mathrm{id}_A)^*(R)$*.*

Proof. The proof is the same as given by Streicher [Str04, p. 94] with minor notational differences. □

Beyond the structural and logical rules, we also wish to reason about equations in our language. Since we proved in section 5 that topoi have for each object an arrow which classifies equality, we would want to simply use that. We will write $t =_A s$ for the term $\mathrm{eq}_A\langle t, s\rangle$, omitting the type when obvious from context. To prove that the expected rules for equality are sound, however; we require the following lemma.

Lemma 6.9
For any morphisms $f, g : A \to B$ *and* $\varphi : A \to \Omega^B$ *we have* $\mathrm{eq}\langle f, g\rangle \wedge \mathrm{ev}\langle \varphi, f\rangle \leq \mathrm{ev}\langle \varphi, g\rangle$*.*

Proof. Let f, g, and φ be given. Then $\mathrm{eq}\langle f, g\rangle \wedge \mathrm{ev}\langle \varphi, f\rangle \leq \mathrm{ev}\langle \varphi, g\rangle$ if and only if for all $x : I \to A$, if $(\mathrm{eq}\langle f, g\rangle \wedge \mathrm{ev}\langle \varphi, f\rangle)x = t_I$ then $\mathrm{ev}\langle \varphi, g\rangle x = t_I$ by proposition 3.4. Let such an x be given with $(\mathrm{eq}\langle f, g\rangle \wedge \mathrm{ev}\langle \varphi, f\rangle)x = t_I$. Then $\mathrm{eq}\langle fx, gx\rangle = t_I$ and $\mathrm{ev}\langle \varphi x, fx\rangle = t_I$, so by proposition 5.2 we have $fx = gx$. But then $\mathrm{ev}\langle \varphi x, fx\rangle = \mathrm{ev}\langle \varphi x, gx\rangle$, so $\mathrm{ev}\langle \varphi x, gx\rangle = t_I$. $\square$

Proposition 6.10 (Soundness of equality)
For any object $A \in \mathrm{Ob}(\mathcal{E})$, the additional rules for equality

$$\frac{\Gamma \vdash t : A}{\Gamma \mid \Phi \vdash t = t}$$

$$\frac{\Gamma \vdash s : A \qquad \Gamma \vdash t : A \qquad \Gamma \vdash \varphi : A \to \Omega \qquad \Gamma \mid \Phi \vdash s = t \qquad \Gamma \mid \Phi \vdash \varphi\ s}{\Gamma \mid \Phi \vdash \varphi\ t}$$

are sound.

Proof. For the first rule, note that $[\Gamma \mid t = t]$ is classified by $[\![\Gamma \vdash t = t]\!]$, which by lemma 6.3 is the same as $\mathrm{eq}_A\langle [\![\Gamma \vdash t]\!], [\![\Gamma \vdash t]\!]\rangle$, which by definition of eq_A is $t_{[\![\Gamma]\!]}$. Hence $[\Gamma \mid \Phi] \leq [\Gamma \mid t = t] = [\Gamma \mid \top]$.

For the second rule, suppose $\Gamma \mid \Phi \vdash s = t$ and $\Gamma \mid \Phi \vdash \varphi s$. Then by assumption $[\Gamma \mid \Phi] \leq [\Gamma \mid s = t]$ and $[\Gamma \mid \Phi] \leq [\Gamma \mid \varphi s]$, so $[\Gamma \mid \Phi] \leq [\Gamma \mid s = t] \wedge [\Gamma \mid \varphi s]$. But

$$[\![\Gamma \vdash s = t]\!] = \mathrm{eq}_A\langle [\![\Gamma \vdash s]\!], [\![\Gamma \vdash t]\!]\rangle \text{ and } [\![\Gamma \vdash \varphi\ s]\!] = \mathrm{ev}\langle [\![\Gamma \vdash \varphi]\!], [\![\Gamma \vdash s]\!]\rangle,$$

so by lemma 6.9, $[\![\Gamma \vdash s = t]\!] \wedge [\![\Gamma \vdash \varphi\ s]\!] \leq [\![\Gamma \vdash \varphi\ t]\!]$. By transitivity we then conclude $[\Gamma \mid \Phi] \leq [\Gamma \mid \varphi\ t]$. Hence both rules for equality are sound. $\square$

6.4 Using the internal language

To show the power of the internal language, we will prove certain properties about the topos $\mathcal{E}$ using it. For example, we may construct the image of a morphism $f : A \to B$ as a subobject of B.

Proposition 6.11
For any objects A, B of $\mathcal{E}$, all morphisms $f : A \to B$ factor as an epimorphism e followed by a monomorphism m. This subobject given by the monomorphism m will be the image *of f.*

Proof. Let A, B and $f : A \to B$ be given. Then take I to be the subobject given by $\exists a.\ \langle f, \mathrm{id}_A\rangle$, where $\langle f, \mathrm{id}_A\rangle$ is a subobject of $B \times A$. From theorem 6.8 then follows that there exists a morphism from $A \to I$, since $\langle f, \mathrm{id}_A\rangle \subseteq \pi_B^*(\exists a.\ \langle f, \mathrm{id}_A\rangle)$ follows from the fact that $\exists a.\ \langle f, \mathrm{id}_A\rangle \subseteq u$ if and only if $\langle f, \mathrm{id}_A\rangle \subseteq \pi_B^* u$ for any u a subobject of B. Thus at least f factors through we have a morphism $e : A \to I$. Furthermore, if $u : U \rightarrowtail B$ is any subobject of B such that f factor through u, i.e. $f = ue'$ for some $e' : A \to U$, then $\pi_2\langle f, \mathrm{id}_A\rangle = f = ue'$, so f factors through $\pi_B^* u$ by the universal property of pullbacks. But then $\langle f, \mathrm{id}_A\rangle \subseteq \pi_B^* u$, so it follows that $I = \exists a.\ \langle f, \mathrm{id}_A\rangle \subseteq u$. Hence I is the least subobject such that f factor through it.

