Submitted on December 15, 2020 to the Notre Dame Journal of Formal Logic
Volume ??, Number ??,

Ordinal Arithmetic in the Category of Sets

James Baxter and Dustin Bryant

Abstract The elementary theory of the category of sets (ETCS) provides an alternate foundation for set theory in the language of category theory. Precisely, ETCS is a well-pointed topos theory with a natural number object. Earlier work on arithmetic in ETCS has mainly focused on cardinal numbers modeled as sets. In this paper, we consider the elements of the natural number object of ETCS as natural numbers, representing the finite ordinals. We show how arithmetical operations can be constructed as functions within the category of sets. We also show how integers can be constructed in terms of these natural numbers, and define corresponding arithmetic operations on the integers. Finally, we discuss how our work compares to other formulations of arithmetic and some of the philosophical implications of our approach.

1 Introduction

The Elementary Theory of the Category of Sets (ETCS), proposed by Lawvere [5], presents an axiomatization of sets and the functions between them in terms of concepts from category theory. This may be viewed as an alternative presentation of set theory, in contrast to the usual axiomatizations in terms of a set membership relation. In ETCS members of sets are instead viewed as particular functions into those sets, and we thus have elements of sets that are of a distinct sort to the sets themselves, in contrast to the traditional approach in which everything is a set. Leinster [6] suggests that such an approach more closely aligns with the working mathematician's intuitions since one may rightly ask, for example, what the elements of π are within ZFC which seems counter to the nature of numbers.

Throughout much of the 20th century, axiomatic set theory has been developed with the aim of using it as foundation for mathematics. As such, one of the earliest projects was to encode the counting numbers in terms of sets and define arithmetic upon them. In 1973, Osius [8] showed that ETCS and Zermelo-Fraenkel set theory (ZF) are equivalent in a certain sense. It is thus possible to define arithmetic on

2010 Mathematics Subject Classification: Primary 03E10, 03E45; Secondary 03G30
Keywords: Elementary Theory of the Category of Sets, Elementary Topos of Sets, foundations of mathematics, natural number object, ordinal arithmetic, set theory

ETCS sets much as it is in ZF. Indeed, such an approach was taken by Hatcher [4] to define arithmetic on cardinal numbers in a categorical setting. Hatcher does also define ordinal numbers in a manner closer to our approach below and proves the Peano postulates for them, although he does not define arithmetic on such numbers.

However, as we noted above, the concept of elements of sets in ETCS differs from that of other set theories. Thus, if we encode numbers as particular sets, we cannot talk about a set of numbers in ETCS, nor do we have operations on numbers as functions in the ETCS sense. It may be noted, however, that the approach of defining numbers in terms of sets is not the only approach to defining numbers. For example, Peano [9], without saying what zero is, defined the natural numbers only in terms of zero and successors of zero, and Church [2] defined an encoding of numbers in terms of functions.

In particular, we want to define a set of numbers as an ETCS set, with the numbers themselves as elements of that set. We note that ETCS comes equipped with a natural number object, so our approach is to just take that as our set of natural numbers. We also wish to define arithmetic operators on this set as ETCS functions. To do so is not trivial, since ETCS does not supply a direct means of defining arbitrary functions, and we can thus only use the functions that follow from the axioms. In this paper, we show that arithmetic operators can indeed be constructed in ETCS and prove basic properties about them, in Section 3. Then, in Section 4, we also show that the set of natural numbers in ETCS can be lifted to define the set of integers, as an example of how more general sets of numbers may be constructed in ETCS. This demonstrates that ETCS can serve as a viable alternative foundation for mathematics.

Next, we present a brief overview of the axioms of ETCS in order to aid understanding of the later sections, particularly drawing attention to how the axioms can be used for defining arithmetic. After that, we present our construction of arithmetic in Sections 3 and 4. Finally, we discuss some of the philosophical implications of our work and conclude in Section 5.

2 The Elementary Theory of the Category of Sets

In this section, we briefly present the axioms of ETCS, particularly following the axiomatization given in Halvorson [3]. However, for didactic reasons we present the axioms in a different order from that Halvorson uses. Our aim here is not to present a full description of ETCS, but to make clear the foundation upon which we are building arithmetic and present some important lemmas that we make use of in our arithmetical proofs. We omit proofs of these lemmas as they are standard lemmas that may be found in Halvorson.

Halvorson's presentation of ETCS consists of 11 axioms, describing a category $\mathbf{Sets}$ in category theoretic terms. The first axiom simply establishes that $\mathbf{Sets}$ is indeed a category, that is, it has an associative function composition operation $\circ$ and identity functions id_X. This is, of course, foundational when working in category theory, but needs to be included in order to produce an adequate axiomatization of $\mathbf{Sets}$. We take full advantage of the associativity of composition in our work, frequently omitting parentheses around function compositions.

Axiom 1 ($\mathbf{Sets}$ is a Category) $\mathbf{Sets}$ consists of functions and sets. Each function f has unique domain and codomain sets, and we write $f : X \to Y$ to mean that X is the domain of f and Y is the codomain of f. For any two functions $f : X \to Y$

and $g : Y \to Z$ in $\mathbf{Sets}$, there is a function $g \circ f : X \to Z$ in $\mathbf{Sets}$ such that $h \circ (g \circ f) = (h \circ g) \circ f$ for any functions f, g and h. We often write gf for $g \circ f$. For each set X in $\mathbf{Sets}$, there is a function $\mathrm{id}_X : X \to X$ such that $\mathrm{id}_X \circ f = f$ for any function f with codomain X and $g \circ \mathrm{id}_X = g$ for any function g with domain X. Occasionally, we just write id for id_X when the set X is clear.

The axioms of ETCS frequently make use of concepts from category theory. One such concept is the notion of a *terminal object*, which is an object that has a unique morphism from each object to itself. Axiom 2 asserts the existence of such an object in ETCS, a set which we refer to as $\mathbf{1}$. It also asserts that $\mathbf{1}$ is a *separator*, which means functions are judged to be the same when their compositions with functions having a domain of $\mathbf{1}$ are all the same.

Axiom 2 (Terminal Object) $\mathbf{Sets}$ contains a set $\mathbf{1}$ such that, for any set X, there is a unique function $\beta_X : X \to \mathbf{1}$. Furthermore, for any functions $f, g : X \to Y$, if $f \circ x = g \circ x$ for all functions $x : \mathbf{1} \to X$, then $f = g$.

The set $\mathbf{1}$ may be seen intuitively as a single element set. Since a function from a single element set into any other set X identifies exactly one element of X, we take them to represent elements of X and write $x \in X$ for $x : \mathbf{1} \to X$. It then follows from the uniqueness of $\beta_{\mathbf{1}}$, that $\mathbf{1}$ does indeed have a single element, which must be equal to both $\beta_{\mathbf{1}}$ and $\mathrm{id}_{\mathbf{1}}$. Thus, while ETCS does not start with an axiomatization of set membership, an intuitive notion of set membership can be defined within it. Application of a function to an element of its domain can then be simply defined by composing the function with the element.

The functions β_X are useful for defining constant functions, since, for any function $y : \mathbf{1} \to Y$, $y \circ \beta_X : X \to Y$ represents the function that yields y when applied to any $x : \mathbf{1} \to X$. We use such functions at various points in our construction of arithmetic. The separator property in Axiom 2 is also occasionally useful in proofs of the laws of arithmetic, since it allows us to apply a form of function extensionality.

The dual notion to an initial object is that of a *terminal object*, which is an object that has a unique morphism from itself to every object. Axiom 3 establishes that the empty set, $\emptyset$, is a terminal object of $\mathbf{Sets}$. It also asserts that $\emptyset$ is indeed empty, that is, there is no function $x \in \emptyset$. While the existence of the empty set is of great importance in set theory in general, we have not found this axiom particularly useful in our construction of arithmetic.

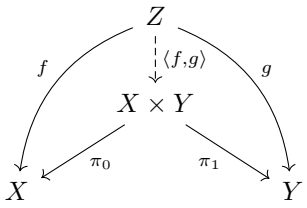
Axiom 3 (Empty Set) $\mathbf{Sets}$ contains a set $\emptyset$ such that for any set X there is a unique function $\alpha_X : \emptyset \to X$, and there is no function $x : \mathbf{1} \to \emptyset$.

Axiom 4 asserts the existence of Cartesian products of sets and provides for construction of functions into Cartesian products from functions into their elements. In particular, for $x \in X$ and $y \in Y$, we have that $\langle x, y \rangle \in X \times Y$. This axiom also provides projection functions π_0 and π_1 to select the individual components of an element of a Cartesian product. Note that we do not fix the types of π_0 and π_1 to specific sets, but allow their types to be inferred from the context in which they are used. This allows for much more compact statements of lemmas to be written, since the Cartesian products in our construction of arithmetic can often be too complex to succinctly annotate the projection functions with.

Axiom 4 (Cartesian Products) For any sets X and Y in $\mathbf{Sets}$, there is a set $X \times Y$ and functions $\pi_0 : X \times Y \to X$ and $\pi_1 : X \times Y \to Y$ in $\mathbf{Sets}$, such that for any

functions $f : Z \to X$ and $g : Z \to Y$, there is a unique function $\langle f, g\rangle : Z \to X \times Y$ such that $\pi_0 \circ \langle f, g\rangle = f$ and $\pi_1 \circ \langle f, g\rangle = g$.

As is usual in category theory, it is frequently helpful to express laws in the form of commuting diagrams. Axiom 4 can be expressed in such a diagram as shown below.



In addition to functions $\langle f, g\rangle$, we have the below definition that allows us to construct the Cartesian product of two functions to act on them in parallel.

Definition 2.1 For any two functions $f : X \to Z$ and $g : Y \to W$, we define $f \times g : X \times Y \to Z \times W$ to mean $\langle f\pi_0, g\pi_1\rangle$.

Since arithmetical functions such as addition and multiplication are binary functions, they have a Cartesian product as their domain. We thus make frequent use of Axiom 4 in our construction of arithmetic. In particular, it is useful to state here some lemmas that we use in the proofs for our construction of arithmetic. The proofs of these lemmas follow easily from $\pi_0 \circ \langle f, g\rangle = f$ and $\pi_1 \circ \langle f, g\rangle = g$, and the fact that the functions $\langle f, g\rangle$ are unique.

Lemma 2.2 $\langle a, b\rangle f = \langle af, bf\rangle$

Lemma 2.3 $(f \times g)\langle a, b\rangle = \langle f \circ a, g \circ b\rangle$

Lemma 2.4 $(x \times y) \circ (a \times b) = (x \circ a) \times (y \circ b)$

Lemma 2.5 $\langle a, b\rangle = \langle c, d\rangle \iff a = c \wedge b = d$

The dual of Cartesian products is coproducts, which may be viewed as representing the disjoint union of two sets. Axiom 5 asserts the existence of coproducts in ETCS and provides coprojection functions i_0 and i_1 to map into each side of a coproduct. While we use Cartesian products frequently in our construction of arithmetic, coproducts are only used in a few facts and constructions that we have found in other sources. We refer to these facts where they are used later in this paper, since they do not form a large part of our work.

Axiom 5 (Coproducts) For any sets X and Y in $\mathbf{Sets}$, there is a set $X \coprod Y$ and functions $i_0 : X \to X \coprod Y$ and $i_1 : Y \to X \coprod Y$ in $\mathbf{Sets}$, such that for any functions $f : X \to Z$ and $g : Y \to Z$, there is a unique function $f \amalg g : X \coprod Y \to Z$ such that $(f \amalg g) \circ i_0 = f$ and $(f \amalg g) \circ i_1 = g$.

ETCS also makes use of the notions of monomorphisms and epimorphisms, which have their standard category theoretical definitions as shown below. The axioms of ETCS are such that it can be shown that these notions correspond to the notions of injectivity and surjectivity respectively (a proof of this can be found in Halvorson). We also have the standard notion of an isomorphism, and it holds that a function in $\mathbf{Sets}$ is an isomorphism if and only if it is both a monomorphism and an epimorphism.

Definition 2.6 (monomorphism) A function $f : X \to Y$ is said to be a *monomorphism* if $fg = fh$ implies $g = h$ for any functions $g, h : Z \to X$.

Definition 2.7 (epimorphism) A function $f : X \to Y$ is said to be an *epimorphism* if $gf = hf$ implies $g = h$ for any functions $g, h : X \to Z$.

Definition 2.8 (isomorphism) A function $f : X \to Y$ is said to be an *isomorphism* if there is a function $g : Y \to X$ such that $g \circ f = \mathrm{id}_X$ and $f \circ g = \mathrm{id}_Y$, and we say that X and Y are *isomorphic*.

In particular, we take monomorphisms to define subobject or subsets, since they characterise an injection from one set to another. This is captured by the definition below.

Definition 2.9 (subobject) A *subobject* or *subset* of a set X is a set A together with a monomorphism $m : A \to X$.

We can then expand our notion of set membership to allow elements of a set to also be members of its subsets, by introducing a notion of relative membership as shown below. This captures the idea of there being a member of the subset that can be injected into the superset by the monomorphism defining the subset relationship, and for which the result of that injection is the corresponding element of the superset.

Definition 2.10 (relative member) If A and $m : A \to X$ form a subobject of X then, for any $x \in X$, we say that $x \in A$ *relative to* X whenever there is some $a \in A$ such that $x = ma$, and we write $x \in_X A$.

Axiom 6 asserts the existence of *equalizers* in ETCS, that is, a set E and a function $m : E \to X$ that makes functions $f, g : X \to Y$ equal when composed with them. It is also the case that there is a mapping between different equalizers of the same two functions. From this fact it can be shown that any equalizer is a monomorphism, and hence defines a subobject. Axiom 6 is thus useful in that it allows us to define subsets of the form $\{x \in X | f \circ x = g \circ x\}$ for any functions $f, g : X \to Y$. We found this useful for constructing an equivalence relation when defining the set of integers.

Axiom 6 (Equalizers) For any functions $f, g : X \to Y$ in $\mathbf{Sets}$, there is a set E and function $m : E \to X$ in $\mathbf{Sets}$ such that $fm = gm$ and, for any other set F and function $h : F \to X$, there is a unique function $k : F \to E$ such that $mk = h$

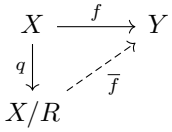
Such a notion of an equivalence relation over an ETCS set can be defined in general as subset of a Cartesian product $X \times X$, using the idea of relative membership. This allows us to state the definition of an equivalence relation in ETCS in a format similar to that of the usual definition, as shown below.

Definition 2.11 (equivalence relation) A subobject R of $X \times X$ is said to be an *equivalence relation on* X when, for any $x, y, z \in X$, we have that $\langle x, x\rangle \in_{X\times X} R$, $\langle x, y\rangle \in_{X\times X} R$ whenever $\langle y, x\rangle \in_{X\times X} R$, and $\langle x, z\rangle \in_{X\times X} R$ whenever $\langle x, y\rangle \in_{X\times X} R$ and $\langle y, z\rangle \in_{X\times X} R$.

Given an equivalence relation R on a set X, it is useful to be able to construct its quotient X/R, and indeed we need such a construction for defining the integers. Axiom 7 asserts the existence of such quotients in ETCS, along with a function q that allows us to map any element of X into its equivalence class in X/R.

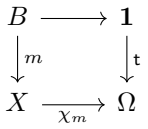
Axiom 7 (Equivalence Classes) For any equivalence relation R on X in $\mathbf{Sets}$, there is a set X/R and a function $q : X \to X/R$ in $\mathbf{Sets}$ such that $\langle x, y\rangle \in_{X\times X} R$ if and only if $q \circ x = q \circ y$, and for any function $f : X \to Y$ such that $\langle x, y\rangle \in_{X\times X} R$ implies $f \circ x = f \circ y$, there is a unique function $\overline{f} : X/R \to Y$ such that $\overline{f} \circ q = f$.

Axiom 7 also provides for the lifting of functions with a a domain of X to functions on the quotient X/R in a way that is consistent with q. This may be expressed using the commuting diagram below, which we instantiate as part of defining operators on the integers. The resulting diagrams are helpful to understanding proofs of certain properties of such operators. The function q is in fact a type of *coequalizer*, the dual of an equalizer, and also an epimorphism.



Another concept that can be applied to subsets is the notion of a *characteristic function*, that is, a function that is true for elements of a particular set and false otherwise. In ETCS, since such a function must have its own domain, we only make such a determination about elements of that domain, and hence we must have characteristic functions defined by subsets. Axiom 8 defines a set of two truth values, t and f representing true and false respectively, and asserts the existence of characteristic functions in ETCS. The properties of characteristic functions are defined using the category-theoretic notion of a *pullback*. This captures the fact that the diagram shown in the axiom commutes, so that any relative member of the subset gives an output of true when composed with the characteristic function. It also posits the existence of a function mapping from a "wider" commuting diagram into the inner commuting diagram, with the consequence that any element for which the characteristic function is true must be a relative member of the subset. The axiom thus captures the fact that a value is a member of the subset if and only if its characteristic function is true for that value.

Axiom 8 (Truth-Value Object) There is a set, Ω, with exactly two elements t and f such that for any set X, and subobject $m : B \to X$, there is a unique function $\chi_B : X \to \Omega$ such that the following diagram is a pullback:



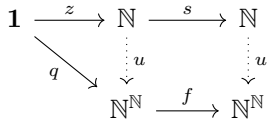
That is, $\chi_m \circ m = \mathsf{t} \circ \beta_B$ and, for any set Z and functions $f : Z \to X$ and $g : Z \to \mathbf{1}$ such that $\chi_m \circ f = \mathsf{t} \circ g$, there is a unique function $h : Z \to B$ such that $f = m \circ h$ and $g = \beta_B \circ h$.

This construction of characteristic functions can be used to construct functions on the truth value set Ω that represent predicate logic operations within ETCS. Axiom 8 thus gives us a way to embed logic within ETCS, and we use this to define a less-than operator on the natural numbers in Section 3.7. In combination with Axiom 6, this also provides a way to construct subsets corresponding to arbitrary predicates, creating an analog of the ZF subset axiom.

