THE CHURCH NUMBERS IN NF SET THEORY

MICHAEL BEESON

Abstract. By NF we mean Quine's New Foundations set theory. We define the Church numerals (or better, Church numbers) and elaborate their properties in INF. Here we investigate the question whether the set of Church numbers is infinite. Usually in NF, the natural numbers are represented by the finite Frege cardinals. We answer the question by proving that if the set of finite Frege cardinals is infinite, then so is the set of Church numbers.

Specker showed in 1953 that classical NF proves the set of finite Frege cardinals is infinite, so using classical logic the set of Church numbers is infinite. It has long been an open problem whether any set can be proved infinite using NF with intuitionistic logic (INF). Perhaps INF proves the set of Church numbers is infinite; we tried to prove that, but we could only succeed with an additional assumption, the "Church counting axiom." That is a fundamental counting principle: it says that iterating successor n times, starting at zero, results in n.

We also prove, without the aid of the counting axiom, that if the set of Church numbers is not finite, then it is infinite, and Church successor is one-to-one. Consequently, Heyting's arithmetic is interpretable in INF plus the Church counting axiom. Finally, we show that the Church counting axiom is equivalent in INF to Rosser's counting axiom. That equivalence is a new theorem even classically. Since it is known that the Rosser counting axiom is not provable in NF (if NF is consistent), it follows that the same is true of the Church counting axiom. The original question, whether INF proves the set of Church numbers is infinite, remains open. At least it has been shown equivalent to the question whether INF proves there exists an infinite set.

In all the world there is nothing so interesting,
so curious, and so beautiful as truth.
–Hercule Poirot

Contents

Date: November 20, 2021.

1. Introduction

Quine's NF set theory is a first-order theory whose language contains only the binary predicate symbol $\in$, and whose axioms are two in number: extensionality and stratified comprehension. The definition of these axioms will be reviewed below; full details can be found in [4]. Intuitionistic NF, or INF, is the theory with the same language and axioms as NF, but with intuitionistic logic instead of classical.

The "axiom" of infinity is a theorem of NF, proved by Rosser [8] and Specker [10]; see also [4], p. 49. These proofs use classical logic in an apparently essential way, and it is still an open question whether INF proves the existence of an infinite set. In [1], the fundamental results of INF have been developed, and on that basis, we analyzed (in unpublished work) the constructive content of Specker's proof, but that did not lead to a proof of infinity. It has also long been known that if $\mathbb{V}$ is not finite, then the logic of stratified formulas must be classical, so Specker's proof could be done; hence the statement "$\mathbb{V}$ is not finite" can be proved in INF. But that does not lead to a proof of infinity, because there might be a maximum integer, whose elements U would be "unenlargeable" in the sense that we cannot find any set that is not in U.

We therefore have two reasons for being interested in the Church numerals in INF: to use them to prove infinity, and to study their structure for its own intrinsic interest.

The Church numerals were introduced by Church (or technically, by his student Kleene) in the context of λ-calculus. They are defined so that the n-th Church number is a function that takes inputs f and x and produces output $f^n(x)$, where f^n is f iterated n times. It turns out that the Church numerals, or Church numbers as we shall call them[1], and the set $\mathbb{N}$ of Church numbers, can be defined by stratified comprehension straightforwardly in INF. The Church numerals were introduced in 1935 [5] and NF set theory in 1937 [7], so the definition of Church numerals in NF could have been done at any time since 1937.[2]

[1]The word "numeral" is usually used for a syntactic object, a name for a number. The "Church numerals" that we define here are sets, not syntax. We therefore refer to them as "Church numbers" instead. Church himself in [2] never mentions the word "numeral" but instead refers to "the formula representing the integer n".

[2]Church defines addition, multiplication, and exponentiation on p. 10 of [2], but he attributes these definitions to Rosser and refers to [5] for detailed proofs. Rosser later worked on Quine's NF, so he had all the background needed to write this paper right after he wrote [8].

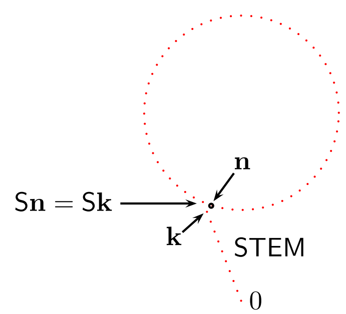
The equation satisfied by Church successor S is

$$\mathsf{S}jfx = f(jfx).$$

It was Church's student Kleene who defined the predecessor function in λ-calculus, in his Ph. D. thesis, and in [5]. The λ-calculus definition of that function does not lead to a definition by stratified comprehension in NF, so to prove that Church successor is injective in NF requires a new argument.

In this paper we analyze the structure of the Church numbers under successor. First we introduce addition $x \oplus y$ on $\mathbb{N}$. Assuming $\mathbb{N}$ is finite, there is exactly one "double successor", i.e., there are exactly two numerals $\mathbf{k}$ and $\mathbf{n}$ with $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$. The numbers from 0 to $\mathbf{k}$ behave "normally" (trichotomy holds there). We call that the "stem." The rest of the Church numbers form a "loop" $\mathcal{L}$, as a directed graph in which the edges are pairs $\langle x, \mathsf{S}x\rangle$. See Fig. 1.