Next we show that e is epic, for which we first show that if $e = mg$ some monomorphism $m : X \rightarrowtail I$, then it follows that $im : M \rightarrowtail B$ is a subobject of B and $f = ie = img$, so f factors through im. From above then follows that $i \subseteq im$, so there is a morphism

$h : I \to M$ such that $imh = i$. But i is a monomorphism, so $mh = \mathrm{id}_B$, in which case m is an isomorphism.

Finally, let $g, h : I \to X$ be given such that $ge = he$. Let $U \rightarrowtail [u]I$ denote the equaliser of g and h. Since $ge = he$ it holds that e factors through u, so $e = ua$ for some $a : A \to U$. But u is monic, so by the previous paragraph follows that u is an isomorphism, and thus also epic. Since $gu = hu$ and u is epic, it follows that $g = h$. Since g, h were arbitrary, it holds that e is epic. □

Corollary 6.12
The image of a morphism $f : A \to B$ is characterised by the extension $[y : B \mid \exists x : A.\ y = fx]$, and f is an epimorphism precisely when f is surjective internally, i.e. when $[y : B \mid \exists x : A.\ y = fx] = \top_B$.

Proof. For the first part, we show that $\langle f, \mathrm{id}_A\rangle$ is (isomorphic to) the subobject classified by $[\![y : B, x : A \vdash y = fx]\!]$, since $[\![y : B \vdash \exists x : A.\ y = fx]\!]$ is precisely $\exists a.\ [\![y : B, x : A \vdash y = fx]\!]$. Note that

$$[\![y : B, x : A \vdash y = fx]\!] = \mathrm{eq}_B\langle \pi_B, f\pi_A\rangle : B \times A \to \Omega,$$

so by corollary 5.3 we have that $[y : B, x : A \mid y = fx]$ is the equaliser of π_1 and $f\pi_2$. Since equalisers are unique up to isomorphism, it suffices to show that $\langle f, \mathrm{id}_A\rangle$ is also an equaliser of $\pi_1, f\pi_2$. Clearly $\langle f, \mathrm{id}_A\rangle : A \to B \times A$ satisfies $\pi_1\langle f, \mathrm{id}_A\rangle = f\pi_2\langle f, id_A\rangle$. Furthermore, given $g : X \to B \times A$ such that $\pi_1 g = f\pi_2 g$, we that g factors through $\langle f, \mathrm{id}_A\rangle$ by $\pi_2 g : X \to A$. Finally, if $h : X \to A$ such that $g = \langle f, \mathrm{id}_A\rangle h$, then $g = \langle fh, h\rangle = \langle f\pi_2 g, \pi_2 g\rangle$, so $h = \pi_g$. Thus $\langle f, \mathrm{id}_A\rangle$ is also an equaliser of π_1 and $f\pi_2$.

For the second part, notice that $[y : B \mid \exists x : A.\ y = fx] = \top_B$ if and only if any representative monomorphism in $[y : B \mid \exists x : A.\ y = fx]$ is an isomorphsim. But then the f factors as the composition of two epimorphisms, so f is also epic. Similarly, if f is epic, then

$$[\![y : B \vdash \exists x : A.\ y = fx]\!]\, f = [\![x' : A \vdash \exists x : A.\ fx' = fx]\!] = t_A = t_B\, f$$

by lemmas 6.1 and 6.3, as well as viewing f as the substitution fx' from $y : B$ to $x' : A$ (This is similar to what is shown by Borceux [Bor94, p. 95]). But then $[\![y : B \vdash \exists x : A.\ y = fx]\!] = t_B$ since f is epic, so $[y : B \mid \exists x : A.\ y = fx]$ is the maximal subobject of B. □

Corollary 6.13 (Streicher [Str04, p. 95])
For every epimorphism $e : A \to B$, it holds that if $e = mh$ for some monomorphism m, then m is an isomorphism. In particular, if e is also monic, then e is an isomorphism.

Proof. Let e be given. We then have by validity of substitution that

$$[\![y : B \vdash \exists x : A.\ z = e(x)]\!] \circ e = [\![x' : A \vdash \exists x : A.\ e(x') = e(x)]\!] = t_A = t_B \circ e,$$

and since e is epic, $[\![y : B \vdash \exists x : A.\ z = e(x)]\!] = t_B$. Hence the image of e is all of B, so $\mathrm{id}_B\, e$ is an image factorisation of e. But we showed earlier that for the epimorphism into the image, the desired property holds. Since e is said morphism, e must also have said property.

If furthermore e is monic, then $e = e\,\mathrm{id}_A$, so e is an isomorphism. □

Similar to f being epic if and only if it is internally surjective, we have that f is monic precisely when it is internally injective.

Proposition 6.14
Let $f : A \to B$ by any morphism in $\mathcal{E}$. Then f is monic if and only if f is internally injective, that is, $x : A, x' : A \mid fx = fx' \vdash x = x'$.