As noted previously, ETCS has a natural number object, $\mathbb{N}$, which we take as our representation of the natural numbers. The existence of this object and its properties are established by Axiom 9. The elements of $\mathbb{N}$ provided by this axiom are a zero element z and elements constructed by applying a successor function s to z one or more times. This gives a similar construction of the natural numbers to that of Peano [9], and indeed Hatcher [4] has proved that the Peano postulates hold for these functions, although he did not construct arithmetic operators on them.

Axiom 9 (Natural Number Object) There is an object $\mathbb{N}$, and functions $z : \mathbf{1} \to \mathbb{N}$ and $s : \mathbb{N} \to \mathbb{N}$ such that for any other set X with functions $q : \mathbf{1} \to X$ and $f : X \to X$, there is a unique function $u : \mathbb{N} \to X$ such that $uz = q$ and $us = fu$.

Axiom 9 also provides for constructing functions from $\mathbb{N}$ to any other set by defining the effect of the desired function on z and for each s applied to a number. The form of such constructions may be visualised using the commuting diagram shown below. This thus gives a way of defining functions on natural numbers by recursion. Additionally, such functions are unique, so by constructing two functions that both satisfy the same diagram (that is, with the same q and f functions), we can prove the equality of those functions by induction. This can, using the embedding of logic from Axiom 8, be extended to prove arbitrary facts by induction by showing equality to a constant true function.

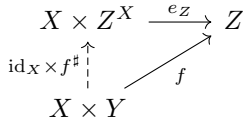


While in ETCS we view functions as representing members of a set and mappings between them, it is also useful to have a set whose members represent functions. Axiom 10 provides for the existence of exponential objects of the form Y^X, which represent sets of functions from X to Y. It also supplies a transpose operator $^\sharp$ to convert functions to members of the exponential set and an evaluation function e_Y to evaluate the transposed functions as the original.

Axiom 10 (Exponential Objects) For any sets A and X in $\mathbf{Sets}$, there is a set X^A and a function $e_X : A \times X^A \to X$ in $\mathbf{Sets}$ such that, for any set Z and function $f : A \times Z \to X$, there is a unique function $f^\sharp : Z \to X^A$ such that $e_X \circ (\mathrm{id}_A \times f^\sharp) = f$.

It is helpful to view this axiom in terms of the commuting diagram shown below, particularly when constructing transposes of some of the more complex functions we encountered in constructing our arithmetic. A particular point of note is that the domain of the function f in the diagram is a Cartesian product, whereas the domain of the transpose function is only the second component of the Cartesian product, with the first component moved to the function "inside" the exponential object. The transpose operation thus represents a form of function currying (named for the logician Haskell Curry), in which a two argument function is converted to a single argument function that outputs a function taking the remaining argument. This is very important in our construction of arithmetic, as most of the arithmetic operators are binary operators, and the functions constructed by Axiom 9 are single argument functions. We thus use this axiom together with Axiom 9 to construct curried versions of the binary

arithmetic operators.



Once we have curried versions of the functions we desire, they can be uncurried using an inverse transpose operator $^\flat$, defined as shown below by evaluating the cross product of a transpose function with the identity function.

Definition 2.12 (inverse transpose) Suppose that $f : Z \to X^A$ is a function then we define $f^\flat : Z \times A \to X$ by $f^\flat = e_X \circ (\mathrm{id} \times f)$.

We also have the following lemmas showing that $^\flat$ functions as an inverse of $^\sharp$:

Lemma 2.13 *For any function $f : A \times Z \to X$, we have $(f^\sharp)^\flat = f$.*

Lemma 2.14 *For any function $f : Z \to X^A$, we have $(f^\flat)^\sharp = f$.*

We also note that any function $g : Y \to Z$ can be lifted to a function $X^A \to Y^A$ on elements of the exponential object, via the definition below. This may be viewed as composing g with the function represented by an element of X^A.

Definition 2.15 (transpose function) Suppose that $g : Y \to Z$ is a function then we define the *transpose* $g^A : X^A \to Y^A$ by $g^A = (g \circ e_Y)^\sharp$.

Such functions are useful at various points while constructing our arithmetic operators in terms of exponential objects. We additionally have the following lemmas from Halvorson [3] allowing us to change between these forms of functions on exponential sets, which we use in our proofs of arithmetical properties.

Lemma 2.16 *For functions $f : A \times X \to Y$ and $g : Y \to Z$, $(g \circ f)^\sharp = g^A \circ f^\sharp$.*

Lemma 2.17 *For functions $f : X \to Y$ and $g : Y \to Z^A$, $(g \circ f)^\flat = g^\flat \circ (\mathrm{id}_A \times f)$.*

Finally, Axiom 11 gives a statement of the axiom of choice in ETCS terms. While this is useful to complete the set of axioms, it is not required for the proof of basic properties of arithmetic, so we do not make further use of it here.

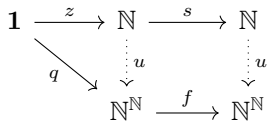
Axiom 11 (Axiom of Choice) For any epimorphism $f : X \to Y$ in $\mathbf{Sets}$, there is a function $s : Y \to X$ such that $fs = \mathrm{id}_Y$.

Next, we proceed to use the axioms described above to construct arithmetic operators on the natural numbers and prove facts about them.

3 Natural Number Arithmetic in ETCS

Having described the axioms of ETCS, we now present our definitions for addition, multiplication, and exponentiation on the natural number object $\mathbb{N}$. These operators are binary operators, each represented by a function $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$. We observe that Axiom 9 provides only for defining functions with a domain of $\mathbb{N}$, so we use it to define curried versions of the operators as functions $\mathbb{N} \to \mathbb{N}^\mathbb{N}$, which we then uncurry using the $^\flat$ transpose operator. The form of Axiom 10 is such that the input to these curried functions represents the second argument of the corresponding uncurried functions. We use Axiom 9 to define these curried functions, which represents defining an operator by recursion in the second argument.

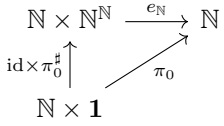
Considering the commuting diagram of Axiom 9, with X set to $\mathbb{N}^{\mathbb{N}}$, we obtain the commuting diagram shown below. The function $u : \mathbb{N} \to \mathbb{N}^{\mathbb{N}}$ is the curried function we wish to obtain, and we need to supply the two functions $q : \mathbf{1} \to \mathbb{N}^{\mathbb{N}}$ and $f : \mathbb{N}^{\mathbb{N}} \to \mathbb{N}^{\mathbb{N}}$ to define it. We may view q as a function representing the application of the operator under construction with zero as its second argument, which is the base case of the recursion. Likewise, f maps a function representing the effect of applying the operator with n as its second argument to a function representing the effect of applying it with $n + 1$ as its second argument, for any natural number n. Thus, f represents the recursive case of the construction of our curried operator.



In addition to constructing the operators, we also prove various equations that they are expected to satisfy. We can in some cases perform a simple calculational proof which amounts to unwrapping definitions. It is often the case, however, that many of the results can only be proven by induction which corresponds to defining recursive functions encoding each side of an equation. For example, to prove $x + y = y + x$ we construct functions $(x, y) \mapsto x + y$ and $(x, y) \mapsto y + x$. We construct these in a curried form, representing $y \mapsto (x \mapsto x + y)$ and $y \mapsto (x \mapsto y + x)$ using Axiom 9, choosing q and f functions that are the same for each. The uniqueness property of Axiom 9 then yields the desired equality. This approach can be extended for proofs involving more than two variables by considering, for example, functions $\mathbb{N} \to \mathbb{N}^{\mathbb{N}\times\mathbb{N}}$.

Having described our general approach to construct operators on the natural numbers and prove properties about them, we now present the construction of each of the operators, stating the q and f functions in each case. After presenting the construction of each operator, we present the properties it satisfies, briefly stating their proofs using the above approach.

3.1 Addition on Naturals As discussed above, we define a curried addition function $u_+ : \mathbb{N} \to \mathbb{N}^{\mathbb{N}}$ using Axiom 9. To motivate the definitions for q and f, which uniquely define u_+, we use lambda calculus to clearly express how we would like q and f to behave. The function $q : \mathbf{1} \to \mathbb{N}^{\mathbb{N}}$ represents a function $\lambda m.\ m + 0$. The function $f : \mathbb{N}^{\mathbb{N}} \to \mathbb{N}^{\mathbb{N}}$ represents a function $(\lambda m.\ m + n) \mapsto (\lambda m.\ (m + n) + 1)$, that is, it returns a function that adds one to the result of its input function. We satisfy the first condition by taking q to be $\pi_0^\sharp : \mathbf{1} \to \mathbb{N}^{\mathbb{N}}$ satisfying the following diagram (which exists uniquely by Axiom 10):



This clearly satisfies the desired property, since it is the element of $\mathbb{N}^{\mathbb{N}}$ that, when applied with the evaluation function $e_{\mathbb{N}}$, returns its input unchanged.

For the function $f : \mathbb{N}^{\mathbb{N}} \to \mathbb{N}^{\mathbb{N}}$, we need to choose a function that satisfies $u_+(s(n)) = f(u_+(n))$ for all n. That is, we want a function that given an "add

n" function, returns an "add $n+1$" function. This is provided for by $s^{\mathbb{N}} : \mathbb{N}^{\mathbb{N}} \to \mathbb{N}^{\mathbb{N}}$, which is defined as $(s \circ e_{\mathbb{N}})^\sharp$ (from Definition 2.15) and satisfies the following diagram (again, existence and uniqueness is ensured by Axiom 10):

$$\begin{array}{ccc} \mathbb{N} \times \mathbb{N}^{\mathbb{N}} & \xrightarrow{e_{\mathbb{N}}} & \mathbb{N} \\ {\scriptstyle \mathrm{id} \times s^{\mathbb{N}}}\uparrow & & \uparrow{\scriptstyle s} \\ \mathbb{N} \times \mathbb{N}^{\mathbb{N}} & \xrightarrow[e_{\mathbb{N}}]{} & \mathbb{N} \end{array}$$

So $s^{\mathbb{N}}$ defines the function that takes a function and has the effect, when applied with $e_{\mathbb{N}}$, of that function, plus applying s ("adding one") to its result.

Plugging $q = \pi_0^\sharp$ and $f = s^{\mathbb{N}}$ into Axiom 9, we then obtain $u_+ : \mathbb{N} \to \mathbb{N}^{\mathbb{N}}$, which satisfies the diagram below.

$$\begin{array}{ccccc} \mathbf{1} & \xrightarrow{z} & \mathbb{N} & \xrightarrow{s} & \mathbb{N} \\ & {\scriptstyle \pi_0^\sharp}\searrow & \downarrow{\scriptstyle u_+} & & \downarrow{\scriptstyle u_+} \\ & & \mathbb{N}^{\mathbb{N}} & \xrightarrow[s^{\mathbb{N}}]{} & \mathbb{N}^{\mathbb{N}} \end{array}$$

We then obtain a function $\mathrm{add} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by $\mathrm{add} = {u_+}^\flat = e_{\mathbb{N}} \circ (\mathrm{id} \times u_+)$. For $\langle m, n \rangle \in \mathbb{N} \times \mathbb{N}$, we have

$$\mathrm{add}(\langle m, n \rangle) = e_{\mathbb{N}} \circ (\mathrm{id} \times u_+) \circ \langle m, n \rangle = e_{\mathbb{N}} \circ \langle m, u_+(n) \rangle$$

So, $\mathrm{add}(\langle m, n \rangle)$ constructs an "add n" function and applies it to m. We now show that this really does have all the usual properties of addition.

Example $1 + 1 = 2$:

$$\begin{aligned} 1 + 1 &= \mathrm{add}(\langle sz, sz \rangle) && \text{(change of notation)} \\ &= e_{\mathbb{N}} \circ (\mathrm{id} \times u_+) \circ \langle sz, sz \rangle && \text{(definition of add)} \\ &= e_{\mathbb{N}} \circ \langle sz, u_+ sz \rangle && \text{(Lemma 2.3)} \\ &= e_{\mathbb{N}} \circ \langle sz, s^{\mathbb{N}} u_+ z \rangle && \text{(diagram defining } u_+) \\ &= e_{\mathbb{N}} \circ \langle sz, s^{\mathbb{N}} \pi_0^\sharp \rangle && \text{(diagram defining } u_+) \\ &= e_{\mathbb{N}} \circ (\mathrm{id} \times s^{\mathbb{N}}) \circ (\mathrm{id} \times \pi_0^\sharp) \circ \langle sz, \mathrm{id} \rangle && \text{(Lemma 2.3)} \\ &= s \circ e_{\mathbb{N}} \circ (\mathrm{id} \times \pi_0^\sharp) \circ \langle sz, \mathrm{id} \rangle && \text{(diagram defining } s^{\mathbb{N}}) \\ &= s \circ \pi_0 \circ \langle sz, \mathrm{id} \rangle && \text{(diagram defining } \pi_0^\sharp) \\ &= s \circ sz && \text{(Axiom 4)} \\ &= 2 && \text{(definition of 2)} \end{aligned}$$

Many of the other proofs in this paper consist of applications of similar proof steps to those used above, particularly applying the definition of add and u_+, and applying Cartesian product lemmas such as Lemma 2.3. We thus omit annotation of proof steps in aligned proofs after this point, to avoid needless repetition.

3.2 Properties of Addition

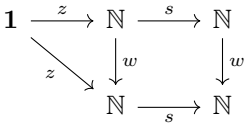
Having defined addition on the naturals, we should now verify that add behaves like ordinary addition. We show that add is commutative, associative, and respects zero and the successor operator.

Respects Zero on Right: First we show that $m + 0 = m$.

$$\begin{aligned} m + 0 &= \mathrm{add}(\langle m, z\rangle) \\ &= e_{\mathbb{N}} \circ (\mathrm{id} \times u_+) \circ \langle m, z\rangle \\ &= e_{\mathbb{N}} \circ \langle m, u_+ z\rangle \\ &= e_{\mathbb{N}} \circ \langle m, \pi_0^\sharp\rangle \\ &= e_{\mathbb{N}} \circ (\mathrm{id} \times \pi_0^\sharp)\langle m, u_+ z\rangle \\ &= \pi_0 \langle m, u_+ z\rangle \\ &= m \end{aligned}$$

This proof only relied on unraveling definitions, however often we will need to use induction as in the next lemma.

Respects Zero on Left: Now we show that $0+n = n$. Consider the following diagram:



From Axiom 9 there is a unique $w : \mathbb{N} \to \mathbb{N}$ such that $w(z) = z$ and $ws = sw$. Consider the function $\mathrm{add} \circ \langle z\beta_{\mathbb{N}}, \mathrm{id}\rangle : \mathbb{N} \to \mathbb{N}$. From the fact that $m + 0 = m$ we have that

$$\mathrm{add} \circ \langle z\beta_{\mathbb{N}}, \mathrm{id}\rangle(z) = \mathrm{add} \circ \langle z(\beta_{\mathbb{N}} z), z\rangle = \mathrm{add} \circ \langle z, z\rangle = z$$

We also have that:

$$\begin{aligned} &(\mathrm{add} \circ \langle z\beta_{\mathbb{N}}, \mathrm{id}\rangle) \circ s \\ &= \mathrm{add} \circ \langle z\beta_{\mathbb{N}} s, s\rangle \\ &= \mathrm{add} \circ \langle z\beta_{\mathbb{N}}, s\rangle \\ &= e_{\mathbb{N}} \circ (\mathrm{id} \times u_+) \circ \langle z\beta_{\mathbb{N}}, s\rangle \\ &= e_{\mathbb{N}} \circ \langle z\beta_{\mathbb{N}}, us\rangle \\ &= e_{\mathbb{N}} \circ \langle z\beta_{\mathbb{N}}, s^{\mathbb{N}} u_+\rangle \\ &= e_{\mathbb{N}} \circ (\mathrm{id} \times s^{\mathbb{N}}) \circ \langle z\beta_{\mathbb{N}}, u_+\rangle \\ &= s \circ e_{\mathbb{N}} \circ \langle z\beta_{\mathbb{N}}, u_+\rangle \\ &= s \circ e_{\mathbb{N}} \circ (\mathrm{id} \times u) \circ \langle z\beta_{\mathbb{N}}, \mathrm{id}\rangle \\ &= s \circ (\mathrm{add} \circ \langle z\beta_{\mathbb{N}}, \mathrm{id}\rangle) \end{aligned}$$

We have that $\mathrm{add} \circ \langle z\beta_{\mathbb{N}}, \mathrm{id}\rangle$ satisfies the same properties as w, so $w = \mathrm{add} \circ \langle z\beta_{\mathbb{N}}, \mathrm{id}\rangle$. However, it is also clear that $\mathrm{id}(z) = z$ and $\mathrm{id} \circ s = s = s \circ \mathrm{id}$, so $w = \mathrm{id}$. We thus have that $\mathrm{add} \circ \langle z\beta_{\mathbb{N}}, \mathrm{id}\rangle = \mathrm{id}$ so, for any $n \in \mathbb{N}$:

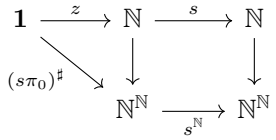
$$0 + n = \mathrm{add} \circ \langle z, n\rangle = \mathrm{add} \circ \langle z\beta_{\mathbb{N}} n, n\rangle = \mathrm{add} \circ \langle z\beta_{\mathbb{N}}, \mathrm{id}\rangle \circ n = \mathrm{id} \circ n = n.$$

While the above lemma closely follows our strategy discussed above by setting $g = \mathrm{add} \circ \langle z\beta_{\mathbb{N}}, \mathrm{id}\rangle$ and $f = \mathrm{id}$, the next example is more technical and presents a general technique of composing flat and sharp together.