Figure 1. The stem STEM, the loop $\mathcal{L}$, and unique double successor



So trichotomy fails dramatically on $\mathcal{L}$: everything in $\mathcal{L}$ is less than everything else. The "length" of the loop is a Church number $\mathbf{m}$ such that $x \oplus \mathbf{m} = x$ for every $x \in \mathcal{L}$. We then prove the Annihilation Theorem: any one-to-one map f on any finite set, when iterated $\mathbf{m}$ times, is the identity. In symbols, $\mathbf{m}f = f$. Here the $\mathbf{m}$-fold iteration of f is expressed by the Church number $\mathbf{m}$.

One could then reach a contradiction if one could simply exhibit a finite set X and a map whose $\mathbf{m}$-th iterate is not the identity. The crucial question here is, what is the order of successor, considered as a permutation of the loop? Intuitively it seems that it should be $\mathbf{m}$, the length of the loop. That assertion, however, is equivalent to the unstratified formula

$$j \in \mathbb{N} \to j\mathsf{S}\mathbf{n} = \mathbf{n} \oplus j,$$

which in turn is equivalent to the Church counting axiom,

$$j \in \mathbb{N} \to j\mathsf{S}\mathbf{0} = j.$$

That unstratified formula, although expressing a fundamental truth about the Church numbers, seems to be unprovable in NF. If we assume the Church counting axiom, then it is a routine exercise to define a permutation of the loop that leaves one element unmoved while cycling the rest, and that permutation will have order $\mathbf{m} - 1$, and hence will not satisfy the Annihilation Theorem. That will show that $\mathbb{N}$ is not finite; and we can go further and prove that $\mathbb{N}$ is actually infinite, and Heyting's arithmetic is thus interpretable in INF plus the counting axiom.

Without the counting axiom, one can exhibit specific permutations of specific finite sets, for example, a permutation of order 3 or one of order 873 or one of order 24,569; so $\mathbf{m}$ must be larger than any integer with a name. In general we must think of the Church numbers as non-standard integers. The counting axiom is a way to outlaw certain non-standard integers. In general in NF set theory one cannot assert the existence of $\{x \in \mathbb{N} : P(x)\}$ unless P is stratified, though such sets do not lead to any known paradoxes. Of course this separation axiom would imply the counting axiom. Without the counting axiom, the order $\mathbf{q}$ of the loop might be smaller than $\mathbf{m}$; in fact the quotient $\mathbf{m}/\mathbf{q}$ would itself be a non-standard integer, and the map $x \mapsto x\mathsf{S}\mathbf{n}$ (which is not definable in NF because the formula is not stratified) would take a small initial part of the loop onto the whole loop, and as x increases past q, $x\mathsf{S}\mathbf{n}$ would wrap around the loop many times before x reached $\mathbf{m}$. It would be interesting to see models of NF in which the Church counting axiom fails; but then again, it would be interesting to see models of NF at all.

Previous studies of infinity in NF have used the "Frege cardinals" $\mathbb{F}$, defined as the least set containing $\mathsf{zero} := \{\Lambda\}$ and closed under inhabited successor, where the Frege successor of x is x^+, the set of all $x \cup \{c\}$ such that $c \notin x$.[3] Of course there are natural functions defined from $\mathbb{N}$ to $\mathbb{F}$ and vice-versa, but nothing about these functions is obvious. If $\mathbb{F}$ is finite, then there is a maximum integer max, containing a set U that is "unenlargeable" in the sense that no c can be produced such that $c \notin U$, in spite of the fact that the universe $\mathbb{V}$ is infinite. In that case there are several possibilities: max might come "too soon", so that there are "not enough" Frege numbers to correspond to all the Church numbers. Or, max might be "too big", so that the correspondence is no longer one-to-one, as the Frege numbers start to wrap the "loop" a second time. Possibly max is "just right" and the Frege numbers correspond to the Church numbers in one-to-one fashion. If $\mathbb{N}$ and $\mathbb{F}$ are both finite, there is no obvious relation between their cardinalities.

If $\mathbb{N}$ is infinite, then of course $\mathbb{F}$ is infinite too, since there are arbitrarily large finite sets, namely initial segments of $\mathbb{N}$. On the other hand, if $\mathbb{F}$ is infinite, then we can prove that $\mathbb{N}$ is infinite too, since if $\mathbb{F}$ is infinite, we can show that every Church number is the order of some permutation, but that contradicts the Annihilation Theorem. Taken together with Specker's result that $\mathbb{F}$ is infinite in classical NF, we see that classical NF does prove that $\mathbb{N}$ is infinite.

In the final section of the paper, we prove that the Church counting axiom and the Rosser counting axiom are equivalent. The proof uses our main result that the Church counting axiom implies $\mathbb{N}$ is infinite and Church successor is one-to-one. This equivalence is proved in INF, without any assumptions.