Proof. Note that $x : A, x' : A \mid fx = fx' \vdash x = x'$ is equivalent to $\mathrm{eq}\langle fx, fx'\rangle = t_X$ implying $\mathrm{eq}\langle x, x'\rangle$ for all $x, x' : X \to A$ by proposition 3.11, and $\mathrm{eq}\langle fx, fx'\rangle = t_A$ if and only if $fx = fx'$ by proposition 5.2. Similarly $\mathrm{eq}\langle x, x'\rangle = t_A$ precisely when $x = x'$. Thus we have a chain of equivalences which give the desired result. □

Thus if f is internally both injective and surjective, then f is an isomorphism.

Furthermore, any elementary topos satisfies some additional properties. First, we have function extensionality, which says that if two functions are equal at all points, then they are equal. That is, we have that for any two morphisms $f, g : A \to B$, the formula $(\forall x : A.\ fx = gx) \to f = g$ holds in all contexts. Similarly, the axiom of propositional extensionality, which says that if two propositions are equivalent, then they are equal, also holds. Finally we verify the axiom of unique choice, which states that any total functional relation is the graph of some morphism, i.e. that if $r : R \rightarrowtail A \times B$, classified by $\rho : A \times B \to \Omega$, satisfies the formula $\forall x : A.\ \exists! y : B.\ \rho(x, y)$, then there exists a morphism $f : A \to B$ such that $r \cong \langle id_A, f\rangle$. We define $\exists! y : B.\ \varphi(y)$ as $\exists y : B.\ \varphi(y) \wedge \forall y' : B.\ (\varphi(y) \wedge \varphi(y') \to y = y')$.

Proposition 6.15
The following hold in all elementary topoi:

1. *The axiom of function extensionality,*
2. *the axiom of propositional extensionality,*
3. *the axiom of unique choice.*

Proof. We prove each in order.

1. We show that for any $f, g : C \to B^A$, we have that if for every $c : X \to C$ we have that $c \in_C \forall a.\mathrm{eq}(\mathrm{ev}(f \times A); \mathrm{ev}(g \times A))$, then $c \in_C \mathrm{eq}(f; g)$. Then it follows that for any context Γ and terms $\Gamma \vdash f : A \to B$, $\Gamma \vdash g : A \to B$, we have $[\Gamma \mid \forall x : A.\ fx = gx] \leq [\Gamma \mid f = g]$, so $(\forall x : A.\ fx = gx) \to f = g$ is true in Γ.

   Note that $c \in_C \forall a.\mathrm{eq}(\mathrm{ev}(f \times A); \mathrm{ev}(g \times A))$ if and only if $c \times A \in_{C \times A} \mathrm{eq}(\mathrm{ev}(f \times A); \mathrm{ev}(g \times A))$. But then $\mathrm{ev}(f \times A)(c \times A) = \mathrm{ev}(g \times A)(c \times A)$ for every $c : X \to C$, so $\mathrm{ev}(fc \times A) = \mathrm{ev}(gc \times A)$. By the uniqueness of transposes the follows that $fc = gc$, that is, $c \in_C \mathrm{eq}(f; g)$. Thus $\forall a.\mathrm{eq}(\mathrm{ev}(f \times A); \mathrm{ev}(g \times A)) \subseteq \mathrm{eq}(f; g)$. By the above argument the follows that function extensionality is valid in every context Γ.

2. For propositional extensionality, we need only show that for all $\varphi, \psi : A \to \Omega$ and $x : X \to A$, if $(\varphi \Rightarrow \psi)x = t_X$ and $(\psi \Rightarrow \varphi)x = t_X$, then $\varphi x = \psi x$, so $x \in_X \mathrm{eq}(\varphi; \psi)$. But if $(\varphi \Rightarrow \psi)x = t_X$, then $\varphi x \leq \psi x$, and similarly we have $\psi x \leq \varphi x$. Since $\mathrm{Hom}(X, \Omega)$ is a poset, we have by antisymmetry that $\varphi x = \psi x$.

   Then we have in any context Γ and terms $\Gamma \vdash \varphi : \Omega$, $\Gamma \vdash \psi : \Omega$, that $[\Gamma \mid \varphi \Rightarrow \psi, \psi \Rightarrow \varphi] \leq [\Gamma \mid \varphi = \psi]$, so the axiom $(\varphi \Rightarrow \psi) \wedge (\psi \Rightarrow \varphi) \to \varphi = \psi$ is valid in every context Γ.

3. We want to show that for any relation $r : R \rightarrowtail A \times B$ which satisfies $\forall x : A.\ \exists! y : B.\ \rho(x, y)$, there is a morphism $f : A \to B$ such that $r \cong \langle \mathrm{id}_A, f\rangle$. Note that if

$r_A = \pi_A r$ is an isomorphism, then the composition $r_B r_A^{-1}$ would be such a desired morphism, and $r = \langle r_A, r_B \rangle = \langle \mathrm{id}_A, r_B r_A^{-1} \rangle r_A$, so r is isomorphic to the graph of $r_B r_A^{-1}$. From earlier it suffices to show that r_A is internally both injective and surjective. That is, $[\![\vdash \forall p : R.\ \exists! a : A.\ a = r_A p]\!] = t$. But for any p in r_A we have $\rho(rp) = \rho(r_A p, r_B p) = t_R$. Arguing internally, we have from the assumption that ρ be functional that r_A is both injective, since if $x = r_A p_1 = r_A p_2$, then $\rho(x, r_B p_1)$ and $\rho(x, r_B p_2)$, so $r_B p_1 = r_B p_2$, hence $p_1 = p_2$, and surjective, since for each $x : A$ we have some $y : B$ with $\rho(x, y)$, so $\langle x, y \rangle$ is in r. Hence r_A is an isomorphism, so r is (isomorphic to) the graph of some morphism $f : A \to B$.