Commutes Successor ($m + S(n) = S(m) + n$): Before we can generally establish that $m + S(n) = S(m) + n$, we must first show that $m + S(n) = S(m + n)$.

$$\begin{aligned} m + S(n) &= \mathrm{add}(\langle m, sn\rangle) \\ &= e_{\mathbb{N}}(\mathrm{id} \times u_+)\langle m, sn\rangle \\ &= e_{\mathbb{N}}\langle m, u_+ sn\rangle \\ &= e_{\mathbb{N}}\langle m, s^{\mathbb{N}} u_+ n\rangle \\ &= e_{\mathbb{N}}(\mathrm{id} \times s^{\mathbb{N}})\langle m, u_+ n\rangle \\ &= s \circ e_{\mathbb{N}}\langle m, u_+ n\rangle \\ &= s \circ \mathrm{add}(\langle m, n\rangle) \\ &= S(m + n) \end{aligned}$$

Now we show that $m + S(n) = S(m) + n$.
Consider the following diagram †:



We aim to show that both $(\mathrm{add} \circ (\mathrm{id} \times s))^\sharp$ and $(\mathrm{add} \circ (s \times \mathrm{id}))^\sharp : \mathbb{N} \to \mathbb{N}^{\mathbb{N}}$ satisfy this diagram. First, consider that:

$$\begin{aligned} & e_{\mathbb{N}} \circ (\mathrm{id} \times ((\mathrm{add} \circ (\mathrm{id} \times s))^\sharp \circ z)) \\ &= e_{\mathbb{N}} \circ (\mathrm{id} \times (\mathrm{add} \circ (\mathrm{id} \times s))^\sharp) \circ (\mathrm{id} \times z) \\ &= \mathrm{add} \circ (\mathrm{id} \times s) \circ (\mathrm{id} \times z) \\ &= \mathrm{add} \circ (\mathrm{id} \times sz) \\ &= e_{\mathbb{N}} \circ (\mathrm{id} \times u_+) \circ (\mathrm{id} \times sz) \\ &= e_{\mathbb{N}} \circ (\mathrm{id} \times u_+ sz) \\ &= e_{\mathbb{N}} \circ (\mathrm{id} \times s^{\mathbb{N}} u_+ z) \\ &= e_{\mathbb{N}} \circ (\mathrm{id} \times s^{\mathbb{N}} \pi_0^\sharp) \\ &= s \circ e_{\mathbb{N}} \circ (\mathrm{id} \times \pi_0^\sharp) \\ &= s \circ \pi_0 \end{aligned}$$

This satisfies the same property as $(s\pi_0)^\sharp$ so we have, by Axiom 10, that

$$(s\pi_0)^\sharp = [\mathrm{add} \circ (\mathrm{id} \times s)]^\sharp \circ z.$$

We have shown that the triangle commutes under $[\mathrm{add} \circ (\mathrm{id} \times s)]^\sharp$. Now we show that it makes the square commute as well. To this end we first show that $s \circ \mathrm{add} \circ (\mathrm{id} \times s) = \mathrm{add} \circ (\mathrm{id} \times s) \circ (\mathrm{id} \times s)$.

Let $\langle m, n\rangle \in \mathbb{N} \times \mathbb{N}$ be an arbitrary element then

$$\begin{aligned}(s \circ \text{add} \circ (\text{id} \times s))\,\langle m, n\rangle &= s \circ \text{add}\langle m, sn\rangle \\ &= S(m + S(n)) = m + S(S(n)) \\ &= \text{add}\langle m, ssn\rangle \\ &= \text{add} \circ (\text{id} \times s)\langle m, sn\rangle \\ &= [\text{add} \circ (\text{id} \times s) \circ (\text{id} \times s)]\,\langle m, n\rangle\end{aligned}$$

It follows by Axiom 2 that $s \circ \text{add} \circ (\text{id} \times s) = \text{add} \circ (\text{id} \times s) \circ (\text{id} \times s)$.

Now we observe that, by Lemmas 2.13 and 2.17,

$$s \circ \text{add} \circ (\text{id} \times s) = \Big((s \circ \text{add})^\sharp\Big)^\flat \circ (\text{id} \times s) = \Big[(\text{add} \circ (\text{id} \times s))^\sharp \circ s\Big]^\flat$$

and by taking sharps of both sides we arrive at

$$(\text{add} \circ (\text{id} \times s))^\sharp \circ s = [s \circ \text{add} \circ (\text{id} \times s)]^\sharp = s^{\mathbb{N}}\,[\text{add} \circ (\text{id} \times s)]^\sharp$$

This proves that $(\text{add} \circ (\text{id} \times s))^\sharp$ makes the square commute and hence satisfies the entire diagram. Now we would like to show that $(\text{add} \circ (s \times \text{id}))^\sharp$ satisfies this as well. To this end, consider an arbitrary element $\langle n, \text{id}\rangle$ of $N \times \mathbf{1}$.

$$\begin{aligned}&e_{\mathbb{N}} \circ (\text{id} \times ((\text{add} \circ (s \times \text{id}))^\sharp \circ z)) \circ \langle n, \text{id}\rangle \\ &= e_{\mathbb{N}} \circ (\text{id} \times (\text{add} \circ (s \times \text{id}))^\sharp) \circ (\text{id} \times z) \circ \langle n, \text{id}\rangle \\ &= e_{\mathbb{N}} \circ (\text{id} \times (\text{add} \circ (s \times \text{id}))^\sharp) \circ \langle n, z\rangle \\ &= \text{add} \circ (s \times \text{id}) \circ \langle n, z\rangle \\ &= \text{add}\langle sn, z\rangle \\ &= sn \\ &= s\pi_0\langle n, \text{id}\rangle\end{aligned}$$

It follows by Axiom 2 that $e_{\mathbb{N}} \circ \Big(\text{id} \times ([\text{add} \circ (s \times \text{id})]^\sharp \circ z)\Big) = s\pi_0$. This satisfies the same property as $(s\pi_0)^\sharp$ so, by Axiom 10, $(s\pi_0)^\sharp = (\text{add} \circ (s \times \text{id}))^\sharp \circ z$. In other words, $[\text{add} \circ (s \times \text{id})]^\sharp$ makes the triangle commute; all that remains to show is that $[\text{add} \circ (s \times \text{id})]^\sharp$ makes the square commute as well.

We essentially only have to prove the dual results as before. Let $\langle m, n\rangle \in \mathbb{N} \times \mathbb{N}$ be arbitrary then

$$\begin{aligned}(s \circ \text{add} \circ (s \times \text{id}))\,\langle m, n\rangle &= s \circ \text{add}\langle sm, n\rangle \\ &= S(S(m) + n) = S(m) + S(n) \\ &= \text{add}\langle sm, sn\rangle \\ &= \text{add} \circ (s \times s)\langle m, n\rangle\end{aligned}$$

it follows from Axiom 2 that $(s \circ \text{add} \circ (s \times \text{id})) = \text{add} \circ (s \times s)$.

Again we observe that

$$\begin{aligned} s \circ \text{add} \circ (s \times \text{id}) = \text{add} \circ (s \times s) &= [\text{add} \circ (s \times \text{id})]^{\sharp\flat} \circ (\text{id} \times s) \\ &= \left[(\text{add} \circ (s \times \text{id}))^{\sharp} \circ s \right]^{\flat} \end{aligned}$$

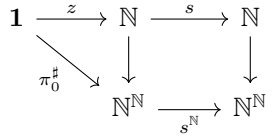
and by taking sharps we arrive at

$$[\text{add} \circ (s \times \text{id})]^{\sharp} \circ s = [s \circ \text{add} \circ (s \times \text{id})]^{\sharp} = s^{\mathbb{N}} \circ [\text{add} \circ (s \times \text{id})]^{\sharp}$$

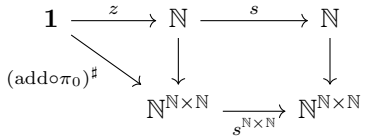
We conclude, therefore, that *both* $(\text{add} \circ (\text{id} \times s))^{\sharp}$ and $(\text{add} \circ (s \times \text{id}))^{\sharp}$ satisfy diagram † it follows that $(\text{add} \circ (\text{id} \times s))^{\sharp} = (\text{add} \circ (s \times \text{id}))^{\sharp}$, hence $\text{add} \circ (\text{id} \times s) = \text{add} \circ (s \times \text{id})$. Finally, we arrive at

$$\begin{aligned} S(a) + b &= \text{add}\langle sa, b\rangle \\ &= \text{add}(s \times \text{id})\langle a, b\rangle \\ &= \text{add}(\text{id} \times s)\langle a, b\rangle \\ &= \text{add}\langle a, sb\rangle \\ &= a + S(b) \end{aligned}$$

To summarize, we have proven that $S(m) + n = m + S(n) = S(m + n)$.
Commutative: Consider the diagram



It can be shown that $(\text{add} \circ \langle \pi_1, \pi_0 \rangle)^{\sharp}$ is precisely the function which satisfies this diagram. By using the previous result it is straight forward albeit tedious to show. Importantly, since the above is the defining diagram for u_+ it follows that addition is commutative.
Associative: Consider the following commuting diagram.



By showing that both $(\text{add} \circ (\text{add} \times \text{id}))^{\sharp}$ and $(\text{add} \circ (\text{id} \times \text{add}) \circ \langle \pi_0 \pi_0, \langle \pi_1 \pi_0, \pi_1 \rangle \rangle)^{\sharp}$ satisfy this diagram, associativity can easily be shown.
Cancellative ($a + c = b + c \implies a + b$): We aim to show

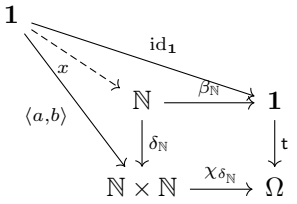
$$a + c = b + c \iff a = b$$

by constructing functions $\mathbb{N} \to \Omega^{\mathbb{N} \times \mathbb{N}}$ representing each side, and showing that they both satisfy the same Axiom 9 diagram and so are equal. The input to these functions is taken to represent the variable c, so that we effectively prove the above fact by induction on c. We can represent equality of natural numbers by the function $\chi_{\delta_{\mathbb{N}}} : \mathbb{N} \times \mathbb{N} \to \Omega$, which is the characteristic function of $\delta_{\mathbb{N}} = \langle \text{id}_{\mathbb{N}}, \text{id}_{\mathbb{N}} \rangle$, and we have, for any $a, b \in \mathbb{N}$,

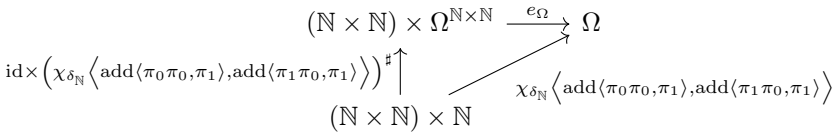
$$a = b \iff \chi_{\delta_{\mathbb{N}}} \circ \langle a, b \rangle = \mathsf{t}$$

This follows from the pullback diagram below, which we obtain from Axiom 8. The forward implication follows from the commuting square on the bottom-right. Explicitly, if $a = b$ then we have $\chi_{\delta_\mathbb{N}}\langle a, b\rangle = \chi_{\delta_\mathbb{N}}\langle a, a\rangle = \chi_{\delta_\mathbb{N}}\delta(a) = \mathtt{t}\beta_X(a) = \mathtt{t}$. Conversely, if $\chi_{\delta_\mathbb{N}} \circ \langle a, b\rangle = \mathtt{t}$ then, from the pullback, we have a function $x : 1 \to \mathbb{N}$ with $\langle a, b\rangle = \delta_\mathbb{N}(x)$, and then

$$\begin{aligned} a &= \pi_0\langle a, b\rangle = \pi_0\delta(x) = \pi_0\langle \mathrm{id}_X, \mathrm{id}_X\rangle \circ x \\ &= \mathrm{id}_X(x) \\ &= \pi_1\langle \mathrm{id}_X, \mathrm{id}_X\rangle \circ x = \pi_1\delta(x) = \pi_1\langle a, b\rangle = b \end{aligned}$$

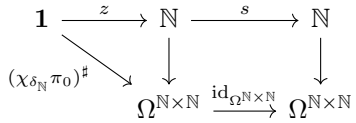


We can then represent the equation predicate $a + c = b + c$ by the function $(\chi_{\delta_\mathbb{N}}\langle \mathrm{add}\langle\pi_0\pi_0, \pi_1\rangle, \mathrm{add}\langle\pi_1\pi_0, \pi_1\rangle\rangle)^\sharp$, which satisfies the following diagram:



The corresponding function representing $a = b$ is simply $(\chi_{\delta_\mathbb{N}}\pi_0)^\sharp$, discarding the c parameter.

We then choose the functions for Axiom 9 that these functions satisfy. The function $q : \mathbf{1} \to \Omega^{\mathbb{N}\times\mathbb{N}}$ should be $(\chi_{\delta_\mathbb{N}}\pi_0)^\sharp$, since $a + 0 = b + 0$ is true precisely when $a = b$. The function $f : \Omega^{\mathbb{N}\times\mathbb{N}} \to \Omega^{\mathbb{N}\times\mathbb{N}}$ should be $\mathrm{id}_{\Omega^{\mathbb{N}\times\mathbb{N}}}$, since adding one to each side does not change the truth of the equation. We are thus seeking for the functions to satisfy the following diagram:



The successor case for $(\chi_{\delta_\mathbb{N}}\langle \mathrm{add}\langle\pi_0\pi_0, \pi_1\rangle, \mathrm{add}\langle\pi_1\pi_0, \pi_1\rangle\rangle)^\sharp$ follows from the fact s is a monomorphism. The other cases are relatively trivial. We thus have that

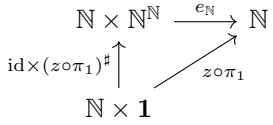
$$\begin{aligned} (\chi_{\delta_\mathbb{N}}\langle \mathrm{add}\langle\pi_0\pi_0, \pi_1\rangle, \mathrm{add}\langle\pi_1\pi_0, \pi_1\rangle\rangle)^\sharp &= (\chi_{\delta_\mathbb{N}}\pi_0)^\sharp \\ \chi_{\delta_\mathbb{N}}\langle \mathrm{add}\langle\pi_0\pi_0, \pi_1\rangle, \mathrm{add}\langle\pi_1\pi_0, \pi_1\rangle\rangle &= \chi_{\delta_\mathbb{N}}\pi_0 \\ \chi_{\delta_\mathbb{N}}\langle \mathrm{add}\langle\pi_0\pi_0, \pi_1\rangle, \mathrm{add}\langle\pi_1\pi_0, \pi_1\rangle\rangle\langle\langle a, b\rangle, c\rangle &= \chi_{\delta_\mathbb{N}}\pi_0\langle\langle a, b\rangle, c\rangle \text{ for any } a, b, c \in \mathbb{N} \\ \chi_{\delta_\mathbb{N}}\langle \mathrm{add}\langle a, c\rangle, \mathrm{add}\langle b, c\rangle\rangle &= \chi_{\delta_\mathbb{N}}\langle a, b\rangle \text{ for any } a, b, c \in \mathbb{N} \end{aligned}$$

Then, from the property of $\chi_{\delta_{\mathbb{N}}}$ discussed above, we have for any $a, b, c \in \mathbb{N}$:

$$\begin{aligned} \mathrm{add}\langle a, c\rangle = \mathrm{add}\langle b, c\rangle &\iff \chi_{\delta_{\mathbb{N}}}\big\langle \mathrm{add}\langle a, c\rangle, \mathrm{add}\langle b, c\rangle\big\rangle = \mathsf{t} = \chi_{\delta_{\mathbb{N}}}\langle a, b\rangle \\ &\iff a = b \end{aligned}$$

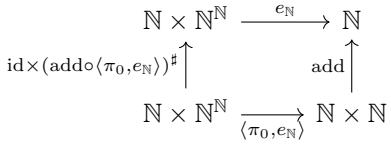
3.3 Multiplication on Naturals To define multiplication, we use a similar approach to that used to define addition, but we choose different functions $q : \mathbf{1} \to \mathbb{N}^{\mathbb{N}}$ and $f : \mathbb{N}^{\mathbb{N}} \to \mathbb{N}^{\mathbb{N}}$, to define a $u_* : \mathbb{N} \to \mathbb{N}^{\mathbb{N}}$ that represents a "multiply by n" function $n \mapsto (\lambda m.\ m \cdot n)$.

For q we need a function that represents multiplying by zero. Since the result of any multiplication by zero is zero, we simply need to lift z into an element of $\mathbb{N}^{\mathbb{N}}$. That can be achieved by using the function $(z \circ \pi_1)^\sharp$, which satisfies the following diagram by Axiom 10.

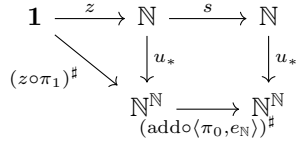


From the diagram, the application of $(z \circ \pi_1)^\sharp$ using $e_{\mathbb{N}}$ results in discarding the input (using π_1) and outputting a constant z. Thus, $(z \circ \pi_1)^\sharp$ represents the function that always outputs zero.

For f we need a function that transforms a "multiply by n" function $(\lambda m.\ n \cdot m)$ into a "multiply by $n + 1$" function $(\lambda m.\ (n + 1) \cdot m)$. This can be achieved by first taking a copy of the input to the function (m) using π_0, while also applying the function using $e_{\mathbb{N}}$ to its ifnput to obtain $n \cdot m$. The add function can then be applied to these two components to obtain $n \cdot m + m = (n + 1) \cdot m$. Combining these and applying the transpose, we obtain $(\mathrm{add} \circ \langle \pi_0, e_{\mathbb{N}}\rangle)^\sharp : \mathbb{N}^{\mathbb{N}} \to \mathbb{N}^{\mathbb{N}}$, which satisfies the diagram below.



We then plug $q = (z \circ \pi_1)^\sharp$ and $f = (\mathrm{add} \circ \langle \pi_0, e_{\mathbb{N}}\rangle)^\sharp$ into Axiom 9 to obtain the unique $u_* : \mathbb{N} \to \mathbb{N}^{\mathbb{N}}$ that satisfies the following diagram.



For each $n \in \mathbb{N}$, $u_* \circ n$ then represents a "multiply by n" function. We then define a two-argument multiplication function $\mathrm{mult} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by $\mathrm{mult} = e_{\mathbb{N}} \circ (\mathrm{id} \times u_*)$.

3.4 Properties of Multiplication All the usual properties of multiplication hold for our mult function. We sketch the proof of each of them in turn.