We refer to [1] for notation, axioms, and the basic theorems of INF, including the properties of finite sets and finite cardinals. In particular we use $\mathbb{F}$ for the set of finite (Frege) cardinals. In this paper we make no use of arithmetic on the Frege cardinals, not even addition, let alone multiplication and exponentiation. What we mostly require from [1] is the intuitionistic theory of finite sets. Lemmas, theorems, and definitions from that [1] will be referenced like this: Lemma 3.3 of [1].

Thanks to Thomas Forster for asking me (once a year for twenty years) about the strength of INF. Thanks to Randall Holmes for his attention to my first draft,

[3]Actually, Rosser and Spector used Nn, defined as the least set containing zero and closed under successor; so possibly Nn might contain Λ, while $\mathbb{F}$ certainly does not contain Λ. Therefore we use a different letter.

and for the idea of the proof of Lemma 4.2. Thanks to Albert Visser for his careful reading of an earlier version; many errors were thus corrected. Thanks to the creators of the proof assistant Lean [3], which has enabled me to state with high confidence that there are no errors in this paper. Thanks to the users of Lean who helped me acquire sufficient expertise in using Lean by answering my questions, especially Mario Carneiro.[4]

There are many lemmas in this paper, and the intention is that each of those lemmas is provable in INF. Inductions are stratified and proofs are intuitionistically valid. When the counting axiom is used, it is explicitly mentioned as a hypothesis.

2. The Church numbers

We define the class of single-valued relations:

Definition 2.1.

$$\mathsf{FUNC} = \{f : \forall x, y, z\,(\langle x, y\rangle \in f \to \langle x, z\rangle \in f \to y = z)\}.$$

The definition does not rule out the possibility that f might contain some members that are not ordered pairs. A function is a single-valued relation, i.e. $f \in \mathsf{FUNC} \ \wedge \ Rel(f)$.

If $f \in \mathsf{FUNC}$ and $\langle x, y\rangle \in f$, then informally we write $y = f(x)$. Formally this is $y = Ap(f, x)$, where Ap is a function symbol defined using stratified comprehension. For details about Ap see Definition 2.6 of [1] and Lemma 2.7 of [1]. We will often suppress mention of the symbol Ap, as there is no other way to interpret $f(x)$. In fact, we will informally follow the λ-calculus convention of writing (fx) or just fx for function application, with association to the left, so fxy means $((fx)y)$.

The Church successor function S is defined in λ-calculus by

$$\mathsf{S}(z) \quad = \quad \lambda f \lambda x f(zfx)$$

Imitating this definition in NF we wish we could define

$$\mathsf{S} \quad = \quad \{\langle z, \{\langle f, \{\langle x, f(zfx)\rangle\}\rangle\}\rangle\}$$

Expanding the formula on the right, it is equivalent, at least for functions f and z, to the formula in the following definition. To explain the relation between the two formulas, $t = zf$, $q = tx = zfx$, $w = fq = f(zfx)$. But we emphasize, everything about Church successor up to this point is merely motivation for the definition below.

Definition 2.2. *Church successor is defined by*

$$\begin{aligned}&\mathsf{S} = \{\langle z, \{\langle f, p\rangle : f \in \mathsf{FUNC} \ \wedge \\ &\forall u\,(u \in p \leftrightarrow \exists x, w, t, q\,(u = \langle x, w\rangle \ \wedge \ t \in \mathsf{FUNC} \ \wedge \\ &\langle f, t\rangle \in z \ \wedge \ \langle x, q\rangle \in t \ \wedge \ \langle q, w\rangle \in f))\} : z \in \mathsf{FUNC}\}\end{aligned}$$

Lemma 2.3. *The definition of Church successor can be given in* INF *using stratified comprehension; that is, the graph of Church successor is definable in* INF*.*

Proof. To stratify the formula in Definition 2.2, we assign indices as follows:

[4] Although the proofs in this paper have been computer-checked for correctness using Lean, they are presented here in human-readable form with detailed proofs. Issues concerning the notation in Lean will not be discussed here.

$$\begin{array}{rl} x,\ q,\ \text{and}\ w & 0 \\ u, \langle x,q\rangle,\ \text{and}\ \langle q,w\rangle & 2 \\ p,\ t\ \text{and}\ f & 3 \\ \langle f,t\rangle & 5 \\ z & 6 \end{array}$$

With this assignment, the left and right members of ordered pairs get the same index, and the formula is stratified. $t \in \mathsf{FUNC}$ can be stratified assigning t any desired index ≥ 2, and that condition is satisfied by the assignments in the table. That completes the proof.