Finally we then have that the axiom

$$\forall \rho : A \times B \to \Omega.\ (\forall x : A.\ \exists! y : B.\ \rho(x, y)) \to \exists f : A \to B.\ \forall x : A.\ \rho(x, f\,x)$$

is valid. □

Note that we we have in our internal language many axioms and rules similar to those of ordinary mathematics. One crucial rule, however, is missing: the law of excluded middle, or equivalently that of double negation elimination. That is because not every elementary topos satisfies these laws; in fact, most do not. When these rules hold we say that the topos is *boolean*; equivalently, a topos is boolean whenever the lattices of subobjects are boolean. This holds in **Set**, since there subobjects are subsets, and every subset has a complement. However, we will give a topos which is not boolean in section 8. Once we have constructed such a topos, we have according to the soundness theorem that the law of excluded middle is not provable; if that were the case, then no such example could exist.

Despite not necessarily having the law of excluded middle, we still have a lot of power to formalise mathematics within the internal language. For example, we may construct within the topos an initial object, it is given by the extension $[\ \mid \bot]$ [Str04, p. 97]. In a similar manner, the coproduct of any two objects A and B may be found as certain subobject of $\Omega^A \times \Omega^B$.

In fact, we are even able to encode quotients in the usual way. That is, given an *internal* equivalence relation ρ on an object A (that is, a morphism $A \times A \to \Omega$ which is internally reflexive, symmetric, and transitive) we may form the object A/ρ given by the extension $[s : \Omega^A \mid \exists x : A.\ s = \{y : A \mid \rho\langle x, y \rangle\}]$. The natural projection is then easily defined by the axiom of unique choice, since every (generalised) element of A belongs to exactly one equivalence class. Similarly, the universal property of quotients, that a morphism $f : A \to B$ which respects ρ, in that the formula $\forall x\, y : A.\ , \rho\langle x, y \rangle \Rightarrow f\,x = f\,y$ is true, factors through A/ρ uniquely, also follows from the axiom of unique choice and function extensionality.

7 Natural numbers objects

Up until now any reasoning available has been, at least to some degree, finitistic; we cannot with the tools provided in the last two sections construct an object which, internally, has infinitely many terms. This is akin to how in set theory, we require the axiom of infinity for such reasoning. For elementary topoi there is a corresponding axiom; the axiom that there exists a *natural numbers object*, an object whose "elements" are natural numbers.

In this section we present the definition of natural numbers objects, and show how these object support a form of recursion and the induction principle for subobjects. Finally we make use of the induction principle to add in the internal language an inference rule for induction, and show that this rule is sound.

The idea of a natural numbers object is quite simple; it should be an object with a global element "zero" and a successor morphism. Finally, it should support a form of recursion, which here is given by a universal property.

Definition 7.1 (Natural Numbers Objects)**.** Let $\mathcal{E}$ denote an elementary topos. Then a *natural numbers object* (abbreviated as *NNO*) in $\mathcal{E}$ is an object $N \in \mathcal{E}$ with morphisms $z : 1 \to N$ and $s : N \to N$, such that for any other object X with morphisms $x : 1 \to X$ and $f : X \to X$ there is a unique morphism $u : N \to X$ making the following diagram commutes:

$$\begin{tikzcd} 1 \arrow[r, "z"] \arrow[dr, "x"'] & N \arrow[r, "s"] \arrow[d, "u"] & N \arrow[d, "u"] \\ & X \arrow[r, "f"] & X \end{tikzcd}$$

Remark. Note that the universal property gives rise to iteration, in the sense that for object X with morphisms $x : 1 \to X$ and $f : X \to X$, the unique morphism h from an NNO N to X satisfies $h\underline{n} = f^n x$, where $\underline{n} : 1 \to N$ denotes $s^n z$ for n an external natural number. This is easily proved by external induction.

Whilst the definition of NNOs only gives us unique morphisms by iteration, we can actually use the cartesian closed structure to gain a form of iteration with parameters. In fact, we can actually prove a stronger statement: if $\mathcal{C}$ has an NNO N, then every slice category $\mathcal{C}/A$ has an NNO given by $N \times A \xrightarrow{\pi_A} A$.

Theorem 7.1
Suppose N is an NNO in $\mathcal{E}$. Then for any object A of $\mathcal{E}$ it holds that $N \times A \xrightarrow{\pi_A} A$ is an NNO in $\mathcal{E}/A$.

Proof. Take $z_A = \langle z!_A, \mathrm{id}_A \rangle : A \to N \times A$ and $s_A = s \times A : A \times N \to A \times N$. We need to show that for any $A \xrightarrow{z'} X \xrightarrow{s'} X$ in $\mathcal{E}/A$ there exists a unique morphism $h : A \times N \to X$ such that the diagram below commutes:

$$\begin{tikzcd} & A \times N \arrow[r, "s_A"] \arrow[d, "h"] & A \times N \arrow[d, "h"] \\ A \arrow[ur, "z_A"] \arrow[r, "z'"] \arrow[dr, "\mathrm{id}_A"'] & X \arrow[r, "s'"] \arrow[d] & X \arrow[dl] \\ & A & \end{tikzcd}$$