Respects Zero to the Right: We have that multiplying by zero on the right yields zero. This follows by a straightforward calculation, since we defined multiplication such that this would hold.

$$\begin{aligned} m \cdot 0 &= \mathrm{mult}(\langle m, z\rangle) \\ &= e_{\mathbb{N}}(\mathrm{id} \times u_*)\langle m, z\rangle \\ &= e_{\mathbb{N}}\langle m, u_* z\rangle \\ &= e_{\mathbb{N}}\langle m, (z \circ \pi_1)^\sharp\rangle \\ &= e_{\mathbb{N}}(\mathrm{id} \times (z \circ \pi_1)^\sharp)\langle m, \mathrm{id}\rangle \\ &= z \circ \pi_1 \langle m, \mathrm{id}\rangle \\ &= 0 \end{aligned}$$

Respects Successor to the Right: We have that multiplication of m by the successor of a number n is the same as multiplying m by n and then adding another m. Again, this is a straightforward calculation as it is part of our definition of multiplication.

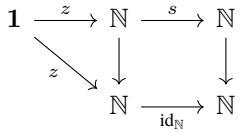
$$\begin{aligned} m \cdot S(n) &= \mathrm{mult}\left(\langle m, sn\rangle\right) \\ &= e_{\mathbb{N}}(\mathrm{id} \times u_*)\langle m, sn\rangle \\ &= e_{\mathbb{N}}\langle m, u_* sn\rangle \\ &= e_{\mathbb{N}}\langle m, (\mathrm{add} \circ \langle \pi_0, e_{\mathbb{N}}\rangle)^\sharp\, u_* n\rangle \\ &= e_{\mathbb{N}}(\mathrm{id} \times [\mathrm{add} \circ \langle \pi_0, e_{\mathbb{N}}\rangle]^\sharp)\langle m, u_* n\rangle \\ &= \mathrm{add}\langle \pi_0, e_{\mathbb{N}}\rangle\langle m, u_* n\rangle \\ &= \mathrm{add}\left\langle m, e_{\mathbb{N}}(\mathrm{id} \times u_*)\langle m, n\rangle\right\rangle \\ &= \mathrm{add}\left\langle m, \mathrm{mult}\langle m, n\rangle\right\rangle \\ &= m + (m \cdot n) \end{aligned}$$

$S(0)$ *is the Right Identity:* The fact that one is the right identity of multiplication then follows from the two facts above:

$$a \cdot S(0) = a + (a \cdot 0) = a + 0 = a$$

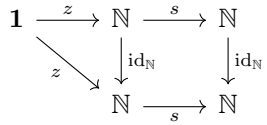
It is worth taking a moment to appreciate that this is our first interesting identity which does not ostensibly rely on facts from ETCS. Of course each step in the computation has ETCS working "in the background".

Respects Zero to the Left: Let $n \in \mathbb{N}$ be arbitrary and consider the diagram



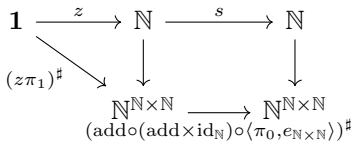
It can be shown that $\mathrm{mult}\langle \mathrm{id}_{\mathbb{N}}, z\beta_{\mathbb{N}}\rangle$ and $\mathrm{mult}\langle z\beta_{\mathbb{N}}, \mathrm{id}_{\mathbb{N}}\rangle$ both satisfy this diagram. We thus have that $0 \cdot m = m \cdot 0 = 0$, since we have already established that multiplication respects zero on the right.

$S(0)$ *is the Left Identity:* Consider the following diagram:



It can be shown that $\mathrm{mult} \circ \langle sz\beta_{\mathbb{N}}, \mathrm{id}_{\mathbb{N}} \rangle$ also satisfies this diagram, so that it is equal to $\mathrm{id}_{\mathbb{N}}$.

Left Distributivity ($(a+b) \cdot c = a \cdot c + b \cdot c$*)* Consider the following diagram:



It can be shown that

- $f = (\mathrm{mult} \circ (\mathrm{add} \times \mathrm{id}_{\mathbb{N}}))^\sharp$
- $g = (\mathrm{add}\langle \mathrm{mult}\langle \pi_0\pi_0, \pi_1 \rangle, \mathrm{mult}\langle \pi_1\pi_0, \pi_1 \rangle)^\sharp$

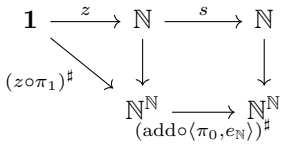
both satisfy this diagram.

Respects Successor to the Left:

$$m + n \cdot m = S(0) \cdot m + n \cdot m = (S(0) + n)\, m = (S(0 + n))\, m = S(n) \cdot m$$

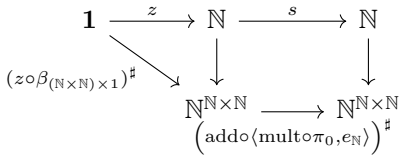
Note, in particular, $S(n) = S(n) \cdot 1 = 1 + n \cdot 1 = 1 + n$.

Commutative: Consider the diagram from the definition of multiplication:



It can be shown that $\big(\mathrm{mult} \circ \langle \pi_1, \pi_0 \rangle\big)^\sharp$ (where $\pi_1, \pi_0 : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$) also satisfies this diagram.

Associative: Consider the following diagram (where $\pi_0 : (\mathbb{N} \times \mathbb{N}) \times \mathbb{N}^{\mathbb{N} \times \mathbb{N}} \to \mathbb{N} \times \mathbb{N}$):



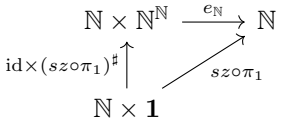
It can be shown that

- $f = \big(\mathrm{mult} \circ (\mathrm{mult} \times \mathrm{id})\big)^\sharp$
- $g = \big(\mathrm{mult} \circ (\mathrm{id} \times \mathrm{mult}) \circ \langle \pi_0\pi_0, \langle \pi_1\pi_0, \pi_1 \rangle \rangle\big)^\sharp$

both satisfy this diagram.

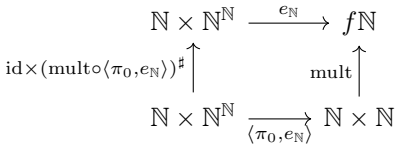
3.5 Exponentiation on Naturals We construct exponentiation in terms of multiplication in a similar way to the definition of multiplication in terms of addition. We first choose an appropriate function $q : \mathbf{1} \to \mathbb{N}^{\mathbb{N}}$ to represent the function raising a natural

number to the power of zero. The result of raising a number to the power of zero is always one, so we use $q = (sz \circ \pi_1)^\sharp$, defined by the following diagram.



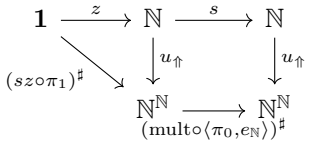
Here, the input of zero is taken as the second argument to the exponentiation, while the first argument is provided when $e_{\mathbb{N}}$ is applied. This matches the ordering of the arguments in the diagram.

Next, we choose $f : \mathbb{N}^{\mathbb{N}} \to \mathbb{N}^{\mathbb{N}}$ describing what happens when we increase the exponent by one. For this, we want to evaluate the exponentiation so far, then take a copy of the first argument to the exponentiation and multiply it on. That is achieved by taking $f = (\mathrm{mult} \circ \langle \pi_0, e_{\mathbb{N}} \rangle)^\sharp$, which satisfies the following diagram.



The construction is similar to the corresponding function in the definition of mult, but we use mult in the definition here instead of add.

Putting these into Axiom 9, we obtain a unique function $u_{\Uparrow} : \mathbb{N} \to \mathbb{N}^{\mathbb{N}}$ that satisfies the following diagram.



We then define a function $\exp : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by $\exp = u_{\Uparrow}^\flat = e_{\mathbb{N}} \circ (\mathrm{id}_{\mathbb{N}} \times u_{\Uparrow})$.

3.6 Properties of Exponentiation As with addition and multiplication, exponentiation also fulfils all the properties we expect of it.f Exponentiation is our first noncommutative operator, so we have separate results giving properties for each of its arguments. *Respects Zero on the Left ($n^0 = 1$):* We have that raising any number to the power of zero yields one. This follows by a straightforward calculation as it is part of our

definition of exponentiation.

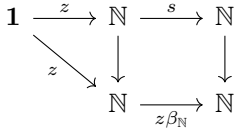
$$\begin{aligned}
n^0 &= \exp \circ \langle n, z \rangle \\
&= e_{\mathbb{N}} \circ (\mathrm{id}_{\mathbb{N}} \times u_{\Uparrow}) \circ \langle n, z \rangle \\
&= e_{\mathbb{N}} \circ \langle n, u_{\Uparrow} z \rangle \\
&= e_{\mathbb{N}} \circ \langle n, (sz \circ \pi_1)^\sharp \rangle \\
&= e_{\mathbb{N}} \circ (\mathrm{id}_{\mathbb{N}} \times (sz \circ \pi_1)^\sharp) \circ \langle n, \mathrm{id}_{\mathbb{N}} \rangle \\
&= sz \circ \pi_1 \circ \langle n, \mathrm{id}_{\mathbb{N}} \rangle \\
&= sz \circ \mathrm{id}_{\mathbb{N}} \\
&= sz \\
&= 1
\end{aligned}$$

Note, in particular, that $0^0 = 1$.

Respects One on the Left ($n^1 = n$): We also have that raising n to the power of one yields n. This is again a straightforward calculation, but a longer one, since fwe must apply both of the equalities defining our exponentiation operator.

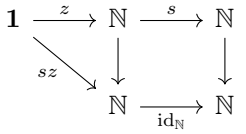
$$\begin{aligned}
n^1 &= \exp \circ \langle n, sz \rangle \\
&= e_{\mathbb{N}} \circ (\mathrm{id}_{\mathbb{N}} \times u_{\Uparrow}) \circ \langle n, sz \rangle \\
&= e_{\mathbb{N}} \circ \langle n, u_{\Uparrow} sz \rangle \\
&= e_{\mathbb{N}} \circ \langle n, (\mathrm{mult} \circ \langle \pi_0, e_{\mathbb{N}} \rangle)^\sharp u_{\Uparrow} z \rangle \\
&= e_{\mathbb{N}} \circ \langle n, (\mathrm{mult} \circ \langle \pi_0, e_{\mathbb{N}} \rangle)^\sharp (sz \circ \pi_1)^\sharp \rangle \\
&= e_{\mathbb{N}} \circ (\mathrm{id}_{\mathbb{N}} \times (\mathrm{mult} \circ \langle \pi_0, e_{\mathbb{N}} \rangle)^\sharp) \circ \langle n, (sz \circ \pi_1)^\sharp \rangle \\
&= \mathrm{mult} \circ \langle \pi_0, e_{\mathbb{N}} \rangle \circ \langle n, (sz \circ \pi_1)^\sharp \rangle \\
&= \mathrm{mult} \circ \langle \pi_0 \circ \langle n, (sz \circ \pi_1)^\sharp \rangle, e_{\mathbb{N}} \circ \langle n, (sz \circ \pi_1)^\sharp \rangle \rangle \\
&= \mathrm{mult} \circ \langle n, e_{\mathbb{N}} \circ \langle n, (sz \circ \pi_1)^\sharp \rangle \rangle \\
&= \mathrm{mult} \circ \langle n, e_{\mathbb{N}} \circ (\mathrm{id}_{\mathbb{N}} \times (sz \circ \pi_1)^\sharp) \circ \langle n, \mathrm{id}_{\mathbb{N}} \rangle \rangle \\
&= \mathrm{mult} \circ \langle n, sz \circ \pi_1 \circ \langle n, \mathrm{id}_{\mathbb{N}} \rangle \rangle \\
&= \mathrm{mult} \circ \langle n, sz \circ \mathrm{id}_{\mathbb{N}} \rangle \\
&= \mathrm{mult} \circ \langle n, sz \rangle \\
&= n \cdot 1 \\
&= n
\end{aligned}$$

Respects Zero on the Right ($0^{S(n)} = 0$): To show that raising zero to a nonzero power also yields zero, we must apply induction using Axiom 9, since we have an arbitrary value in the second argument. Consider the following commuting diagram:



It can be shown that $z\beta_{\mathbb{N}}$ and $\exp \circ \langle z\beta_{\mathbb{N}}, s \rangle$ both satisfy this diagram.

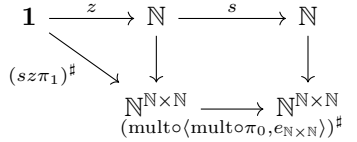
Respects One on the Right ($1^n = 1$): Similar to the previous proof, we must apply induction to show that raising one to any power yields one. Consider the following commuting diagram:



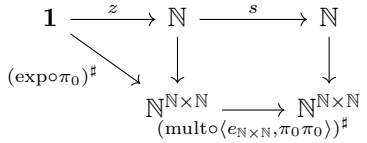
It can be shown that both $sz\beta_{\mathbb{N}}$ and $\exp \circ \langle sz\beta_{\mathbb{N}}, \mathrm{id}_{\mathbb{N}} \rangle$ satisfy this diagram.
Respects Successor ($a \cdot a^b = a^{S(b)}$): We have that adding one to an exponent is the same as multiplying. This follows by a straightforward proof, as for exponentiation respecting zero, since it forms part of our definition of exponentiation.

$$\begin{aligned}
m^{S(n)} &= \exp\langle m, sn\rangle \\
&= e_{\mathbb{N}}(\mathrm{id} \times u_{\Uparrow})\langle m, sn\rangle \\
&= e_{\mathbb{N}}(\mathrm{id} \times u_{\Uparrow} s)\langle m, n\rangle \\
&= e_{\mathbb{N}}\big(\mathrm{id} \times [\mathrm{mult}\langle \pi_0, e_{\mathbb{N}}\rangle]^\sharp u_{\Uparrow}\big)\langle m, n\rangle \\
&= e_{\mathbb{N}}\big(\mathrm{id} \times [\mathrm{mult}\langle \pi_0, e_{\mathbb{N}}\rangle]^\sharp\big)\langle m, u_{\Uparrow} n\rangle \\
&= \mathrm{mult}\langle \pi_0, e_{\mathbb{N}}\rangle\langle m, u_{\Uparrow} n\rangle \\
&= \mathrm{mult}\langle m, e_{\mathbb{N}}\langle m, u_{\Uparrow} n\rangle\rangle \\
&= \mathrm{mult}\langle m, e_{\mathbb{N}}(\mathrm{id} \times u_{\Uparrow})\langle m, n\rangle\rangle \\
&= \mathrm{mult}\langle m, \exp\langle m, n\rangle\rangle \\
&= m \cdot m^n
\end{aligned}$$

Left Distributivity ($(n \cdot m)^k = n^k \cdot m^k$): We have that exponentiation of a product is a product of exponentiations. We prove this by induction on the exponent, considering the following diagram:



It can be shown that this is satisfied by the both of the functions $[\exp \circ (\mathrm{mult} \times \mathrm{id})]^\sharp$ and $[\mathrm{mult} \circ (\exp \times \exp) \circ \langle\langle \pi_0\pi_0, \pi_1\rangle, \langle \pi_1\pi_0, \pi_1\rangle\rangle]^\sharp$. The triangle in the diagram follows easily from the properties of zero. The square then follows from the successor case in our definition of exponentiation.
Right Distributivity ($n^{m+k} = n^m \cdot n^k$): We also have that raising something to a sum is the same as the product of two exponentiations. This is again proved by induction, taking the second element of the sum (k) as the induction variable. Consider the following diagram:



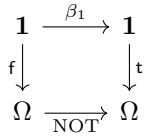
Similarly to left distributivity, both $[\exp \circ (\mathrm{id} \times \mathrm{add}) \circ \langle \pi_0 \pi_0, \langle \pi_1 \pi_0, \pi_1 \rangle \rangle]^\sharp$ and $[\mathrm{mult} \circ (\exp \times \exp) \circ \langle \langle \pi_0 \pi_0, \pi_1 \pi_0 \rangle, \langle \pi_0 \pi_0, \pi_1 \rangle \rangle]^\sharp$ satisfy this diagram. The triangle follows from a calculation using the properties of zero, as for left distributivity. For the square, we use the fact that exponentiation respects successor, proved above.

3.7 Comparison We define a less than comparison operator by constructing a function $\mathbb{N} \times \mathbb{N} \to \Omega$ that represents the following definition:

$$n \leq m \equiv \exists k \in \mathbb{N}.\ n + k = m$$

For this definition we require a function $\mathrm{EXISTS} : \Omega^{\mathbb{N}} \to \Omega$ that represents an existential quantifier. It is most convenient to define EXISTS in terms of the negation function $\mathrm{NOT} : \Omega \to \Omega$ and a universal quantifier $\mathrm{FORALL} : \Omega^{\mathbb{N}} \to \Omega$, using the fact that $\exists x.\ P(x) \equiv \neg \forall x.\ \neg P(x)$.

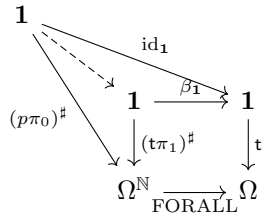
We obtain a $\mathrm{NOT} : \Omega \to \Omega$ function by taking the characteristic function of $\mathsf{f} : \mathbf{1} \to \Omega$, such that the following diagram is a pullback by Axiom 8:



It follows from this that $\mathrm{NOT}(\mathsf{f}) = \mathsf{t}$. We also have that $\mathrm{NOT}(\mathsf{t}) = \mathsf{f}$, since if it were equal to t then from the pullback property we have $\mathsf{t} = \mathsf{f}$ which is a contradiction. Therefore, $\mathrm{NOT}(\mathsf{t})$ is *not* t and hence equal to f.

To define the function $\mathrm{FORALL} : \Omega^{\mathbb{N}} \to \Omega$, we observe that if a function $\mathbb{N} \to \Omega$ is true for all inputs, then it is equal to a constant true function. If a function is equal to a constant true function, then there is a function corresponding to it that is in the singleton subset of $\Omega^{\mathbb{N}}$ containing the member of $\Omega^{\mathbb{N}}$ representing a constant true function. We can thus obtain FORALL by taking the characteristic function of that subset.