Lemma 2.4. *Let $f \in \mathsf{FUNC}$ and $z \in \mathsf{FUNC}$. Then $\mathsf{S}zf$ is a relation (contains only ordered pairs).*

Proof. Suppose $t \in \mathsf{S}zf$. We have to prove t is an ordered pair. Officially $\mathsf{S}zf$ is $Ap(\mathsf{S}z, f)$. By definition of Ap, there exists y such that $\langle f,y\rangle \in \mathsf{S}z$ and $t \in y$. Then by definition of Church successor, $z \in \mathsf{FUNC}$ and $f \in \mathsf{FUNC}$ and for every u,

$$u \in y \leftrightarrow \exists x,w,r,q\,(u = \langle x,w\rangle \ \wedge\ r \in \mathsf{FUNC} \ \wedge\ \langle f,r\rangle \in z \ \wedge\ \langle x,q\rangle \in r \ \wedge\ \langle q,w\rangle \in f).$$

Instantiate the quantified u to t; then $t = \langle x,w\rangle$ for some x and w. That completes the proof of the lemma.

Lemma 2.5. *Let $f \in \mathsf{FUNC}$ and $z \in \mathsf{FUNC}$. Then*

$$\mathsf{S}zf \quad = \quad \{\langle x,w\rangle : \exists t,q\,(t \in \mathsf{FUNC} \wedge \langle f,t\rangle \in z \wedge \langle x,q\rangle \in t \wedge \langle q,w\rangle \in f)\}$$

Proof. Let $f \in \mathsf{FUNC}$ and $z \in \mathsf{FUNC}$. By Lemma 2.4, it suffices to prove

$$\langle x,w\rangle \in Ap(\mathsf{S}z,f) \leftrightarrow \exists t,q\,(t \in \mathsf{FUNC} \ \wedge\ \langle f,t\rangle \in z \ \wedge\ \langle x,q\rangle \in t \ \wedge\ \langle q,w\rangle \in f)$$

Left to right: Assume $\langle x,w\rangle \in Ap(\mathsf{S}z,f)$. By Definition 2.6, that assumption is equivalent to

$$\exists y\,(\langle\langle f,y\rangle, z\rangle \in \mathsf{S} \ \wedge\ \langle x,y\rangle \in y.$$

it suffices to prove

$$t \in y \leftrightarrow \exists y\,(\langle x,y\rangle \in f \ \wedge\ t \in y.$$

Applying the definition of Church successor, in a few steps we obtain

$$t \in \mathsf{FUNC} \ \wedge\ \langle f,t\rangle \in z \ \wedge\ \langle x,q\rangle \in f \ \wedge\ \langle q,w\rangle \in f.$$

That completes the left-to-right direction.

Right to left: Assume

$$t \in \mathsf{FUNC} \ \wedge\ \langle f,t\rangle \in z \ \wedge\ \langle x,q\rangle \in t \ \wedge\ \langle q,w\rangle \in f.$$

We have to prove $\langle x,w\rangle \in Ap(\mathsf{S}z,f)$. Applying the definitions of Ap and S, we find that it suffices to prove

$$\begin{aligned} &\exists y\,(z \in \mathsf{FUNC} \wedge\ \exists g,p\,(\langle f,y\rangle = \langle g,p\rangle \ \wedge\ g \in \mathsf{FUNC} \ \wedge \\ &\forall x,w\,(\langle x,w\rangle \in p \leftrightarrow \exists t,q\,(t \in \mathsf{FUNC} \ \wedge\ \langle g,t\rangle \in z \ \wedge\ \langle x,q\rangle \in t \ \wedge\ \langle q,w\rangle \in g))) \\ &\wedge \langle x,w\rangle \in y). \end{aligned}$$

Now we choose

$$Y := \{\langle x,w\rangle : \exists t,q\,(t \in \mathsf{FUNC} \ \wedge\ \langle f,t\rangle \in z \ \wedge\ \langle x,q\rangle \in t \ \wedge\ \langle q,w\rangle \in f.\}$$

(It is important to quantify over t and q even though there are free variables t and q in scope here.) The formula is stratified giving x,w,t,q index 0 and z,f index

3; FUNC is a parameter. Hence the definition can be given in INF. Using Y to instantiate $\exists y$, we have to prove

$$\begin{aligned}&z \in \mathsf{FUNC} \wedge\ \exists g, p\,(\langle f, Y\rangle = \langle g, p\rangle\ \wedge\ g \in \mathsf{FUNC}\ \wedge\\ &\forall x, w\,(\langle x, w\rangle \in p \leftrightarrow \exists t, q\,(t \in \mathsf{FUNC}\ \wedge\ \langle g, t\rangle \in z\ \wedge\ \langle x, q\rangle \in t\ \wedge\ \langle q, w\rangle \in g)))\\ &\wedge \langle x, w\rangle \in Y.\end{aligned}$$

We have $z \in \mathsf{FUNC}$ and $t \in \mathsf{FUNC}$; take $g = f$ and $p = Y$; then it suffices to prove

$$\begin{aligned}&\forall x, w\,(\langle x, w\rangle \in Y \leftrightarrow \exists t, q\,(t \in \mathsf{FUNC}\ \wedge\ \langle f, t\rangle \in z\ \wedge\ \langle x, q\rangle \in t\ \wedge\ \langle q, w\rangle \in f)))\\ &\wedge \langle x, w\rangle \in Y).\end{aligned}$$

The first line follows from the definition of Y. It remains to prove $\langle x, w\rangle \in Y$. Note that in the last line, x and w are free variables. We have by assumption

$$\langle f, t\rangle \in z\ \wedge\ \langle x, q\rangle \in t\ \wedge\ \langle q, w\rangle \in f.$$

Then by definition of Y we have $\langle x, w\rangle \in Y$, as desired. That completes the proof of the lemma.