Since N is an NNO, we have a unique morphism $\overline{h} : N \to X^A$ such that the diagram

$$\begin{tikzcd} 1 \arrow[r, "z"] \arrow[dr, "\ulcorner z' \urcorner"'] & N \arrow[r, "s"] \arrow[d, "\overline{h}"] & N \arrow[d, "\overline{h}"] \\ & X^A \arrow[r, "\overline{s'}"] & X^A \end{tikzcd}$$

commutes, which uniquely defines h by corollary 4.4. We then have by proposition 4.5 that

$$hz_A = h\langle z, \mathrm{id}_A \rangle = \mathrm{ev}(\overline{h} \times A)\langle z, \mathrm{id}_A \rangle = \mathrm{ev}\langle \overline{h}\, z, \mathrm{id}_A \rangle = \mathrm{ev}\langle \ulcorner z' \urcorner, \mathrm{id}_A \rangle = z' \,\mathrm{id}_A = z'.$$

Similarly we have

$$hs_A = h(s \times A) = \mathrm{ev}(\overline{h} \times A)(s \times A) = \mathrm{ev}(\overline{h}\, s \times A) = \mathrm{ev}(\overline{s'} \times A) = s'.$$

Thus the chosen h makes the required diagram commute. Uniqueness follows from similar computations. ∎

Iteration with parameters follows immediately from this result.

Corollary 7.2
Let N be an NNO in a cartesian closed category $\mathcal{C}$. Then for any objects P and X with a morphism $b : P \to X$ and $i : P \times X \to X$. Then there exists a unique morphism f from $P \times N \to X$ such that $f\langle P, z!_P\rangle) = b$ and $f(P \times s) = i\langle \pi_P, f\rangle$.

Proof. Notice that $b : P \to X$ in $\mathcal{C}$ gives rise to a global element $\langle b, \mathrm{id}_P\rangle : P \to X \times P$ in $\mathcal{C}/P$. Similarly, i gives a morphism $\langle i\sigma_{X,P}, \pi_P\rangle : X \times P \to X \times P$ in $\mathcal{C}/P$, where $\sigma_{X,P} = \langle \pi_2, \pi_1\rangle : X \times P \to P \times X$. Since $N \times P$ is an NNO in $\mathcal{C}/P$, we have a unique morphism $h : N \times P \to X \times N$ such that $hz_P = \langle b, \mathrm{id}_P\rangle$ and $hs_P = \langle i\sigma_{X,P}, \pi_P\rangle h$ in $\mathcal{C}/P$. Furthermore we have $\pi_P = \pi_P h$ in $\mathcal{C}$ since h is a morphism in $\mathcal{C}/P$. The composite $f = \pi_X h \sigma_{P,N} : P \times N \to X$ gives a morphism of the desired form, and computation shows that the expected equations

$$f\langle P, z!_P\rangle = b \text{ and } f(P \times s) = i\langle \pi_P, f\rangle$$

hold. Finally, uniqueness follows from uniqueness of h; any other f' would yield $h' = \langle f'\sigma_{N,P}, \mathrm{id}_P\rangle$ would yield a morphism from $N \times P$ to $X \times P$ with $h'z_P = \langle b, \mathrm{id}_P\rangle$ and $h's_P = \langle i\sigma_{X,P}, \pi_P\rangle h'$, so $h = h'$. □

Beyond recursion with parameters, a useful property of the natural numbers is that we can use them to prove statements by induction. The statement in set theory can be given as saying that the only subset of the set of natural numbers containing zero and being closed under successors is the whole set. This can equivalently be stated in our language for subobjects as follows:

Theorem 7.3
Let U be a subobject of N a natural numbers object. Then if $z \in U$ and $U \subseteq s^*(U)$, then $U = \top$ is the maximal subobject.

Proof. Let $u : U \rightarrowtail A$ be a representative of U. From $z \in U$ there is some $z' : 1 \to U$ such that $z = uz'$. Similarly there is an $s' : U \to U$ such that $su = us'$. By the universal property of NNOs there is then a morphism $h : N \to U$ for which $hz = z'$ and $hs = s'h$. But $uhz = uz' = z$ and $uhs = us'h = suh$, so $uh : N \to N$ must be identity from the universal property of natural numbers objects. Furthermore $uhu = u = u1_N$, and u is a monomorphism, so $hu = 1_n$. □

Furthermore, we can just as with recursion extend the statement to allow for parameters.

Corollary 7.4
Let R be a subobject of $A \times N$, where N is an NNO. If $\langle A, z\rangle \in R$ and $R \subseteq (A \times s)^*(R)$, then $R = \top_{A\times N}$ is the maximal subobject.

Proof. Notice that R is a subobject of the natural numbers object in $\mathcal{E}/A$ by theorem 7.1, and that $z_A = \langle A, z\rangle \in R$ and $R \subseteq (A \times s)^*(R) = s_A^*(R)$. Thus by the previous theorem we have that $R = \top_{A\times N}$ in $\mathcal{E}/A$, and thus also in $\mathcal{E}$. □

Finally we can prove that induction is valid in an elementary topos with a natural numbers object.

Theorem 7.5
In any topos $\mathcal{E}$ with a natural numbers object N, the induction rule

$$\frac{\Gamma \vdash \varphi : N \to \Omega \qquad \Gamma \mid \Phi \vdash \varphi\ z \qquad \Gamma, n : N \mid \Phi, \varphi\ n \vdash \varphi\ (s\ n)}{\Gamma \mid \Phi \vdash \forall n : N.\ \varphi\ n}$$

is sound.