The constant true function in $\Omega^{\mathbb{N}}$ is represented by the function $(\mathsf{t}\pi_1)^\sharp : \mathbf{1} \to \Omega^{\mathbb{N}}$. Since this is a function from $\mathbf{1}$, it is a monomorphism and hence defines a subset. Axiom 8 then gives us a characteristic function for it, which we define to be FORALL, and, for any predicate $p : \mathbb{N} \to \Omega$, we have the following pullback:



Note that, for any predicate $p : \mathbb{N} \to \Omega$, we have that:

$$\begin{aligned}
&\mathrm{FORALL} \circ (p\pi_0)^\sharp = \mathtt{t} \\
&\iff (p\pi_0)^\sharp = (\mathtt{t}\pi_1)^\sharp \\
&\iff e_\Omega \circ (\mathrm{id} \times (p\pi_0)^\sharp) = e_\Omega \circ (\mathrm{id} \times (\mathtt{t}\pi_1)^\sharp) \\
&\iff p\pi_0 = \mathtt{t}\pi_1 \\
&\iff p\pi_0 = \mathtt{t}\beta_{\mathbb{N}}\pi_0 \\
&\iff p = \mathtt{t}\beta_{\mathbb{N}} \\
&\iff \forall n \in \mathbb{N}.\ p(n) = \mathtt{t}\beta_{\mathbb{N}}(n) \\
&\iff \forall n \in \mathbb{N}.\ p(n) = \mathtt{t}
\end{aligned}$$

We then define $\mathrm{EXISTS} = \mathrm{NOT} \circ \mathrm{FORALL} \circ \mathrm{NOT}^{\mathbb{N}} : \Omega^{\mathbb{N}} \to \Omega$. We then have, for any predicate $p : \mathbb{N} \to \Omega$:

$$\begin{aligned}
&\mathrm{EXISTS} \circ (p\pi_0)^\sharp = \mathtt{t} \\
&\iff \mathrm{NOT} \circ \mathrm{FORALL} \circ \mathrm{NOT}^{\mathbb{N}} \circ (p\pi_0)^\sharp = \mathtt{t} \\
&\iff \mathrm{NOT} \circ \mathrm{FORALL} \circ (\mathrm{NOT} \circ p\pi_0)^\sharp = \mathtt{t} \\
&\iff \mathrm{FORALL} \circ (\mathrm{NOT} \circ p\pi_0)^\sharp = \mathtt{f} \\
&\iff \neg\forall n \in \mathbb{N}.\ \mathrm{NOT} \circ p(n) = \mathtt{t} \\
&\iff \exists n \in \mathbb{N}.\ \mathrm{NOT} \circ p(n) = \mathtt{f} \\
&\iff \exists n \in \mathbb{N}.\ p(n) = \mathtt{t}
\end{aligned}$$

We have a general fact, suppose $\pi_0 : X \times \mathbf{1} \to X$ and $y \in Y$ and $f : X \times Y \to Z$ (and $f^\sharp : Y \to Z^X$) then

$$f^\sharp \circ y = (f \circ \langle \mathrm{id}_X, y\beta_X \rangle \circ \pi_0)^\sharp$$

To establish this, let $x \in X$ be arbitrary then

$$\begin{aligned}
&f \circ \langle \mathrm{id}_X, y\beta_X \rangle \circ \pi_0\langle x, \mathrm{id}_{\mathbf{1}} \rangle \\
&= f \circ \langle \mathrm{id}_X, y\beta_X \rangle x = f\langle x, y\beta_X x \rangle = f\langle x, y \rangle \\
&= f \circ (\mathrm{id}_X \times y) \circ \langle x, \mathrm{id}_{\mathbf{1}} \rangle = (f^\sharp \circ y)^\flat \circ \langle x, \mathrm{id}_{\mathbf{1}} \rangle
\end{aligned}$$

Since $\langle x, \mathrm{id}_{\mathbf{1}} \rangle$ was arbitrary it follows that $f \circ \langle \mathrm{id}_X, y\beta_X \rangle \circ \pi_0 = (f^\sharp \circ y)^\flat$; by taking sharps we arrive at the desired result.

With EXISTS in place, we can define $\leq_{\mathbb{N}} : \mathbb{N} \times \mathbb{N} \to \Omega$ by

$$\leq_{\mathbb{N}} = \mathrm{EXISTS} \circ (\chi_{\delta_{\mathbb{N}}} \langle \mathrm{add}\langle \pi_0, \pi_0\pi_1 \rangle, \pi_1\pi_1 \rangle)^\sharp$$

Commonly we will simply write $n \leq_{\mathbb{N}} m$ in place of $\leq_{\mathbb{N}} \langle n, m\rangle$ when the context is clear.

$$
\begin{aligned}
&\leq_{\mathbb{N}} \langle n, m\rangle = \mathsf{t} \\
&\iff \mathrm{EXISTS} \circ (\chi_{\delta_{\mathbb{N}}} \langle \mathrm{add}\langle \pi_0, \pi_0\pi_1\rangle, \pi_1\pi_1\rangle)^\sharp \circ \langle n, m\rangle = \mathsf{t} \\
&\iff \mathrm{EXISTS} \circ (\chi_{\delta_{\mathbb{N}}} \langle \mathrm{add}\langle \pi_0, \pi_0\pi_1\rangle, \pi_1\pi_1\rangle \circ \langle \mathrm{id}_{\mathbb{N}}, \langle n, m\rangle \beta_{\mathbb{N}}\rangle \circ \pi_0)^\sharp = \mathsf{t} \\
&\iff \exists k \in \mathbb{N}.\ \chi_{\delta_{\mathbb{N}}} \langle \mathrm{add}\langle \pi_0, \pi_0\pi_1\rangle, \pi_1\pi_1\rangle \circ \langle \mathrm{id}_{\mathbb{N}}, \langle n, m\rangle \beta_{\mathbb{N}}\rangle \circ k = \mathsf{t} \\
&\iff \exists k \in \mathbb{N}.\ \chi_{\delta_{\mathbb{N}}} \langle \mathrm{add}\langle \pi_0, \pi_0\pi_1\rangle, \pi_1\pi_1\rangle \circ \langle k, \langle n, m\rangle\rangle = \mathsf{t} \\
&\iff \exists k \in \mathbb{N}.\ \chi_{\delta_{\mathbb{N}}} \langle \mathrm{add}\langle k, n\rangle, m\rangle = \mathsf{t} \\
&\iff \exists k \in \mathbb{N}.\ \mathrm{add}\langle k, n\rangle = m
\end{aligned}
$$

$\leq_{\mathbb{N}}$ *is a Total order:* We now prove that $\leq_{\mathbb{N}}$ satisfies the following properties:

1. *Antisymmetry:* If $\leq_{\mathbb{N}} \langle n, m\rangle = \mathsf{t}$ and $\leq_{\mathbb{N}} \langle m, n\rangle = \mathsf{t}$ then $n = m$.
2. *Transitivity:* If $\leq_{\mathbb{N}} \langle n, m\rangle = \mathsf{t}$ and $\leq_{\mathbb{N}} \langle m, p\rangle = \mathsf{t}$ then $\leq_{\mathbb{N}} \langle n, p\rangle = \mathsf{t}$.
3. *Connexity:* $\leq_{\mathbb{N}} \langle n, m\rangle = \mathsf{t}$ or $\leq_{\mathbb{N}} \langle m, n\rangle = \mathsf{t}$.

For the first, suppose that $\leq_{\mathbb{N}} \langle n, m\rangle = \mathsf{t}$ and $\leq_{\mathbb{N}} \langle m, n\rangle = \mathsf{t}$ then there exists $k \in \mathbb{N}$ such that $k+n = m$ and there exists $j \in \mathbb{N}$ such that $j+m = n$. It follows that $0+m = m = k+n = k+j+m$, so that by the cancellation law we have $0 = k+j$. Now if $k \neq 0$ then $k = S(a)$ for some $a \in \mathbb{N}$[1], but then $0 = S(a)+j = S(a+j)$ and zero is not the successor of any natural number (Hatcher [4] proves this along with the other Peano postulates in ETCS). Therefore, $k = 0$ and $n = m$.

For the second, suppose that $\leq_{\mathbb{N}} \langle n, m\rangle = \mathsf{t}$ and $\leq_{\mathbb{N}} \langle m, p\rangle = \mathsf{t}$ then there exists $k \in \mathbb{N}$ such that $k + n = m$ and there exists $j \in \mathbb{N}$ such that $j + m = p$. It follows that $(j + k) + n = j + (k + n) = j + m = p$ so that $\leq_{\mathbb{N}} \langle n, p\rangle = \mathsf{t}$.

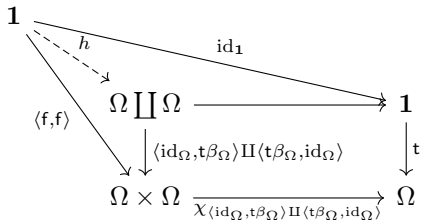
For the third, we want to first convert our logical "or" into an ETCS "OR". Hatcher defines OR as $\chi_{\langle \mathrm{id}_\Omega, \mathsf{t}\beta_\Omega\rangle \amalg \langle \mathsf{t}\beta_\Omega, \mathrm{id}_\Omega\rangle} : \Omega \times \Omega \to \Omega$. We now show that this function does in fact behave as you would suspect.

$$
\begin{aligned}
&\chi_{\langle \mathrm{id}_\Omega, \mathsf{t}\beta_\Omega\rangle \amalg \langle \mathsf{t}\beta_\Omega, \mathrm{id}_\Omega\rangle} \circ \langle \mathsf{t}, \star\rangle \\
&= \chi_{\langle \mathrm{id}_\Omega, \mathsf{t}\beta_\Omega\rangle \amalg \langle \mathsf{t}\beta_\Omega, \mathrm{id}_\Omega\rangle} \circ \langle \mathsf{t}\beta_\Omega, \mathrm{id}_\Omega\rangle \circ \star \\
&= \chi_{\langle \mathrm{id}_\Omega, \mathsf{t}\beta_\Omega\rangle \amalg \langle \mathsf{t}\beta_\Omega, \mathrm{id}_\Omega\rangle} \circ (\langle \mathrm{id}_\Omega, \mathsf{t}\beta_\Omega\rangle \amalg \langle \mathsf{t}\beta_\Omega, \mathrm{id}_\Omega\rangle) \circ i_1 \circ \star \\
&= \mathsf{t} \circ \beta_{\Omega \coprod \Omega} \circ i_1 \circ \star \\
&= \mathsf{t} \circ \mathrm{id}_{\mathbf{1}} \\
&= \mathsf{t} \\
&= \mathsf{t} \circ \beta_{\Omega \coprod \Omega} \circ i_0 \circ \star \\
&= \chi_{\langle \mathrm{id}_\Omega, \mathsf{t}\beta_\Omega\rangle \amalg \langle \mathsf{t}\beta_\Omega, \mathrm{id}_\Omega\rangle} \circ (\langle \mathrm{id}_\Omega, \mathsf{t}\beta_\Omega\rangle \amalg \langle \mathsf{t}\beta_\Omega, \mathrm{id}_\Omega\rangle) \circ i_0 \circ \star \\
&= \chi_{\langle \mathrm{id}_\Omega, \mathsf{t}\beta_\Omega\rangle \amalg \langle \mathsf{t}\beta_\Omega, \mathrm{id}_\Omega\rangle} \circ \langle \mathrm{id}_\Omega, \mathsf{t}\beta_\Omega\rangle \circ \star \\
&= \chi_{\langle \mathrm{id}_\Omega, \mathsf{t}\beta_\Omega\rangle \amalg \langle \mathsf{t}\beta_\Omega, \mathrm{id}_\Omega\rangle} \circ \langle \star, \mathsf{t}\rangle
\end{aligned}
$$

where $\star : \mathbf{1} \to \Omega$. The above computation shows that as long as *at least one* value in the argument is true then the full expression is true.

Now suppose that both of the arguments are false. We prove by contradiction that $\chi_{\langle \mathrm{id}_\Omega, \mathsf{t}\beta_\Omega\rangle \amalg \langle \mathsf{t}\beta_\Omega, \mathrm{id}_\Omega\rangle} \circ \langle \mathsf{f}, \mathsf{f}\rangle = \mathsf{f}$. Suppose that $\chi_{\langle \mathrm{id}_\Omega, \mathsf{t}\beta_\Omega\rangle \amalg \langle \mathsf{t}\beta_\Omega, \mathrm{id}_\Omega\rangle} \circ \langle \mathsf{f}, \mathsf{f}\rangle = \mathsf{t}$, then, from Axiom 8, we have $h : \mathbf{1} \to \Omega \coprod \Omega$ that satisfies the following commuting

diagram:



The only possible values for h are $i_0\mathsf{t}$, $i_0\mathsf{f}$, $i_1\mathsf{t}$, $i_1\mathsf{f}$, but from Axiom 5 we have:

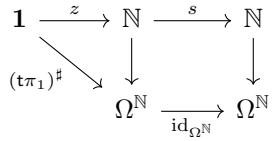
$$\begin{aligned}
(\langle \mathrm{id}_\Omega, \mathsf{t}\beta_\Omega\rangle \amalg \langle \mathsf{t}\beta_\Omega, \mathrm{id}_\Omega\rangle) \circ i_0\mathsf{t} &= \langle \mathrm{id}_\Omega, \mathsf{t}\beta_\Omega\rangle \circ \mathsf{t} = \langle \mathsf{t}, \mathsf{t}\rangle \\
(\langle \mathrm{id}_\Omega, \mathsf{t}\beta_\Omega\rangle \amalg \langle \mathsf{t}\beta_\Omega, \mathrm{id}_\Omega\rangle) \circ i_0\mathsf{f} &= \langle \mathrm{id}_\Omega, \mathsf{t}\beta_\Omega\rangle \circ \mathsf{f} = \langle \mathsf{f}, \mathsf{t}\rangle \\
(\langle \mathrm{id}_\Omega, \mathsf{t}\beta_\Omega\rangle \amalg \langle \mathsf{t}\beta_\Omega, \mathrm{id}_\Omega\rangle) \circ i_1\mathsf{t} &= \langle \mathsf{t}\beta_\Omega, \mathrm{id}_\Omega\rangle \circ \mathsf{t} = \langle \mathsf{t}, \mathsf{t}\rangle \\
(\langle \mathrm{id}_\Omega, \mathsf{t}\beta_\Omega\rangle \amalg \langle \mathsf{t}\beta_\Omega, \mathrm{id}_\Omega\rangle) \circ i_1\mathsf{f} &= \langle \mathsf{t}\beta_\Omega, \mathrm{id}_\Omega\rangle \circ \mathsf{t} = \langle \mathsf{t}, \mathsf{f}\rangle
\end{aligned}$$

Since none of these are equal to $\langle \mathsf{f}, \mathsf{f}\rangle$, this contradicts the diagram, so we have the desired result.

Connexity can then be defined in ETCS terms as:

$$\chi_{\langle \mathrm{id}_\Omega, \mathsf{t}\beta_\Omega\rangle \amalg \langle \mathsf{t}\beta_\Omega, \mathrm{id}_\Omega\rangle} \circ \left\langle \leq_{\mathbb{N}} \langle n, m\rangle, \leq_{\mathbb{N}} \langle m, n\rangle \right\rangle = \mathsf{t}$$

To show this, we show that $\left(\chi_{\langle \mathrm{id}_\Omega, \mathsf{t}\beta_\Omega\rangle \amalg \langle \mathsf{t}\beta_\Omega, \mathrm{id}_\Omega\rangle} \circ \langle \leq_{\mathbb{N}} \langle \pi_0, \pi_1\rangle, \leq_{\mathbb{N}} \circ \langle \pi_1, \pi_0\rangle\rangle\right)^\sharp$ satisfies the diagram below, as well as $(\mathsf{t}\beta_{\mathbb{N}\times\mathbb{N}})^\sharp$, so that the two are equal.



To this end, let $n \in \mathbb{N}$ be arbitrary then

$$\begin{aligned}
e(\mathrm{id} \times (\mathsf{t}\beta_{\mathbb{N}\times\mathbb{N}})^\sharp \circ z)\langle n, \mathrm{id}\rangle &= e(\mathrm{id} \times (\mathsf{t}\beta_{\mathbb{N}\times\mathbb{N}})^\sharp) \circ (\mathrm{id} \times z)\langle n, \mathrm{id}\rangle \\
&= e(\mathrm{id} \times (\mathsf{t}\beta_{\mathbb{N}\times\mathbb{N}})^\sharp)\langle n, z\rangle \\
&= \mathsf{t}\beta_{\mathbb{N}\times\mathbb{N}}\langle n, z\rangle \\
&= \mathsf{t}
\end{aligned}$$

We get the same result if we use the other function

$$\begin{aligned}
& e\left(\mathrm{id} \times \left(\chi_{\langle \mathrm{id}_\Omega, \mathsf{t}\beta_\Omega\rangle \amalg \langle \mathsf{t}\beta_\Omega, \mathrm{id}_\Omega\rangle} \circ \langle \leq_{\mathbb{N}}, \leq_{\mathbb{N}} \circ \langle \pi_1, \pi_0\rangle\rangle\right)^\sharp \circ z\right) \langle n, \mathrm{id}\rangle \\
&= \chi_{\langle \mathrm{id}_\Omega, \mathsf{t}\beta_\Omega\rangle \amalg \langle \mathsf{t}\beta_\Omega, \mathrm{id}_\Omega\rangle} \circ \left\langle \leq_{\mathbb{N}} \langle z, n\rangle, \leq_{\mathbb{N}} \langle n, z\rangle \right\rangle \\
&= \chi_{\langle \mathrm{id}_\Omega, \mathsf{t}\beta_\Omega\rangle \amalg \langle \mathsf{t}\beta_\Omega, \mathrm{id}_\Omega\rangle} \circ \langle \mathsf{t}, \star\rangle \\
&= \mathsf{t}
\end{aligned}$$

where $\star : 1 \to \Omega$.

Finally, note that $e(\mathrm{id} \times (\mathsf{t}\pi_1)^\sharp)\langle n, \mathrm{id}\rangle = \mathsf{t}\pi_1\langle n, \mathrm{id}\rangle = \mathsf{t}$; therefore, both functions make the triangle commute.