Lemma 2.6. *For all z, $z \in \mathsf{FUNC} \to \mathsf{S}z \in \mathsf{FUNC}$.*

Proof. Immediate from Definition 2.2.

Lemma 2.7. *For all z, $\mathsf{S}z$ is a relation.*

Remark. Since our definition of FUNC does not require a function to be a relation (i.e., contain only ordered pairs), this lemma adds something to the previous lemma.

Proof. Immediate from Definition 2.2.

Definition 2.8. *$f : \mathbb{N} \to \mathbb{N}$ means $f \in \mathsf{FUNC}$ and for each $n \in \mathbb{N}$ there is a unique $m \in \mathbb{N}$ such that $\langle n, m\rangle \in f$.*

The concept just defined does not prevent the domain of f from being larger than $\mathbb{N}$.

Definition 2.9. *id is the identity function, $\{\langle x, x\rangle : x = x\}$.*

Definition 2.10. *$\mathbf{0}$ is the function $\lambda f\, x.x$, which as a set of ordered pairs is*

$$\{\langle f, \mathsf{id}\,\rangle : f = f\},$$

Remark. Then $\mathbf{0} : X \to X$ for any set X, but the domain of $\mathbf{0}$ is the whole universe, usually larger than X.

Lemma 2.11. $\mathbf{0} \in \mathsf{FUNC}$.

Proof. Immediate from the definition of $\mathbf{0}$.

Lemma 2.12. *For all x, $\mathbf{0}x = \mathsf{id}$, the identity function.*

Proof. By definition of $\mathbf{0}$, $\langle f, u\rangle \in \mathbf{0}$ if and only if $u = \mathsf{id}$. Then for any f, $\langle f, \mathsf{id}\rangle \in \mathbf{0}$, so by Lemma 2.7 of [1], we have $\mathsf{id} = Ap\,(\mathbf{0}, f) = \mathbf{0}f$ as desired. That completes the proof.

Lemma 2.13. *For all x, $\mathbf{0}fx = x$.*

Proof. By Lemma 2.12, $\mathbf{0}f$ is the identity function. It follows from Lemma 2.7 of [1] that $x = Ap((\mathbf{0}f), x)$. Suppressing explicit mention of Ap, that is $\mathbf{0}fx = x$. That completes the proof of the lemma.

Lemma 2.14. *For all f, $f \in \mathsf{FUNC} \to Rel(f) \to \mathsf{S}\mathbf{0}f = f$.*

Proof Lemma 2.5, with z in the lemma set to $\mathbf{0}$,

$$\mathsf{S}\mathbf{0}f \quad = \quad \{\langle x, w\rangle : \exists t, q\,(t \in \mathsf{FUNC} \land \langle f, t\rangle \in \mathbf{0} \land \langle x, q\rangle \in t \land \langle q, w\rangle \in f)\}$$

By the definition of $\mathbf{0}$, $\langle f, t\rangle \in \mathbf{0}$ is equivalent to $t = \mathsf{id}$; then $\langle x, q\rangle \in t$ is equivalent to $x = q$, and we have

$$\begin{aligned} \mathsf{S}\mathbf{0}f \quad &= \quad \{\langle x, w\rangle : \langle x, w\rangle \in f\} \\ &= \quad f \qquad \text{by extensionality and } Rel(f) \end{aligned}$$

Definition 2.15. *The set of Church numbers is the least set containing $\mathbf{0}$ and closed under Church successor S. That is, it is the intersection of all sets containing $\mathbf{0}$ and closed under S.*

Theorem 2.16. *The set of Church numbers is definable (by stratified formulas) in* INF.

Proof. By Lemma 2.3, S is definable in NF. Then

$$\mathbb{N} = \{\ x : \forall X(0 \in X \land \forall u \in X(\mathsf{S}u \in X)) \to x \in X\ \}$$

In other words,

$$\mathbb{N} = \{\ x : \exists z(z = 0) \land \forall X(z \in X \land \forall u \in X \exists v(v = \mathsf{S}u \land v \in X)) \to x \in X\ \}$$

To check that this definition is legal in NF, we stratify the formula on the right, giving v and u the same index, say 6, since S is a function. Then X gets index 7 and x and z get index 6. As discussed above we can stratify $z = 0$ giving z any index ≥ 3, so 6 is OK. $\mathbb{N}$ is a parameter and does not need an index. This stratification shows that $\mathbb{N}$ is well-defined in NF. That completes the proof of the theorem.