Proof. From the assumption we have $[\Gamma \mid \Phi] \subseteq [\Gamma \mid \varphi\ z]$ and

$$[\Gamma, n : N \mid \Phi] \cap [\Gamma, n : N \mid \varphi\ n] \subseteq [\Gamma, n : N \mid \varphi\ (s\ n)].$$

Overloading notation somewhat, let Φ and φ denote the classifying morphisms of $[\Gamma \mid \Phi]$ and $[\Gamma, n : N \mid \varphi n]$ respectively. Then let $A := [\![\Gamma]\!]$ and define $\rho := \Phi\pi_A \Rightarrow \varphi$. Then we have $\rho\langle \mathrm{id}_A, z!_A\rangle = t_A$ since $\Phi \leq \varphi\langle \mathrm{id}_A, z!_A\rangle$ by substituting n for z. Similarly $\rho \leq \rho(A \times s)$ since

$$\rho(A \times s) = (\Phi\pi_A \Rightarrow \varphi)(A \times s) = \Phi\pi_A \Rightarrow \varphi(A \times s),$$

and since $\Phi\pi_2 \wedge \varphi \leq \varphi(A \times s)$, we may deduce $\Phi\pi_2 \Rightarrow \varphi \leq \Phi\pi_2 \Rightarrow \varphi(A \times s)$. So $\rho = \Phi\pi_2 \to \varphi$ classifies the maximal subobject, i.e. $\rho = t_{A\times N}$, by the previous corollary. Hence $\Phi\pi_2 \leq \varphi$, so $\Phi \leq \forall_A \varphi$, which is what we needed to prove. □

Once we have natural numbers and induction, most common constructions we use throughout mathematics can be carried out in the internal language as well. For example, integers can be constructed as a quotient of the object $N \times N$ as usual, rationals as quotients of of pairs integers, etc.

8 Examples of elementary topoi

In this section we cover a few examples of elementary topoi. First we show how both **Set** and **FinSet**, the category of finite sets and functions, form elementary topoi, with the latter lacking a natural numbers object. Then we move on to the construction of presheaf topoi, which are an important and useful class of topoi.

8.1 FinSet

We have already seen that **Set** is an elementary topos, since it was the motivating example for both subobject classifiers and cartesian closedness. However, note that we never used any appeals to infinite sets in these definitions. Thus one may wonder if finite sets are enough, that is, if the category **FinSet**, of finite sets and functions, is also an elementary topos. We show here that it is an elementary topos, and that it also, expectedly, has no natural numbers object.

Proposition 8.1
FinSet *is an elementary topos.*

Proof. We first show that **FinSet** has all finite limits. This follows immediately from the fact that **Set** has all finite limits, and as well as the fact that any singleton set is finite, the product of two finite sets is finite, and any subset of a finite set is finite, so the equaliser of two morphisms $f, g : A \to B$ between finite sets is as well.

For cartesian closure, it suffices to show that the set of functions between to finite sets is also finite, since then we simply appeal to **Set** again. But this is a well-known fact.

Finally, the same reasoning applies to the subobject classifier: in **Set** the subobject classifier has exactly two elements, and so it is also a finite set. Then we apply the reasoning motivating the definition of the subobject classifier in section 3, and we are done. □

Since the set of natural numbers is not finite, we would expect **FinSet** not to have a natural numbers object.

Proposition 8.2
FinSet *does not have a Natural Numbers Object.*

Proof. Suppose it did; that is, that (N, z, s) were some NNO in **FinSet**. Since s is a monomorphism, it is injective in **FinSet**. But any injective function from a finite set to itself is bijective, so s is an isomorphism. Let us denote the inverse by p, since p would take a number to its predecessor. From the universal property of NNOs we then have a morphism $e : N \to 2$ given by the recursion data $f : 1 \to 2$ the constant false function and $t_2 = t!_2$ the constant true function. Thus $ez = f$ and $es = t_2 e = t_N$. But then $f = ez = espz = t_n pz = t$, which is a contradiction. □

8.2 Presheaf topoi

In this section we investigate presheaf categories, that is, functor categories valued in **Set**, and show that for $\mathcal{C}$ small, the category of presheaves on $\mathcal{C}$ is an elementary topos.

For the remainder of this section $\mathcal{C}$ will denote a (small) category, and $[\mathcal{C}^{\mathrm{op}}, \mathbf{Set}]$ will denote the category of presheaves on $\mathcal{C}$.

We start again by showing that the category $[\mathcal{C}^{\mathrm{op}}, \mathbf{Set}]$ has all finite limits, which amounts to showing that it has a terminal object and pullbacks.

Proposition 8.3
The category $[\mathcal{C}^{\mathrm{op}}, \mathbf{Set}]$ *has all pullbacks and a terminal object.*

Proof. The terminal object is given by the presheaf 1 sending each object I of $\mathcal{C}$ to $\{*\}$. Thus for any other presheaf A, we construct the natural transformation $! : A \to 1$ by sending each I to $!_{A_I} : A(I) \to \{*\}$ in **Set**. Since at each component the corresponding map exists uniquely, naturality follows.

For pullbacks, let $F : A \to C$ and $G : B \to C$ be natural transformations, with A, B, C presheaves on $\mathcal{C}$. The pullback P of F, G can then be constructed by taking pullbacks component-wise on on objects; $P(I) = A(I) \times_{C(I)} B(I)$. On morphisms $f : J \to I$ in $\mathcal{C}$, we have the, the following diagram commutes by naturality of F, G and the definitions

$$\begin{tikzcd}
P(I) \arrow[rr] \arrow[dr, dashed, "P(f)"'] \arrow[dd] & & B(I) \arrow[dr, "B(f)"] \arrow[dd, "G_I" near start] & \\
& P(J) \arrow[rr] \arrow[dd] & & B(J) \arrow[dd, "G_J"] \\
A(I) \arrow[rr, "F_I"' near end] \arrow[dr, "A(f)"'] & & C(I) \arrow[dr, "C(f)"] & \\
& A(J) \arrow[rr, "F_J"'] & & C(J)
\end{tikzcd}$$

where the dashed morphism $P(f)$ exists by the universal property of the pullback $P(J)$. Since the diagram commutes, it follows that the expected expected projections are natural transformations. Uniqueness follows directly from the fact that each component has the uniqueness condition for pullbacks. $\square$

Note that products and equalisers are likewise given pointwise. That is, the product of two presheaves A and B is given by the presheaf defined on objects as $(A \times B)(I) = A(I) \times B(I)$.