Now we prove that both make the square commute.

$$\begin{aligned}
&e(\mathrm{id} \times (\mathtt{t}\beta_{\mathbb{N}\times\mathbb{N}})^\sharp \circ s)\langle m, n\rangle \\
&= \mathtt{t}\beta_{\mathbb{N}\times\mathbb{N}}\langle m, sn\rangle \\
&= \mathtt{t} \\
&= \mathtt{t}\beta_{\mathbb{N}\times\mathbb{N}}\langle m, n\rangle \\
&= e(\mathrm{id} \times (\mathtt{t}\beta_{\mathbb{N}\times\mathbb{N}})^\sharp)\langle m, n\rangle
\end{aligned}$$

To show that $\left(\chi_{\langle \mathrm{id}_\Omega, \mathtt{t}\beta_\Omega\rangle \amalg \langle \mathtt{t}\beta_\Omega, \mathrm{id}_\Omega\rangle} \circ \langle \leq_{\mathbb{N}}, \leq_{\mathbb{N}} \langle \pi_1, \pi_0\rangle\rangle\right)^\sharp$ makes the square commute, it suffices to only consider the case when $\leq_{\mathbb{N}} \langle n, m\rangle = \mathtt{f}$ *and* $\leq_{\mathbb{N}} \langle m, n\rangle = \mathtt{f}$, since if at least one of these is true then we have our main result but this would also prove the square commutes. To this end, we show that $\leq_{\mathbb{N}} \langle sm, n\rangle = \mathtt{f}$ and $\leq_{\mathbb{N}} \langle n, sm\rangle = \mathtt{f}$. Therefore, we assume, for a contradiction, that $\leq_{\mathbb{N}} \langle sm, n\rangle = \mathtt{t}$ or $\leq_{\mathbb{N}} \langle n, sm\rangle = \mathtt{t}$. In the former case there exists $k \in \mathbb{N}$ such that $sm + k = n$ but then $n = sm + k = m + sk$ so that $\leq_{\mathbb{N}} \langle m, n\rangle = \mathtt{t}$, a contradiction. In the latter case, if $\leq_{\mathbb{N}} \langle n, sm\rangle = \mathtt{t}$ then there exists $j \in \mathbb{N}$ such that $n + j = sm = m + 1$. If $j = 0$ then $n = m + 1$ so that $\leq_{\mathbb{N}} \langle m, n\rangle = \mathtt{t}$, a contradiction. Otherwise, $j = sp$ for some $p \in \mathbb{N}$ then $sm = n + j = n + sp = s(n + p)$ but the successor is injective so that $m = n + p$ but then $\leq_{\mathbb{N}} \langle n, m\rangle = \mathtt{t}$, a contradiction. Either way we arrive at a contradiction so it must be the case that $\leq_{\mathbb{N}} \langle n, sm\rangle = \mathtt{f}$.

In assuming that $\leq_{\mathbb{N}} \langle n, m\rangle = \mathtt{f}$ and $\leq_{\mathbb{N}} \langle m, n\rangle = \mathtt{f}$ we concluded that $\leq_{\mathbb{N}} \langle sm, n\rangle = \mathtt{f}$ and $\leq_{\mathbb{N}} \langle n, sm\rangle = \mathtt{f}$, now we show that the square is made to commute in such cases.

$$\begin{aligned}
&e(\mathrm{id} \times [\chi_{\langle \mathrm{id}_\Omega, \mathtt{t}\beta_\Omega\rangle \amalg \langle \mathtt{t}\beta_\Omega, \mathrm{id}_\Omega\rangle} \circ \left\langle \leq_{\mathbb{N}}, \leq_{\mathbb{N}} \langle \pi_1, \pi_0\rangle \right\rangle]^\sharp \circ s)\langle n, m\rangle \\
&= \chi_{\langle \mathrm{id}_\Omega, \mathtt{t}\beta_\Omega\rangle \amalg \langle \mathtt{t}\beta_\Omega, \mathrm{id}_\Omega\rangle} \circ \left\langle \leq_{\mathbb{N}}, \leq_{\mathbb{N}} \langle \pi_1, \pi_0\rangle \right\rangle \langle n, sm\rangle \\
&= \chi_{\langle \mathrm{id}_\Omega, \mathtt{t}\beta_\Omega\rangle \amalg \langle \mathtt{t}\beta_\Omega, \mathrm{id}_\Omega\rangle} \circ \left\langle \leq_{\mathbb{N}} \langle n, sm\rangle, \leq_{\mathbb{N}} \langle sm, n\rangle \right\rangle \\
&= \chi_{\langle \mathrm{id}_\Omega, \mathtt{t}\beta_\Omega\rangle \amalg \langle \mathtt{t}\beta_\Omega, \mathrm{id}_\Omega\rangle} \circ \langle \mathtt{f}, \mathtt{f}\rangle \\
&= \chi_{\langle \mathrm{id}_\Omega, \mathtt{t}\beta_\Omega\rangle \amalg \langle \mathtt{t}\beta_\Omega, \mathrm{id}_\Omega\rangle} \circ \left\langle \leq_{\mathbb{N}} \langle n, m\rangle, \leq_{\mathbb{N}} \langle m, n\rangle \right\rangle \\
&= e(\mathrm{id} \times [\mathrm{id}_{\Omega^{\mathbb{N}}} \circ \chi_{\langle \mathrm{id}_\Omega, \mathtt{t}\beta_\Omega\rangle \amalg \langle \mathtt{t}\beta_\Omega, \mathrm{id}_\Omega\rangle} \circ \left\langle \leq_{\mathbb{N}}, \leq_{\mathbb{N}} \langle \pi_1, \pi_0\rangle \right\rangle]^\sharp)\langle n, m\rangle
\end{aligned}$$

We then have that

$$\chi_{\langle \mathrm{id}_\Omega, \mathtt{t}\beta_\Omega\rangle \amalg \langle \mathtt{t}\beta_\Omega, \mathrm{id}_\Omega\rangle} \circ \langle \leq_{\mathbb{N}} \langle \pi_0, \pi_1\rangle, \leq_{\mathbb{N}} \circ \langle \pi_1, \pi_0\rangle\rangle = \mathtt{t}\beta_{\mathbb{N}\times\mathbb{N}}$$

and connexity clearly follows.

4 Integers in ETCS

We define integers in terms of equivalence classes of pairs. One may think of the first element of a pair as representing a negative component, and the second element as representing a positive component, so that $\langle a, b\rangle$ represents "$b - a$". We thus say that two pairs $\langle a, b\rangle$ and $\langle c, d\rangle$ represent the same integer if $b + c = a + d$. We use Axiom 6 to define an equivalence relation (a subset of $(\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N})$) with this property. We have $\mathrm{add} \circ \langle \pi_1\pi_0, \pi_0\pi_1\rangle \circ \langle \langle a, b\rangle, \langle c, d\rangle\rangle = b + c$ and $\mathrm{add} \circ \langle \pi_0\pi_0, \pi_1\pi_1\rangle \circ \langle \langle a, b\rangle, \langle c, d\rangle\rangle = a + d$. Therefore, we let $f = \mathrm{add} \circ \langle \pi_1\pi_0, \pi_0\pi_1\rangle$ and $g = \mathrm{add} \circ \langle \pi_0\pi_0, \pi_1\pi_1\rangle$ for Axiom 6, this yields a set $R_{\mathbb{Z}}$ and monomorphism $m_{R_{\mathbb{Z}}}$ representing the equivalence relation we desire. We also have that, for any other function $h : F \to (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N})$ that equalizes f and g, there is a function

$k : F \to R_{\mathbb{Z}}$ such that $m_{R_{\mathbb{Z}}} \circ k = h$. Now we show our equivalence relation indeed has the desired property, $\langle a, b\rangle \sim \langle c, d\rangle$ just in case $b + c = a + d$.

$$
\begin{aligned}
&\langle\langle a, b\rangle, \langle c, d\rangle\rangle \in R_{\mathbb{Z}} \\
&\quad\iff \langle\langle a, b\rangle, \langle c, d\rangle\rangle \text{ factors through } m_{R_{\mathbb{Z}}} \\
&\quad\iff \mathrm{add} \circ \langle \pi_1\pi_0, \pi_0\pi_1\rangle(\langle\langle a, b\rangle, \langle c, d\rangle\rangle) = \mathrm{add} \circ \langle \pi_0\pi_0, \pi_1\pi_1\rangle(\langle\langle a, b\rangle, \langle c, d\rangle\rangle) \\
&\quad\iff b + c = a + d
\end{aligned}
$$

Taking $R_{\mathbb{Z}}$ as our equivalence relation, we use Axiom 7 to construct $\mathbb{Z}$ as the quotient $(\mathbb{N} \times \mathbb{N})/R_{\mathbb{Z}}$ and obtain a function $q_{\mathbb{Z}} : \mathbb{N} \times \mathbb{N} \to \mathbb{Z}$ such that $\langle a, b\rangle \sim \langle c, d\rangle$ if and only if $q\langle a, b\rangle = q\langle c, d\rangle$. We also have that for any $f : \mathbb{N} \times \mathbb{N} \to Y$ that is constant on equivalence classes, there is a unique function $\overline{f} : \mathbb{Z} \to Y$ such that the following function commutes:

$$
\begin{array}{ccc}
\mathbb{N} \times \mathbb{N} & \xrightarrow{\ f\ } & Y \\
{\scriptstyle q_{\mathbb{Z}}}\downarrow & \nearrow_{\overline{f}} & \\
\mathbb{Z} & &
\end{array}
$$

If $n \in \mathbb{N}$ then its canonical integer representation is $q_{\mathbb{Z}}\langle z, n\rangle$; note, in particular, that $z \in \mathbb{N}$ lifts to $q_{\mathbb{Z}}\langle z, z\rangle$. Moreover, an integer of the form $q_{\mathbb{Z}}\langle n, z\rangle$ can be thought of as a negative integer.

Representation: For every nonzero integer m there exists nonzero $n \in \mathbb{N}$ such that $m = q_{\mathbb{Z}}\langle z, n\rangle$ or $m = q_{\mathbb{Z}}\langle n, z\rangle$. Such a representation is said to be canonical. That is to say, every integer is either positive, negative, or zero.

If $m \in \mathbb{Z}$ then there exists $a, b \in \mathbb{N}$ (not both z, since m is assumed to be nonzero) such that $m = q_{\mathbb{Z}}\langle a, b\rangle$, since $q_{\mathbb{Z}}$ is an epimorphism and hence surjective. If $\leq_{\mathbb{N}} \langle a, b\rangle = \mathtt{t}$ then there exists $k \in \mathbb{N}$ such that $k +_{\mathbb{N}} a = b$, and we may write $k = b - a$. Now since $(b - a) + a = z + b$ it follows that $\langle z, b - a\rangle \sim \langle a, b\rangle$ and $q_{\mathbb{Z}}\langle z, b-a\rangle = q_{\mathbb{Z}}\langle a, b\rangle = m$. Otherwise, $\leq_{\mathbb{N}} \langle b, a\rangle = \mathtt{t}$ by connexity and there exists $j \in \mathbb{N}$ such that $j+b = a$, so that $b+(a-b) = a+z$ and $q_{\mathbb{Z}}\langle a-b, z\rangle = q_{\mathbb{Z}}\langle a, b\rangle = m$.

4.1 Negation To define negation, we simply swap the left and right components of the pair representing an integer. The function $\langle \pi_1, \pi_0\rangle : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ swaps the elements of a pair, then the corresponding $\mathbb{Z} \to \mathbb{Z}$ function is $\overline{q_{\mathbb{Z}}\langle \pi_1, \pi_0\rangle}$, which we abbreviate as neg, representing negation, and which satisfies the following diagram:

$$
\begin{array}{ccc}
\mathbb{N} \times \mathbb{N} & \xrightarrow{\langle \pi_1, \pi_0\rangle} & \mathbb{N} \times \mathbb{N} \\
{\scriptstyle q_{\mathbb{Z}}}\downarrow & & \downarrow{\scriptstyle q_{\mathbb{Z}}} \\
\mathbb{Z} & \xrightarrow[\mathrm{neg}]{} & \mathbb{Z}
\end{array}
$$

Note that we have $q_{\mathbb{Z}}\langle \pi_1, \pi_0\rangle$ is constant on equivalence classes (that is, for any $\langle x, y\rangle \in R_{\mathbb{Z}}$, $q_{\mathbb{Z}}\langle \pi_1, \pi_0\rangle(x) = q_{\mathbb{Z}}\langle \pi_1, \pi_0\rangle(y)$). To see this, assume that $\langle\langle a, b\rangle, \langle c, d\rangle\rangle \in R_{\mathbb{Z}}$ then note that $\langle a, b\rangle \sim \langle b, a\rangle$ and $\langle c, d\rangle \sim \langle d, c\rangle$ therefore $\langle b, a\rangle \sim \langle d, c\rangle$ hence

$$q_{\mathbb{Z}}\langle \pi_1, \pi_0\rangle\langle a, b\rangle = q_{\mathbb{Z}}\langle b, a\rangle = q_{\mathbb{Z}}\langle d, c\rangle = q_{\mathbb{Z}}\langle \pi_1, \pi_0\rangle\langle c, d\rangle$$

Where the middle equality follows from the definition of $q_{\mathbb{Z}}$ in Axiom 7. The application of Axiom 7 above to define negation is thus justified.

4.2 Binary function lifting Given $f : X \times (\mathbb{N} \times \mathbb{N}) \to \mathbb{Z}$ (for any X) that is constant on equivalence classes (that is, if $\langle c, d\rangle \sim \langle c', d'\rangle$ and $x \in X$ then $f\langle x, \langle c, d\rangle\rangle = f\langle x, \langle c', d'\rangle\rangle$), define $\mathbf{liftr}_{\mathbb{Z}}(f) : X \times \mathbb{Z} \to \mathbb{Z}$ by

$$\mathbf{liftr}_{\mathbb{Z}}(f) = (\overline{f^\sharp})^\flat$$

We have that $f^\sharp$ is constant on equivalence classes since if $\langle c, d\rangle \sim \langle c', d'\rangle$ then

$$\begin{aligned} e_{\mathbb{Z}} \circ (\mathrm{id} \times f^\sharp)\langle x, \langle c, d\rangle\rangle &= f\langle x, \langle c, d\rangle\rangle \\ &= f\langle x, \langle c', d'\rangle\rangle \\ &= e_{\mathbb{Z}} \circ (\mathrm{id} \times f^\sharp)\langle x, \langle c', d'\rangle\rangle \end{aligned}$$

Then we have that

$$e_{\mathbb{Z}} \circ (\mathrm{id} \times (f^\sharp\langle c, d\rangle))\langle x, \mathrm{id}_{\mathbf{1}}\rangle = e_{\mathbb{Z}} \circ (\mathrm{id} \times (f^\sharp\langle c', d'\rangle))\langle x, \mathrm{id}_{\mathbf{1}}\rangle$$

Since every element of $X \times \mathbf{1}$ is of the form $\langle x, \mathrm{id}_{\mathbf{1}}\rangle$ and x is arbitrary then from Axiom 2 we have that

$$e_{\mathbb{Z}} \circ (\mathrm{id} \times (f^\sharp\langle c, d\rangle)) = e_{\mathbb{Z}} \circ (\mathrm{id} \times (f^\sharp\langle c', d'\rangle))$$

Then, from Axiom 10, we have that there is a unique function that satisfies this so

$$f^\sharp\langle c, d\rangle = f^\sharp\langle c', d'\rangle$$

So $f^\sharp$ is constant on equivalence classes.

We want to show that $\mathbf{liftr}_{\mathbb{Z}}(f)$ is the unique function g such that $g \circ (\mathrm{id} \times q_{\mathbb{Z}}) = f$.

First, we have that

$$\begin{aligned} \mathbf{liftr}_{\mathbb{Z}}(f) \circ (\mathrm{id} \times q_{\mathbb{Z}}) &= (\overline{f^\sharp})^\flat \circ (\mathrm{id} \times q_{\mathbb{Z}}) \\ &= e_{\mathbb{Z}} \circ (\mathrm{id} \times \overline{f^\sharp}) \circ (\mathrm{id} \times q_{\mathbb{Z}}) \\ &= e_{\mathbb{Z}} \circ (\mathrm{id} \times (\overline{f^\sharp} \circ q_{\mathbb{Z}})) \\ &= e_{\mathbb{Z}} \circ (\mathrm{id} \times f^\sharp) \\ &= f \end{aligned}$$

Suppose there is another function $g : X \times \mathbb{Z} \to \mathbb{Z}$ such that $g \circ (\mathrm{id} \times q_{\mathbb{Z}}) = f$. Then we have that $g \circ (\mathrm{id} \times q_{\mathbb{Z}}) = \mathbf{liftr}_{\mathbb{Z}}(f) \circ (\mathrm{id} \times q_{\mathbb{Z}})$. Since $\mathrm{id} \times q_{\mathbb{Z}}$ is an epimorphism (because id and $q_{\mathbb{Z}}$ are epimorphisms and the product of two epimorphisms is an epimorphism), then we have that $g = \mathbf{liftr}_{\mathbb{Z}}(f)$, so $\mathbf{liftr}_{\mathbb{Z}}(f)$ is unique.

Similarly, given $f : (\mathbb{N} \times \mathbb{N}) \times Y \to \mathbb{Z}$ (for any Y) that is constant on equivalence classes (that is, if $\langle a, b\rangle \sim \langle a', b'\rangle$ and $y \in Y$ then $f\langle\langle a, b\rangle, y\rangle = f\langle\langle a', b'\rangle, y\rangle$), define $\mathbf{liftl}_{\mathbb{Z}}(f) : \mathbb{Z} \times Y \to \mathbb{Z}$ by

$$\mathbf{liftl}_{\mathbb{Z}}(f) = (\overline{(f\langle \pi_1, \pi_0\rangle)^\sharp})^\flat\langle \pi_1, \pi_0\rangle$$

By letting $F = f\langle \pi_1, \pi_0\rangle$ we have that $F^\sharp$ is constant on equivalence classes by the same proof as we showed above for $f^\sharp$. We want to show that $\mathbf{liftl}_{\mathbb{Z}}(f)$ is the unique function such that $g \circ (q_{\mathbb{Z}} \times \mathrm{id}) = f$.