Lemma 2.17 (Proof by induction)**.**

$$\mathbf{0} \in x \land \forall n \in \mathbb{N}(n \in x \to \mathsf{S}n \in x) \to \forall k \in \mathbb{N}\,(k \in x).$$

Proof. By Definition 2.15 and Theorem 2.16, $\mathbb{N}$ is the intersection of all sets closed under successor. There is at least one such set, since $\mathbb{V}$ is closed under successor and contains 0, so $\mathbb{N}$ is not empty. Then x contains 0 and is closed under successor. Hence $\mathbb{N} \subseteq x$. That completes the proof.

Remark. If we wish to prove a stratified formula ϕ "by induction on n", we use stratified comprehension to define $x = \{n : \phi(n)\}$, and then prove the "base case" that $\Phi(0)$and the "induction step" that $\phi(n) \to \phi(\mathsf{S}n)$. Then $\mathbf{0} \in x$ and $n \in x \to \mathsf{S}n \in x$. Then Lemma 2.17 can be used to conclude that $\mathbb{N} \subseteq x$. Hence $\forall n \in \mathbb{N}\,\phi(n)$.

Lemma 2.18. $\mathbf{0} \in \mathbb{N}$.

Lemma 2.19. $\mathsf{S} : \mathbb{N} \to \mathbb{N}$

Proof. By definition $\mathbb{N}$ is the intersection of all sets containing $\mathbf{0}$ and closed under successor. Therefore $\mathbf{0} \in \mathbb{N}$. That completes the proof of the lemma.

Proof. By definition $\mathbb{N}$ is the intersection of all sets containing $\mathbf{0}$ and closed under successor. Let $n \in \mathbb{N}$. Then n belongs to every set X containing $\mathbf{0}$ and closed under successor. Hence $\mathsf{S}n$ belongs to every such set X. Hence $\mathsf{S}n$ belongs to $\mathbb{N}$. That completes the proof of the lemma.

Lemma 2.20. *Every Church number n is a function.*

Proof. By induction on n.

Base case: $\mathbf{0} \in \mathsf{FUNC}$ by Lemma 2.11.

Induction step: Suppose $n \in \mathbb{N}$ and $n \in \mathsf{FUNC}$. By Lemma 2.6, $\mathsf{S}n \in \mathsf{FUNC}$. That completes the induction step. That completes the proof of the lemma.

Lemma 2.21. *Every Church number n is a relation.*

Proof. By induction on n, similar to Lemma 2.20, but appealing to Lemma 2.7 in the induction step.

Lemma 2.22. *Let $n \in \mathsf{FUNC}$ and $f \in \mathsf{FUNC}$. Then there exists y such that $\langle f, y\rangle \in \mathsf{S}n$.*

Proof. Let n and f be given, with $n \in \mathsf{FUNC}$ and $f \in \mathsf{FUNC}$. Define

$$y := \{\langle x, z\rangle : \langle f, p\rangle \in n \ \wedge\ \langle x, q\rangle \in p \ \wedge\ \langle q, z\rangle \in f \ \wedge\ p \in \mathsf{FUNC}\}.$$

The formula defining y is stratified, giving x, z, and q index 0; then $\langle x, q\rangle$ gets index 2, so p gets index 3. Then f gets index 3 and $\langle f, p\rangle$ gets index 5, so n gets index 6. Therefore the formula is stratified, and the definition of y is legal.

The verification that $\langle f, y\rangle \in \mathsf{S}n$ then proceeds by unfolding the definitions of $\mathsf{S}n$ and y. We omit the 65 routine steps of this verification.

3. Iteration of a function

If we have a mapping $f : X \to X$, we can iterate it j times. Often mathematicians write the j-times iterated mapping as f^j, or if there is danger of confusion, as $f^{(j)}$. Formally it is just jf, where j is a Church number. In treating this subject rigorously one has to distinguish the relevant concepts precisely. Namely, we have

$$\begin{aligned} f : X \to Y \\ Rel(f) \\ f \in \mathsf{FUNC} \\ oneone(f, X, Y) \end{aligned}$$

$Rel(f)$ means that all the members of f are ordered pairs. $f \in \mathsf{FUNC}$ means that two ordered pairs in f with the same first member have the same second member. (Nothing is said about possible members of f that are not ordered pairs.) $f : X \to Y$ means that if $x \in X$, there is a unique y such that $\langle x, y\rangle \in f$ and that y is in Y. (But nothing is said about $\langle x, y\rangle \in f$ with $x \notin X$.) "f is one-to-one from X to Y", or $oneone(f, X, Y)$, means $f : X \to Y$ and in addition, if $\langle x, y\rangle \in f$ and $\langle u, y\rangle \in f$ then $x = u$, and if $y \in Y$ then $x \in X$. (So $x = u$ does not require $y \in Y$ or $x \in X$.) In particular, $f : X \to Y$ does not require $domX \subseteq X$, so the identity function maps X to X for every X; but the identity function (on the universe) has to be restricted to X before it is one-to-one.

We shall be mostly concerned with iterations of a map f from some set X to that same set. In that setting the following concept is useful.