To show that the category of presheaves is cartesian-closed we will use the fact that the exponential is right adjoint to the product, should it exist. Thus for any object I of C we should have that $\mathrm{Hom}(\text{よ}(I) \times A, B)$ is isomorphic to $\mathrm{Hom}(\text{よ}(I), B^A) \cong B^A(I)$ by the yoneda lemma. But this completely determines the presheaf $B^A(I)$, that is, we may define $B^A(I) = \mathrm{Hom}(\text{よ}(I) \times A, B)$. Then all that remains is to show that this actually is the exponential of A and B.

Proposition 8.4 (Streicher [Str04, p. 64, theorem 11.1])
Given presheaves A, B, their exponential is the presheaf B^A given by $B^A(I) = \mathrm{Hom}(\text{よ}(I) \times A, B)$ on objects and $B^A(f) = \mathrm{Hom}(\text{よ}(f) \times A, B)$ on morphisms. The evaluation map $\mathrm{ev} : B^A \times A \to B$ is given by

$$\mathrm{ev}_I(\varphi, a) = \varphi_I(\mathrm{id}_I, a)$$

for $\varphi \in B^A(I)$ and $a \in A(I)$. The transpose of a transformation $\tau : X \times A \to B$ is given by $(\overline{\tau}_I(x))_J(f, a) = \tau_J(X(f)(x), a)$ with X a presheaf, $x \in X(I)$, $f : J \to I$ a morphism in C, and $a \in A(J)$.

We can use the same trick to show that the presheaf category has a subobject classifier; supposing a subobject classifier Ω exists in $[\mathcal{C}^{\mathrm{op}}, \mathbf{Set}]$, we would for each object I of $\mathcal{C}$ have by the Yoneda lemma that $\Omega(I) \cong [\mathcal{C}^{\mathrm{op}}, \mathbf{Set}](\text{よ}(I), \Omega) \cong \mathrm{Sub}(\text{よ}(I))$. Thus we may take $\Omega(I) = \mathrm{Sub}(\text{よ}(I))$ as the definition of Ω. Then all that remains is to show that this actually is the subobject classifier.

Proposition 8.5 ([Str04, p. 82, theorem 12.1])
The presheaf defined by $\Omega(I) = \mathrm{Sub}(\text{よ}(I))$ is a subobject classifier.

Using the same method as with sets, we may canonically represent subobjects of presheaves as well:

Definition 8.1 (Subpresheaves)**.** A *subpresheaf* U of a presheaf A over $\mathcal{C}$ is a presheaf such that for each object c of $\mathcal{C}$, we have $U(c) \subseteq A(c)$, and for each morphism $f \in \mathcal{C}(c, d)$, $U(f)$ is the restriction of $A(f)$ to the domain $U(d)$; that is, $U(f)(x) = A(f)(x)$ for all $x \in U(d)$.

Then a subpresheaf U of a representable functor $\mathcal{C}(-, c)$ for some object $c \in \mathcal{C}$ is simply a set of morphisms of $\mathcal{C}$ into c, closed under precomposition; such sets are called *sieves* [Str04, p. 82, theorem 21.1] of the object c. With this rephrasing of subobjects of representables, we may explicitly compute the subobject classifier for certain presheaves.

For example, if $\mathcal{C} = [0 \xrightarrow{\alpha} 1]$ is the category with two objects 0 and 1, exactly one non-identity morphism $\alpha : 0 \to 1$, then $\Omega(0) = \{\emptyset, \{\mathrm{id}_0\}\}$, since these are the only sieves on 0, and $\Omega(1) = \{\emptyset, \{\alpha\}, \{\alpha, \mathrm{id}_1\}\}$. The global elements of $\Omega \in [\mathcal{C}^{\mathrm{op}}, \mathbf{Set}]$ are then

- f given by $f_0(*) = \emptyset$ and $f_1(*) = \emptyset$, corresponding to the minimal element of Ω,
- u given by $u_0(*) = \{\mathrm{id}_0\}$ and $u_1(*) = \{\alpha\}$, and lastly
- t given by $t_0(*) = \{\mathrm{id}_0\}$ and $t_1(*) = \{\alpha, \mathrm{id}_1\}$.

Naturality for each of these is easy to check. Thus $[\mathcal{C}^{\mathrm{op}}, \mathbf{Set}](1, \Omega)$ has three elements. Furthermore, we infer from this that $[\mathcal{C}^{\mathrm{op}}, \mathbf{Set}]$ is not boolean; if it were, then $[\mathcal{C}^{\mathrm{op}}, \mathbf{Set}](1, \Omega)$ would be a boolean algebra, but it has three elements, where a finite boolean algebra must have an even number of elements, since every element has a distinct complement.

Furthermore, every presheaf topos inherits a natural numbers object from **Set**:

Proposition 8.6
Let $\mathcal{C}$ be some small category, such that $[\mathcal{C}^{\mathrm{op}}, \mathbf{Set}]$ is a topos. Then $\mathcal{C}$ has a natural numbers object given by $N(c) = \mathbb{N}$ for each object c, and which acts as identity on the morphisms of $\mathcal{C}$.