First, we have that

$$\begin{aligned}
\mathbf{liftl}_{\mathbb{Z}}(f) \circ (q_{\mathbb{Z}} \times \mathrm{id}) &= (\overline{(f\langle \pi_1, \pi_0\rangle)^\sharp})^\flat \langle \pi_1, \pi_0\rangle \circ (q_{\mathbb{Z}} \times \mathrm{id}) \\
&= (\overline{(f\langle \pi_1, \pi_0\rangle)^\sharp})^\flat \langle \pi_1, \pi_0\rangle \circ \langle q_{\mathbb{Z}}\pi_0, \mathrm{id}\pi_1\rangle \\
&= (\overline{(f\langle \pi_1, \pi_0\rangle)^\sharp})^\flat \langle \mathrm{id}\pi_1, q_{\mathbb{Z}}\pi_0\rangle \\
&= e_{\mathbb{Z}} \circ (\mathrm{id} \times \overline{(f\langle \pi_1, \pi_0\rangle)^\sharp}) \langle \mathrm{id}\pi_1, q_{\mathbb{Z}}\pi_0\rangle \\
&= e_{\mathbb{Z}} \circ (\mathrm{id} \times \overline{(f\langle \pi_1, \pi_0\rangle)^\sharp} q_{\mathbb{Z}}) \langle \pi_1, \pi_0\rangle \\
&= e_{\mathbb{Z}} \circ (\mathrm{id} \times (f\langle \pi_1, \pi_0\rangle)^\sharp) \langle \pi_1, \pi_0\rangle \\
&= f\langle \pi_1, \pi_0\rangle \langle \pi_1, \pi_0\rangle \\
&= f\langle \pi_0, \pi_1\rangle \\
&= f
\end{aligned}$$

Suppose there is another function $g : \mathbb{Z} \times X \to \mathbb{Z}$ such that $g \circ (q_{\mathbb{Z}} \times \mathrm{id}) = f$. Then $g \circ (q_{\mathbb{Z}} \times \mathrm{id}) = \mathbf{liftl}_{\mathbb{Z}}(f) \circ (q_{\mathbb{Z}} \times \mathrm{id})$ and, since $q_{\mathbb{Z}} \times \mathrm{id}$ is an epimorphism, $g = \mathbf{liftl}_{\mathbb{Z}}(f)$ so $\mathbf{liftl}_{\mathbb{Z}}(f)$ is unique.

Finally, given a function $f : (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N}) \to \mathbb{Z}$ that is constant on equivalence classes (that is, if $\langle a, b\rangle \sim \langle a', b'\rangle$ and $\langle c, d\rangle \sim \langle c', d'\rangle$ then $f\langle\langle a, b\rangle, \langle c, d\rangle\rangle = f\langle\langle a', b'\rangle, \langle c', d'\rangle\rangle$), then we define $\mathbf{lift2}_{\mathbb{Z}}(f) : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ by

$$\mathbf{lift2}_{\mathbb{Z}}(f) = \mathbf{liftr}_{\mathbb{Z}}(\mathbf{liftl}_{\mathbb{Z}}(f))$$

We want to show that that $\mathbf{liftl}_{\mathbb{Z}}(f)$ is constant on equivalence classes in the $\mathbf{liftr}_{\mathbb{Z}}$ sense and that this is the unique function such that $\mathbf{lift2}_{\mathbb{Z}}(f) \circ (q_{\mathbb{Z}} \times q_{\mathbb{Z}}) = f$.

Suppose that $\langle c, d\rangle \sim \langle c', d'\rangle$ and $z \in \mathbb{Z}$ are arbitrary, then

$$\begin{aligned}
\mathbf{liftl}_{\mathbb{Z}}(f)\langle z, \langle c, d\rangle\rangle &= (\overline{(f\langle \pi_1, \pi_0\rangle)^\sharp})^\flat \langle \pi_1, \pi_0\rangle \langle z, \langle c, d\rangle\rangle \\
&= (\overline{(f\langle \pi_1, \pi_0\rangle)^\sharp})^\flat \langle \langle c, d\rangle, z\rangle \\
&= e_{\mathbb{Z}} \circ (\mathrm{id} \times \overline{(f\langle \pi_1, \pi_0\rangle)^\sharp}) \langle \langle c, d\rangle, z\rangle \\
&= e_{\mathbb{Z}} \circ (\mathrm{id} \times \overline{(f\langle \pi_1, \pi_0\rangle)^\sharp}) \langle \langle c, d\rangle, q_{\mathbb{Z}}x\rangle \text{ for some } x \in \mathbb{N} \times \mathbb{N} \\
&= e_{\mathbb{Z}} \circ (\mathrm{id} \times \overline{(f\langle \pi_1, \pi_0\rangle)^\sharp} q_{\mathbb{Z}}) \langle \langle c, d\rangle, x\rangle \text{ for some } x \in \mathbb{N} \times \mathbb{N} \\
&= e_{\mathbb{Z}} \circ (\mathrm{id} \times (f\langle \pi_1, \pi_0\rangle)^\sharp) \langle \langle c, d\rangle, x\rangle \text{ for some } x \in \mathbb{N} \times \mathbb{N} \\
&= f\langle \pi_1, \pi_0\rangle \langle \langle c, d\rangle, x\rangle \text{ for some } x \in \mathbb{N} \times \mathbb{N} \\
&= f\langle x, \langle c, d\rangle\rangle \text{ for some } x \in \mathbb{N} \times \mathbb{N} \\
&= f\langle x, \langle c', d'\rangle\rangle \text{ for some } x \in \mathbb{N} \times \mathbb{N} \\
&\cdots \\
&= \mathbf{liftl}_{\mathbb{Z}}(f)\langle z, \langle c', d'\rangle\rangle
\end{aligned}$$

Observe that

$$\begin{aligned}
\mathbf{lift2}_{\mathbb{Z}}(f) \circ (q_{\mathbb{Z}} \times q_Z) &= \mathbf{liftr}_{\mathbb{Z}}(\mathbf{liftl}_{\mathbb{Z}}(f)) \circ ((\mathrm{id} \times q_{\mathbb{Z}})) \circ (q_{\mathbb{Z}} \times \mathrm{id}) \\
&= \mathbf{liftr}_{\mathbb{Z}}(f) \circ (q_{\mathbb{Z}} \times \mathrm{id}) = f
\end{aligned}$$

Suppose there is another function $g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ such that $g \circ (q_\mathbb{Z} \times q_\mathbb{Z}) = f$. Then $g \circ (q_\mathbb{Z} \times q_\mathbb{Z}) = \mathbf{lift2}_\mathbb{Z}(f) \circ (q_\mathbb{Z} \times q_\mathbb{Z})$ and, since $q_\mathbb{Z} \times q_\mathbb{Z}$ is an epimorphism, $g = \mathbf{lift2}_\mathbb{Z}(f)$, so $\mathbf{lift2}_\mathbb{Z}(f)$ is unique.

These lifting operators give us a general way to convert functions on pairs of pairs of natural numbers to functions on pairs of integers. Next, we use them to construct binary operations over the integers in terms of functions over the natural numbers.

4.3 Addition For addition on integers we want to define a function $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, similarly to natural numbers. We start with a function $(\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N}) \to \mathbb{N} \times \mathbb{N}$, and use $\mathbf{lift2}_\mathbb{Z}$ and $q_\mathbb{Z}$ to lift it to $\mathbb{Z}$.

$$\mathrm{add}_{\mathbb{N}\times\mathbb{N}} = (\mathrm{add} \times \mathrm{add}) \circ \langle\langle \pi_0\pi_0, \pi_0\pi_1\rangle, \langle \pi_1\pi_0, \pi_1\pi_1\rangle\rangle$$

We lift the output of this by applying $q_\mathbb{Z}$ to it. Then, in order to apply $\mathbf{lift2}_\mathbb{Z}$, we need to show that $q_\mathbb{Z} \circ \mathrm{add}_{\mathbb{N}\times\mathbb{N}}$ is constant on equivalence classes. Suppose that $\langle a, b\rangle \sim \langle a', b'\rangle$ and $\langle c, d\rangle \sim \langle c', d'\rangle$ then, $a + b' = b + a'$ and $c + d' = d + c'$ then

$$a + b' + c + d' = b + a' + d + c'$$

equivalently

$$(a + c) + (b' + d') = (a' + c') + (b + d)$$

then

$$\langle a + c, b + d\rangle \sim \langle a' + c', b' + d'\rangle$$

hence $q_\mathbb{Z}\langle a + c, b + d\rangle = q_\mathbb{Z}\langle a' + c', b' + d'\rangle$, since $q_\mathbb{Z}$ is constant on equivalence classes. We thus have that $q_\mathbb{Z} \circ \mathrm{add}_{\mathbb{N}\times\mathbb{N}}$ is constant on equivalence classes, so we can define $\mathrm{add}_\mathbb{Z} : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ by

$$\mathrm{add}_\mathbb{Z} = \mathbf{lift2}_\mathbb{Z}(q_\mathbb{Z} \circ \mathrm{add}_{\mathbb{N}\times\mathbb{N}})$$

By the lifting property (see the previous section) this satisfies the following commuting diagram:

$$\begin{array}{ccc} (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N}) & \xrightarrow{\mathrm{add}_{\mathbb{N}\times\mathbb{N}}} & \mathbb{N} \times \mathbb{N} \\ \downarrow{\scriptstyle q_\mathbb{Z}\times q_\mathbb{Z}} & & \downarrow{\scriptstyle q_\mathbb{Z}} \\ \mathbb{Z} \times \mathbb{Z} & \xrightarrow{\mathrm{add}_\mathbb{Z}} & \mathbb{Z} \end{array}$$

4.4 Properties of Addition In this section, we show a general strategy for proving the results from natural numbers in the integer setting. To this end, we directly show a few results. First note that

$$\begin{aligned} &\mathrm{add}_{\mathbb{N}\times\mathbb{N}}\big\langle\langle a, b\rangle, \langle c, d\rangle\big\rangle \\ &= (\mathrm{add} \times \mathrm{add}) \circ \langle\langle \pi_0\pi_0, \pi_0\pi_1\rangle, \langle \pi_1\pi_0, \pi_1\pi_1\rangle\rangle\big\langle\langle a, b\rangle, \langle c, d\rangle\big\rangle \\ &= \big\langle \mathrm{add}\langle a, c\rangle, \mathrm{add}\langle b, d\rangle\big\rangle \end{aligned}$$

Respects Identity

$$0 +_\mathbb{Z} x = \mathrm{add}_\mathbb{Z}\langle q_\mathbb{Z}\langle z, z\rangle, q_\mathbb{Z}\langle a, b\rangle\rangle = \mathrm{add}_\mathbb{Z}(q_\mathbb{Z} \times q_\mathbb{Z})\langle\langle z, z\rangle, \langle a, b\rangle\rangle$$

$$= q_\mathbb{Z}\mathrm{add}_{\mathbb{N}\times\mathbb{N}}\langle\langle z, z\rangle, \langle a, b\rangle\rangle = q_\mathbb{Z}\langle \mathrm{add}\langle z, a\rangle, \mathrm{add}\langle z, b\rangle\rangle = q_\mathbb{Z}\langle a, b\rangle = x$$

Commutative Suppose that $n, m \in \mathbb{Z}$ then $n = q_{\mathbb{Z}}\langle a, b\rangle$ and $m = q_{\mathbb{Z}}\langle c, d\rangle$ for some $a, b, c, d \in \mathbb{N}$

$$\begin{aligned} n +_{\mathbb{Z}} m &= \mathrm{add}_{\mathbb{Z}}\big\langle q_{\mathbb{Z}}\langle a, b\rangle, q_{\mathbb{Z}}\langle c, d\rangle\big\rangle \\ &= q_{\mathbb{Z}}\big\langle \mathrm{add}\langle a, c\rangle, \mathrm{add}\langle b, d\rangle\big\rangle \\ &= q_{\mathbb{Z}}\big\langle \mathrm{add}\langle c, a\rangle, \mathrm{add}\langle d, b\rangle\big\rangle \qquad (\ddagger) \\ &= \mathrm{add}_{\mathbb{Z}}\big\langle q_{\mathbb{Z}}\langle c, d\rangle, q_{\mathbb{Z}}\langle a, b\rangle\big\rangle \\ &= m +_{\mathbb{Z}} n \end{aligned}$$

We note that (‡) follows from commutativity within $\mathbb{N}$; in general, we can prove results about $\mathbb{Z}$ by reducing it to the analogous result for $\mathbb{N}$.

Additive Inverse $(n + (-n) = 0)$*:*

$$\begin{aligned} n +_{\mathbb{Z}} (-n) &= \mathrm{add}_{\mathbb{Z}}\big\langle q_{\mathbb{Z}}\langle a, b\rangle, \mathrm{neg} \circ q_{\mathbb{Z}}\langle a, b\rangle\big\rangle \\ &= \mathrm{add}_{\mathbb{Z}}\big\langle q_{\mathbb{Z}}\langle a, b\rangle, q_{\mathbb{Z}}\langle \pi_1, \pi_0\rangle\langle a, b\rangle\big\rangle \\ &= \mathrm{add}_{\mathbb{Z}}(q_{\mathbb{Z}} \times q_{\mathbb{Z}})\big\langle\langle a, b\rangle, \langle b, a\rangle\big\rangle \\ &= q_{\mathbb{Z}} \circ \mathrm{add}_{\mathbb{N}\times\mathbb{N}}\big\langle\langle a, b\rangle, \langle b, a\rangle\big\rangle \\ &= q_{\mathbb{Z}}\big\langle \mathrm{add}\langle a, b\rangle, \mathrm{add}\langle b, a\rangle\big\rangle \\ &= q_{\mathbb{Z}}\langle a +_{\mathbb{N}} b, a +_{\mathbb{N}} b\rangle \\ &= q_{\mathbb{Z}}\langle z, z\rangle \\ &= 0 \end{aligned}$$

where we used the fact that $(a +_{\mathbb{N}} b) +_{\mathbb{N}} 0 = (a +_{\mathbb{N}} b) +_{\mathbb{N}} 0$ if and only if $\langle a +_{\mathbb{N}} b, a +_{\mathbb{N}} b\rangle \sim \langle z, z\rangle$ if and only if $q_{\mathbb{Z}}\langle a +_{\mathbb{N}} b, a +_{\mathbb{N}} b\rangle = q_{\mathbb{Z}}\langle z, z\rangle$.

One can easily show that $0_{\mathbb{Z}} = -0_{\mathbb{Z}}$ and $-(-n) = n$ for every $n \in \mathbb{Z}$.

4.5 Multiplication As with addition, we first define multiplication on pairs of naturals. Since we want to have $(b - a) \cdot (d - c) = (ac + bd) - (ad + bc)$ we define

$$\begin{aligned} &\mathrm{mult}_{\mathbb{N}\times\mathbb{N}} = \\ &\quad\Big\langle \mathrm{add}\big\langle \mathrm{mult}\langle \pi_0\pi_0, \pi_1\pi_1\rangle, \mathrm{mult}\langle \pi_1\pi_0, \pi_0\pi_1\rangle\big\rangle, \\ &\qquad \mathrm{add}\big\langle \mathrm{mult}\langle \pi_0\pi_0, \pi_0\pi_1\rangle, \mathrm{mult}\langle \pi_1\pi_0, \pi_1\pi_1\rangle\big\rangle\Big\rangle \end{aligned}$$

And acting on an arbitrary element we see that

$$\begin{aligned} &\mathrm{mult}_{\mathbb{N}\times\mathbb{N}}\big\langle\langle a, b\rangle, \langle c, d\rangle\big\rangle = \\ &\quad\Big\langle \mathrm{add}\big\langle\langle \mathrm{mult}\langle a, d\rangle, \langle \mathrm{mult}\langle b, c\rangle\big\rangle, \mathrm{add}\big\langle\langle \mathrm{mult}\langle a, c\rangle, \langle \mathrm{mult}\langle b, d\rangle\big\rangle\Big\rangle \end{aligned}$$

We want to prove that $q_{\mathbb{Z}} \circ \mathrm{mult}_{\mathbb{N}\times\mathbb{N}}$ is constant on equivalence classes and then define

$$\mathrm{mult}_{\mathbb{Z}} = \mathbf{lift2}_{\mathbb{Z}}(q_{\mathbb{Z}} \circ \mathrm{mult}_{\mathbb{N}\times\mathbb{N}})$$

As before, multiplication satisfies the following diagram via the lifting property

$$\begin{array}{ccc} (\mathbb{N}\times\mathbb{N}) \times (\mathbb{N}\times\mathbb{N}) & \xrightarrow{\mathrm{mult}_{\mathbb{N}\times\mathbb{N}}} & \mathbb{N}\times\mathbb{N} \\ \Big\downarrow{\scriptstyle q_{\mathbb{Z}}\times q_{\mathbb{Z}}} & & \Big\downarrow{\scriptstyle q_{\mathbb{Z}}} \\ \mathbb{Z}\times\mathbb{Z} & \xrightarrow{\quad\mathrm{mult}_{\mathbb{Z}}\quad} & \mathbb{Z} \end{array}$$

Now we show that $q_{\mathbb{Z}} \circ \mathrm{mult}_{\mathbb{N}\times\mathbb{N}}$ is indeed constant on equivalence classes. Suppose $\langle a, b\rangle \sim \langle a', b'\rangle$ and $\langle c, d\rangle \sim \langle c', d'\rangle$ then we have $b + a' = a + b'$ and $d + c' = c + d'$ from which it follows

$$\begin{aligned}
& ac + (a' + b)d' = ac + (a' + b)d' \\
\implies & ac + (a' + b)d' = ac + (a + b')d' \\
\implies & ac + (a' + b)d' = ac + ad' + b'd' \\
\implies & ac + (a' + b)d' = a(c + d') + b'd' \\
\implies & ac + (a' + b)d' = a(d + c') + b'd' \\
\implies & ac + bd' + a'd' = ad + ac' + b'd' \\
\implies & ac + bc + bd' + a'd' + b'c' = ad + bc + ac' + b'c' + b'd' \\
\implies & ac + b(c + d') + a'd' + b'c' = ad + bc + (a + b')c' + b'd' \\
\implies & ac + b(d + c') + a'd' + b'c' = ad + bc + (a' + b)c' + b'd' \\
\implies & ac + bd + bc' + a'd' + b'c' = ad + bc + a'c' + bc' + b'd' \\
\implies & (ac + bd) + (a'd' + b'c') = (a'c' + b'd') + (ad + bc)
\end{aligned}$$

It follows that

$$\langle ad + bc, ac + bd\rangle \sim \langle a'd' + b'c', a'c' + b'd'\rangle$$

equivalently

$$q_{\mathbb{Z}}\langle ad + bc, ac + bd\rangle = q_{\mathbb{Z}}\langle a'd' + b'c', a'c' + b'd'\rangle$$

this shows that $q_{\mathbb{Z}} \circ \mathrm{mult}_{\mathbb{N}\times\mathbb{N}}$ is constant on equivalence classes.