Definition 3.1. *f is a* **permutation** *of a finite set X if and only if $f : X \to X$, and $Rel(f)$ and $f \in \mathsf{FUNC}$, and $dom(f) \subseteq X$, and f is both one-to-one and onto from X to X.*

But for some purposes, we don't need f to be onto, but we still need it to be a relation and a function and to control its range and domain. Therefore we define

Definition 3.2. *f is an* **injection** *of a set X into Y if and only if $f : X \to Y$, and $Rel(f)$ and $f \in \mathsf{FUNC}$, and $dom(f) \subseteq X$, and f is one-to-one from X to X.*

Note that the definition does not require X to be finite.

Any function can be iterated, even if it doesn't map some X to itself:

Lemma 3.3. *Let $n \in \mathbb{N}$ and $f \in \mathsf{FUNC}$. Then there exists y such that $\langle f, y\rangle \in n$.*

Proof. The formula is stratified, so we may prove it by induction.

Base case: By the definition of Church zero, we have $\langle f, \mathsf{id}\rangle \in \mathbf{0}$.

Induction step: By Lemma 2.22. That completes the induction step. That completes the proof of the lemma.

Lemma 3.4. *Let $n \in \mathbb{N}$ and suppose $f \in \mathsf{FUNC}$ and $Rel(f)$. Then $nf \in \mathsf{FUNC}$ and $Rel(nf)$.*

Proof. By induction on n, which is legal since the formula is stratified. (Although $Ap(n, f)$ gets the same type as f, that observation is not even needed here, as FUNC is just a parameter, so f can be given any type and it doesn't matter what type nf gets.)

Base case: $\mathbf{0}f$ is the identity function, by definition of $\mathbf{0}$. Since the identity function is also a a relation, that completes the base case (though it requires 24 steps, here omitted, to spell out the details).

Induction step: Suppose $f \in \mathsf{FUNC}$ and $n \in \mathbb{N}$ and $nf \in \mathsf{FUNC}$. By Lemma 2.5, we have

$$(1) \quad \mathsf{S}nf \quad = \quad \{\langle x, w\rangle : \exists t, q\,(t \in \mathsf{FUNC} \wedge \langle f, t\rangle \in n \wedge \langle x, q\rangle \in t \wedge \langle q, w\rangle \in f)\}$$

Then $\mathsf{S}nf$ is a relation. We next will prove $\mathsf{S}nf \in \mathsf{FUNC}$. Suppose $\langle x, y\rangle \in \mathsf{S}nf$ and $\langle x, z\rangle \in \mathsf{S}nf$. We must prove $y = z$. By (1) there exist t_1, q_1 and t_2, q_2 such that

$$\begin{gathered}
\mathsf{FUNC}(t_1) \\
\mathsf{FUNC}(t_2) \\
\langle f, t_1\rangle \in n \\
\langle f, t_2\rangle \in n \\
\langle x, q_1\rangle \in t_1 \\
\langle x, q_2\rangle \in t_2 \\
\langle q_1, y\rangle \in f \\
\langle q_2, z\rangle \in f
\end{gathered}$$

Using the definition of FUNC several times we obtain, in order, $t_1 = t_2$, then $q_1 = q_2$, and finally $y = z$. That completes the induction step. That completes the proof of the lemma.

Lemma 3.5. *Let X be any set. Suppose $f : X \to X$ and $f \in \mathsf{FUNC}$ and $Rel(f)$). Then for all $n \in \mathbb{N}$ and $x \in X$,*

$$\langle f, nf\rangle \in n \ \wedge \ nf : X \to X$$

Proof. Let $f \in \mathsf{FUNC}$ and $Rel(f)$ and $f : \mathbb{N} \to \mathbb{N}$. By Lemma 2.7 of [1], $\langle f, nf\rangle \in n$ is equivalent to $\exists y\,(\langle f, y\rangle \in n)$.

The formula is stratified, giving X index 1, f index 3 (since the members of f are ordered pairs of members of X), x index 0; nf gets index 3, since n is a function by Lemma 2.20; so we have to give n index 6, since its members are pairs of objects of type 3.

Base case: By Lemma 2.11, $\mathbf{0}$ is a function, and by definition of $\mathbf{0}$, $\mathbf{0}f$ is the identity function, so $\mathbf{0}f : X \to X$. That completes the base case.

Induction step: We first have to show that $\langle f, \mathsf{S}nf\rangle \in \mathsf{S}n$. By Lemma 2.22, we have $\exists y\,(\langle f, y \in \mathsf{S}n)$. Then by Lemma 2.7 of [1], we have $\langle f, \mathsf{S}nf\rangle \in \mathsf{S}n$, as claimed.