Proof. We must show that N satisfies the universal property, so let X be some presheaf with natural transformations $x : 1 \to X$ and $f : X \to X$. Then at each $I \in \mathrm{Ob}(\mathcal{C})$, we have a function $h_I : N(I) \to X(I)$ by the universal property of $\mathbb{N}$ in **Set**. Thus we have a candidate family of maps $h_I : N(I) \to X(I)$, given uniquely by the $\mathbb{N}$, to be the required natural transformation. We need only show naturality: let $f \in \mathcal{C}(J, I)$ be given. Then we have a diagram as below:

$$\begin{tikzcd}
1 \arrow[rr, "z"] \arrow[dr] \arrow[ddrr, "x_I"'] & & \mathbb{N} \arrow[rr, "s"] \arrow[dr] \arrow[dd, "h_I"] & & \mathbb{N} \arrow[dr] \arrow[dd, "h_I"] & \\
& 1 \arrow[rr, "z"] \arrow[ddrr, "x_J"] & & \mathbb{N} \arrow[rr, "s"] \arrow[dd, "h_J"] & & \mathbb{N} \arrow[dd, "h_J"] \\
& & X(I) \arrow[rr, "f_I"] \arrow[dr, "X(f)"'] & & X(I) \arrow[dr, "X(f)"] & \\
& & & X(J) \arrow[rr, "f_J"] & & X(J)
\end{tikzcd}$$

The top squares, bottom square, and diagonal square all commute. Similarly, the front and back squares commute by the universal property of NNOs. Hence all squares commute, so h is a natural transformation $N \to X$. Uniqueness follows from uniqueness of each morphism h_I, since $\mathbb{N}$ is an NNO of **Set**. $\square$

9 Conclusion

The goal of the thesis was to present the axioms of elementary topoi, and then to show how to, for any elementary topos $\mathcal{E}$, interpret a formal language into $\mathcal{E}$, with a sound proof system built atop the language. With the internal language and proof system at hand, we can show several properties about elementary topoi themselves, such as explicit constructions of finite colimits and image factorisations. Furthermore, the internal language provides a new possible semantics for higher-order intuitionistic logic, and so gives another tool for studying independence properties of statements in such a logic.

We gave only a small sample of the elementary topoi which are interesting to consider. Thus there are plenty more examples, such as the large and useful class of topoi of categories of *shaves*, which are covered in MacLane and Moerdijk [MM12]. As an example of the nice logical properties of this class, we note that an equivalent to the notion of Cohen forcing in set theory can be recovered using the language of sheaves [MM12, p. VI. 2]. Another interesting class of elementary topoi are so called *realisability topoi* [Van08], such as the effective topos, which verifies the statement that "all functions $\mathbf{N} \to \mathbf{N}$ are computable" [Van08, p. 124, Proposition 3.1.6]. Further generalisation of the concept of realisability may even be used to construct an elementary topos in which the real numbers are countable, in that there exists a surjection from the natural numbers object to a construction of real numbers within the topos [And22].

Another direction that could have been explored is that of Kripke-Joyal semantics, which allows for reasoning about the validity of formulas at generalised elements, instead of just the internal notion of validity [McL92, ch. 18]. In a similar vein, we chose in this thesis to present the internal language as a simple type theory, with a proof system built atop it. Another option would have been to present the internal language as a dependent type theory, which would allow for lessening the distinction between proof and term, and would have given a much richer language to reason within. However, that richness comes at the cost of more complicated semantics.

References

[And22] James E. Hanson Andrej Bauer. *The countable reals*. Topos Institute. 2022. URL: `https://www.youtube.com/watch?v=4CBFUojXoq4`.

[Bor94] Francis Borceux. *Handbook of Categorical Algebra: Volume 3, Sheaf Theory*. Vol. 3. Cambridge University Press, 1994.

[Fre72] Peter Freyd. "Aspects of topoi". In: *Bulletin of the Australian Mathematical Society* 7.1 (1972), pp. 1–76.

[Geu09] Herman Geuvers. "Introduction to Type Theory". In: *Language Engineering and Rigorous Software Development: International LerNet ALFA Summer School 2008, Piriapolis, Uruguay, February 24 - March 1, 2008, Revised Tutorial Lectures*. Ed. by Ana Bove et al. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 1–56. ISBN: 978-3-642-03153-3. DOI: `10.1007/978-3-642-03153-3_1`. URL: `https://doi.org/10.1007/978-3-642-03153-3_1`.

[McL92] Colin McLarty. *Elementary categories, elementary toposes*. Clarendon Press, 1992.

[MM12] Saunders MacLane and Ieke Moerdijk. *Sheaves in geometry and logic: A first introduction to topos theory*. Springer Science & Business Media, 2012.

[MR11] Jean-Pierre Marquis and Gonzalo Reyes. "The history of categorical logic: 1963-1977". In: (2011).

[Str04] Thomas Streicher. "Introduction to category theory and categorical logic". In: *Lecture notes, Technische Universitat Darmstadt* (2004).

[Tie11] M. Tierney. "Axiomatic Sheaf Theory : Some Constructions and Applications". In: *Categories and Commutative Algebra*. Ed. by P. Salmon. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 249–326. ISBN: 978-3-642-10979-9. DOI: `10.1007/978-3-642-10979-9_8`. URL: `https://doi.org/10.1007/978-3-642-10979-9_8`.

[Van08] Jaap Van Oosten. *Realizability: an introduction to its categorical side*. Elsevier, 2008.