4.6 Properties of Multiplication As expected, multiplication on $\mathbb{Z}$ satisfies the usual laws. Often times, the result in question simply reduces to corresponding results in $\mathbb{N}$ and the working is straightforward. We thus omit full proofs for most of the results in this section. As an example we explicitly demonstrate the proof that $\cdot_{\mathbb{Z}}$ is an associative operation.

Respects Identity We have that the integer representation of 1, $q_{\mathbb{Z}}\langle z, sz\rangle$, is the identity of (integer) multiplication by a straightforward calculation, using the identity and zero properties of natural number addition and multiplication. Since we have that multiplication is constant on equivalence classes, it is sufficient to prove this for the canonical representation $q_{\mathbb{Z}}\langle z, sz\rangle$.

Respects Zero The integer representation of 0 is $q_{\mathbb{Z}}\langle z, z\rangle$ and, as expected, 0 does annihilate anything it is multiplied against. This follows, similarly to the identity law above, from the zero law of natural number multiplication and the identity law of natural number addition.

Commutative We obtain commutativity of integer multiplication by observing that natural number addition and multiplication are commutative. Swapping the numbers in the natural number addition and multiplication then results in a corresponding swap in the integer representations. Since we have commutativity, it is, of course, sufficient to prove the other laws in this section only in a single direction.

Associative Here we explicitly demonstrate that multiplication is associate. Suppose that $x = q_{\mathbb{Z}}\langle a, b\rangle$, $y = q_{\mathbb{Z}}\langle c, d\rangle$, and $t = q_{\mathbb{Z}}\langle e, f\rangle$ then

$$
\begin{aligned}
&(x \cdot_{\mathbb{Z}} y) \cdot_{\mathbb{Z}} t \\
&= \mathrm{mult}_{\mathbb{Z}}\Big\langle \mathrm{mult}_{\mathbb{Z}}\big\langle q_{\mathbb{Z}}\langle a, b\rangle, q_{\mathbb{Z}}\langle c, d\rangle\big\rangle, q_{\mathbb{Z}}\langle e, f\rangle\Big\rangle \\
&= \mathrm{mult}_{\mathbb{Z}}\Big\langle \mathrm{mult}_{\mathbb{Z}}(q_{\mathbb{Z}} \times q_{\mathbb{Z}})\big\langle\langle a, b\rangle, \langle c, d\rangle\big\rangle, q_{\mathbb{Z}}\langle e, f\rangle\Big\rangle \\
&= \mathrm{mult}_{\mathbb{Z}}\Big\langle q_{\mathbb{Z}} \circ \mathrm{mult}_{\mathbb{N}\times\mathbb{N}}\big\langle\langle a, b\rangle, \langle c, d\rangle\big\rangle, q_{\mathbb{Z}}\langle e, f\rangle\Big\rangle \\
&= \mathrm{mult}_{\mathbb{Z}}\Big\langle q_{\mathbb{Z}} \circ \big\langle a \cdot_{\mathbb{N}} d +_{\mathbb{N}} b \cdot_{\mathbb{N}} c, a \cdot_{\mathbb{N}} c +_{\mathbb{N}} b \cdot_{\mathbb{N}} d\big\rangle, q_{\mathbb{Z}}\langle e, f\rangle\Big\rangle \\
&= q_{\mathbb{Z}} \circ \mathrm{mult}_{\mathbb{N}\times\mathbb{N}}\Big\langle \langle a \cdot d + b \cdot c, a \cdot c + b \cdot d\rangle, \langle e, f\rangle\Big\rangle \\
&= q_{\mathbb{Z}}\Big\langle (ad + bc)f + (ac + bd)e, (ad + bc)e + (ac + bd)f\Big\rangle \\
&= q_{\mathbb{Z}}\Big\langle (ad)f + (bc)f + (ac)e + (bd)e, (ad)e + (bc)e + (ac)f + (bd)f\Big\rangle \\
&= q_{\mathbb{Z}} \circ \Big\langle a(ce + df) + b(cf + de), a(cf + de) + b(ce + df)\Big\rangle \\
&= q_{\mathbb{Z}} \circ \mathrm{mult}_{\mathbb{N}\times\mathbb{N}}\Big\langle \langle a, b\rangle, \langle cf + de, ce + df\rangle\Big\rangle \\
&= \mathrm{mult}_{\mathbb{Z}}\Big\langle q_{\mathbb{Z}}\langle a, b\rangle, q_{\mathbb{Z}}\langle cf + de, ce + df\rangle\Big\rangle \\
&= \mathrm{mult}_{\mathbb{Z}}\Big\langle q_{\mathbb{Z}}\langle a, b\rangle, \mathrm{mult}_{\mathbb{Z}}\langle q_{\mathbb{Z}}\langle c, d\rangle, q_{\mathbb{Z}}\langle e, f\rangle\rangle\Big\rangle \\
&= x \cdot_{\mathbb{Z}} (y \cdot_{\mathbb{Z}} t)
\end{aligned}
$$

Distributive We have that multiplication on the integers distributes over addition. This follows easily from the corresponding distributivity law on the natural numbers once the definitions of multiplication and addition on integers have been unfolded.

4.7 Cancellation Laws For every integer we have

$$a + c = b + c \implies a = b$$

and provided $c \neq 0$

$$a \cdot c = b \cdot c \implies a = b$$

To prove the first, $a = a + c - c = b + c - c = b$.

Now we prove the second cancellation law. Suppose that $a \cdot_{\mathbb{Z}} c = b \cdot_{\mathbb{Z}} c$ (with $c \neq 0$). First let us assume that $a, b, c > 0$ then $a = q_{\mathbb{Z}}\langle z, u\rangle$, $b = q_{\mathbb{Z}}\langle z, v\rangle$, and $c = q_{\mathbb{Z}}\langle z, w\rangle$ for some $u, v, w \in \mathbb{N}$.

$$\begin{aligned} q_{\mathbb{Z}}\big\langle 0, u \cdot_{\mathbb{N}} w\big\rangle &= q_{\mathbb{Z}}\big\langle 0 \cdot_{\mathbb{N}} w +_{\mathbb{N}} u \cdot_{\mathbb{N}} 0, 0 \cdot_{\mathbb{N}} 0 +_{\mathbb{N}} u \cdot_{\mathbb{N}} w\big\rangle \\ &= q_{\mathbb{Z}} \circ \mathrm{mult}_{\mathbb{N}\times\mathbb{N}}\big\langle\langle z, u\rangle, \langle z, w\rangle\big\rangle \\ &= \mathrm{mult}_{\mathbb{Z}} \circ (q_{\mathbb{Z}} \times q_{\mathbb{Z}})\big\langle\langle z, u\rangle, \langle z, w\rangle\big\rangle \\ &= a \cdot_{\mathbb{Z}} c \\ &= b \cdot_{\mathbb{Z}} c \\ &= \cdots \\ &= q_{\mathbb{Z}}\big\langle 0 \cdot_{\mathbb{N}} w +_{\mathbb{N}} v \cdot_{\mathbb{N}} 0, 0 \cdot_{\mathbb{N}} 0 +_{\mathbb{N}} v \cdot_{\mathbb{N}} w\big\rangle \\ &= q_{\mathbb{Z}}\big\langle 0, v \cdot_{\mathbb{N}} w\big\rangle \end{aligned}$$

from which we have $\big\langle 0, u \cdot_{\mathbb{N}} w\big\rangle \sim \big\langle 0, v \cdot_{\mathbb{N}} w\big\rangle$ and hence

$$u \cdot_{\mathbb{N}} w = u \cdot_{\mathbb{N}} w +_{\mathbb{N}} 0 = 0 +_{\mathbb{N}} v \cdot_{\mathbb{N}} w = v \cdot_{\mathbb{N}} w.$$

We conclude that $u = v$ from the corresponding cancellation law in $\mathbb{N}$, and it then follows that $a = b$. Similar proofs exist in case either a (and hence b) or c are negative.

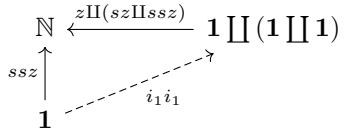
5 Discussion and Conclusion

The above results show that one can successfully ground the theory of arithmetic within ETCS. That is, ETCS's $\mathbb{N}$ together with the operations defined above serve as a model for the theory of arithmetic.

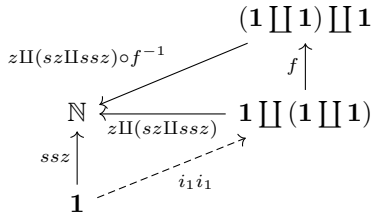
We note that Hatcher [4] defines both cardinals and ordinals within the framework of ETCS, with ordinals corresponding to the elements of $\mathbb{N}$. While Hatcher did develop a full theory of arithmetic for cardinals, he did not construct a parallel theory for ordinals, although he did prove the Peano postulates for the ordinals. Our work thus focuses on defining arithmetic for the ordinals in ETCS. In many ways these ordinal numbers correspond better to numbers as mathematical objects, since they allow us to construct higher kinds of number, as in our construction of the integers. By contrast, cardinal numbers in ETCS are represented by the set objects themselves, and so focus particularly on the size of the set as their main defining property. The former are defined as certain objects within $\mathbf{Sets}$ while the latter are elements of the natural number object $\mathbb{N}$. Hatcher develops a theory of cardinal arithmetic by defining 0 as the initial object $\emptyset$, 1 as the terminal object $\mathbf{1}$, addition as the coproduct, multiplication as the cartesian product, and exponentiation as given by Axiom 10. Under that system, two is defined as $1 + 1$ and 3 is either $2 + 1$ or $1 + 2$. In order for "$1 + 2 = 2 + 1$" to be true, we must require that sets are equal up to isomorphism, thus justifying the label of "cardinal arithmetic". That is to say, we cannot prove in this framework that $1 + 2 = 2 + 1$, rather we must agree that sets of the same size are equal. There is, of course, an ongoing philosophical debate among category theorists and metaphysicians as to whether sets are equal up to isomorphism [7].

The distinction between cardinals and ordinals in ETCS and ZFC can be particularly illustrated by considering the question of whether 2 is an element of 3. For the von Neumann construction of cardinals and ordinals [10] in ZFC this can be unambiguously affirmed; moreover, the von Neumann construction cannot discriminate between finite ordinals and cardinals. However, ETCS views ordinals and cardinals as different types – the former are functions while the latter are sets. Thus, the question, "Is $2 \in 3$?" is only made meaningful if 2 is the ordinal ssz while 3 must be

a set isomorphic to $\mathbf{1} \coprod (\mathbf{1} \coprod \mathbf{1})$. In fact, the following diagram demonstrates that $2 \in_{\mathbb{N}} 1 + (1 + 1)$, yet we cannot simply say $2 \in 1 + (1 + 1)$ since the types do not match up.



Moreover, it is easy to see that isomorphic sets have the same *relative* elements. Notice that we can think of $z \amalg (sz \amalg ssz)$ as characterising the subset $\{0, 1, 2\}$ of $\mathbb{N}$ in ETCS. This shows how functions are taken to characterize subsets in ETCS, and we observe that ssz would not be a relative element of the subset characterised by a different monomorphism such as $sssz \amalg (sssssz \amalg ssssssz)$, which would characterise the subset $\{3, 4, 5\}$. Thus, while sets of the same size are isomorphic in both ETCS and ZFC, this isomorphism is more specific in ETCS since it does not necessarily associate specific subsets of $\mathbb{N}$ with one another. Rather, subsets of $\mathbb{N}$ are different characterisations of the same set $\mathbf{1} \coprod (\mathbf{1} \coprod \mathbf{1})$, and the isomorphism between sets of the same size yields a way to construct analogous subsets over other sets, such as $(\mathbf{1} \coprod \mathbf{1}) \coprod \mathbf{1}$ or $\mathbf{1} \coprod \Omega$. However, this does not relate the subsets themselves, since an isomorphism f from $\mathbf{1} \coprod (\mathbf{1} \coprod \mathbf{1})$ to $(\mathbf{1} \coprod \mathbf{1}) \coprod \mathbf{1}$ provides a way to make a subset of $(\mathbf{1} \coprod \mathbf{1}) \coprod \mathbf{1}$ corresponding to $z \amalg (sz \amalg ssz)$, as shown in the diagram below, but cannot transform it to correspond to $sssz \amalg (sssssz \amalg ssssssz)$. To meaningfully change the contents of the subset instead requires an isomorphism from $\mathbb{N}$ to $\mathbb{N}$ swapping 0, 1 and 2 with 3, 4 and 5, which would also change the relative element in the same way.



By contrast, in ZFC we have that $\{0, 1, 2\}$ and $\{3, 4, 5\}$ are isomorphic but distinct sets, rather than different views of a particular set, and isomorphism in ZFC does not preserve elements in the way ETCS allows, since ZFC does not distinguish the properties that are captured in ETCS by the combination of a set and monomorphism. This suggests that there is some deeper property of sets that is being captured by the notion of a set in ETCS when it is not associated with a monomorphism denoting it as a particular subset. We thus see that ETCS not only has a distinction between finite. ordinal and cardinal numbers that is not present in ZFC, but also makes stronger distinctions concerning the elements of sets and relations between them.

Another point to note in our construction of the natural number is that, while we can construct infinitely large sets (representing transfinite cardinals) by considering $\mathbb{N}$ and exponentials of it, our set $\mathbb{N}$ of natural numbers contains only the finite ordinals. It is an open question whether we can construct transfinite ordinals or if ETCS represents some form of finitism in its approach to constructing ordinal numbers. A form of infinite ordinal could perhaps be constructed over a set larger than $\mathbb{N}$, such as $\Omega^{\mathbb{N}}$, up to some limit. By the Burali-Forti paradox [1] we cannot find the transfinite

ordinals in any one set, so we would need to develop a general method for developing sets containing increasing larger ordinals. However, it remains unclear what the definition of such ordinals would be, or how arithmetic may be defined over them. We thus leave consideration of such a topic to future work.

In the course of our research, we discovered that ETCS comes equipped with its own first-order logic with quantifier. Hatcher previously demonstrated that ETCS has the usual connectives of first-order logic, in particular conjunction, disjunction, and negation. For our purposes we found it necessary to construct universal and existential quantifiers over this logic in addition to the connectives defined by Hatcher. In doing so, we were able to express core arithmetical statements such as "$m \leq n$". It could be explored in future work whether we are able to define modal concepts such as *necessity* and *possibility* so that ETCS could serve not only as a groundwork for mathematics but meta-mathematics as well.

Having developed the theory of arithmetic over naturals and integers, we wish to consider in future work a construction of the rationals, reals, and complex numbers. A construction of the rationals would be similar to our construction of the integers, but with a different lifting function. However, a construction of the real numbers would involve a different construction considering infinite sequences based on exponential sets, which would go beyond what we have considered in this paper.

Note

1. This follows by applying Propositions 2.4.3 and 2.6.6 of Halvorson. Suppose $x \in \mathbf{1} \coprod \mathbb{N}$ then either $x = i_0(\mathrm{id}_{\mathbf{1}})$ or there exists $n \in \mathbb{N}$ such that $x = i_1(n)$. It follows either $z \amalg s(x) = (z \amalg s \circ i_0) \circ \mathrm{id}_{\mathbf{1}} = z \circ \mathrm{id}_{\mathbf{1}} = z$ or $z \amalg s(x) = (z \amalg s \circ i_1) \circ n = s \circ n$.

References

[1] Burali-Forti, C., "Una questione sui numeri transfiniti," *Rendiconti del Circolo Matematico di Palermo (1884-1940)*, vol. 11 (1897), pp. 154–164.

[2] Church, A., "An unsolvable problem of elementary number theory," *American journal of mathematics*, vol. 58 (1936), pp. 345–363.

[3] Halvorson, H., *The Logic in Philosophy of Science*, Cambridge University Press, 2019.

[4] Hatcher, W. S., *The Logical Foundations of Mathematics*, Pergamon, 1982. DOI: https://doi.org/10.1016/C2013-0-05962-2.

[5] Lawvere, F. W., "An elementary theory of the category of sets," *Proceedings of the National academy of Sciences of the United States of America*, vol. 52 (1964), p. 1506.

[6] Leinster, T., "Rethinking set theory," *The American Mathematical Monthly*, vol. 121 (2014), pp. 403–415.

[7] Linnebo, Ø., and R. Pettigrew, "Category theory as an autonomous foundation," *Philosophia Mathematica*, vol. 19 (2011), pp. 227–254. URL `https://doi.org/10.1093/philmat/nkr024`.

[8] Osius, G., "Categorical set theory: A characterization of the category of sets," *Journal of Pure and Applied Algebra*, vol. 4 (1974), pp. 79–119. URL `http://www.sciencedirect.com/science/article/pii/0022404974900322`.

[9] Peano, G., *Arithmetices principia: Nova methodo exposita*, Fratres Bocca, 1889.

[10] Von Neumann, J., "Zur einführung der transfiniten zahlen," *Acta Litterarum ac Scientiarum Regiae Universitatis Hungaricae Francisco-Josephinae, sectio scientiarum mathematicarum*, vol. 1 (1923), pp. 199–208.