We turn to the proof that $\mathsf{S}nf : X \to X$. By Lemma 2.20, n is a function, and by Lemma 3.4, nf is a function. Then according to Lemma 2.5, we have

$$\mathsf{S}nf \quad = \quad \{\langle x, w\rangle : \exists t, q\,(t \in \mathsf{FUNC} \wedge \langle f, t\rangle \in n \wedge \langle x, q\rangle \in t \wedge \langle q, w\rangle \in f)\} \tag{2}$$

Let $x \in X$. By Lemma 3.3, $\langle f, t\rangle \in n$ for some t; by Lemma 2.7 of [1], $t = nf$. By the induction hypothesis, $nf : X \to X$, so there exists q with $\langle x, q\rangle \in t$ and $q \in X$. Then since $f : X \to X$, there exists w with $\langle q, w\rangle \in f$. Then by (2), we have $\langle x, w\rangle \in \mathsf{S}nf$. Since x was arbitrary, we have proved $\mathsf{S}nf : X \to X$. That completes the induction step. That completes the proof of the lemma.

Theorem 3.6 (successor equation)**.** *Let X be any set and f any function ($f \in \mathsf{FUNC}$ and $Rel(f)$) with $f : X \to X$. Then for all $n \in \mathbb{N}$ and $x \in X$,*

$$\mathsf{S}nfx = f(nfx).$$

Proof. Let $f : X \to X$ and $n \in \mathbb{N}$ and $x \in X$. By Lemma 2.20, n is a function, and by Lemma 3.4, nf is a function. Then according to Lemma 2.5, we have

$$\mathsf{S}nf \quad = \quad \{\langle x, w\rangle : \exists t, q\,(t \in \mathsf{FUNC} \wedge \langle f, t\rangle \in n \wedge \langle x, q\rangle \in t \wedge \langle q, w\rangle \in f)\}$$

By Lemma 3.5, $nf : X \to X$. Then as in the proof of that lemma, we have $t = nf$, $q = tx = nfx$, and $w = fq$, with $\langle x, w\rangle \in \mathsf{S}nf$. That completes the proof of the theorem.

Lemma 3.7. *Define* $1 := \mathsf{S}0$. *Then* $1 \neq 0$.

Proof. Let f and z be functional relations. Then by Lemma 2.4, $\mathsf{S}zf$ is a relation, and by Lemma 2.5,

$$\langle x, w\rangle \in \mathsf{S}zf \quad \leftrightarrow \quad \exists t, q(t \in \mathsf{FUNC} \wedge \langle f, t\rangle \in z \wedge \langle x, q\rangle \in t \wedge \langle q, w\rangle \in f)$$

Take $z = 0$. Then on the right, $t = zf$ and $q = tx = zfx = x$ since $z = 0$. Then $w = fx$. Thus

$$\langle x, w\rangle \in \mathsf{S}0f \quad = \quad \langle x, w\rangle \in f$$

By Lemma 2.22, $\mathsf{S}0f$ is a relation, and by hypothesis f is a relation. Therefore

$$\forall u\,(u \in \mathsf{S}0f \leftrightarrow u \in f).$$

Then by extensionality, $1f = f$, for all functional relations f.

Now suppose, for proof by contradiction, that $1 = 0$. Then on the one hand, $1f = f$, and on the other hand $1f = 0f = \mathsf{id}$. Now we can get a contradiction by exhibiting some (any) functional relation f that is not the identity. For example, we can use $f = \{\langle \Lambda, \{\Lambda\}\}$. It is easily verified that f is a functional relation and is not equal to id. That completes the proof of the lemma.

Remark. The proof does not follow immediately from Theorem 3.6, it seems. For if we assume $1 = 0$, that equation says

$$1fx \;=\; \mathsf{S}0fx \;=\; f(0fx)$$

and since we have assumed $1 = 0$, also $1fx = 0fx$. But by definition of 0, we have $0fx = x$. Thus $x = 0fx = 1fx = f(0fx) = fx$. Hence f is the identity function on $\mathbb{N}$. That is, however, not yet a contradiction.

Theorem 3.8. *The Church successor function does not take the value* $\mathbf{0}$ *on* $\mathbb{N}$*; that is,* $n \in \mathbb{N} \to \mathsf{S}n \neq \mathbf{0}$.

Proof. Let a and b be any two unequal members of $\mathbb{N}$; by Lemma 3.7 there do exist two unequal members of $\mathbb{N}$. Let f be the constant function with value a. Then $f : \mathbb{N} \to \mathbb{N}$. Suppose, for proof by contradiction, that $\mathsf{S}(z) = 0$. Applying both sides to f and b we have, by the definitions of S and 0,

$$\begin{array}{rcll} \mathsf{S}zfb &=& 0fb & \\ f(zfb) &=& 0fb & \text{by Theorem 3.6} \\ f(zfb) &=& b & \text{since } 0fb = b \text{ by definition of } 0 \\ a &=& b & \text{since } f(u) = a \text{ for all } u \end{array}$$

But that contradicts $a \neq b$. That completes the proof of the theorem.

Remark. All we needed to prove that successor omits the value 0 is that there is some function $f : \mathbb{N} \to \mathbb{N}$ that omits some value; and we can construct such a function if there are two distinct members of $\mathbb{N}$.

Lemma 3.9 (Predecessor)**.** *If* $n \in \mathbb{N}$ *and* $n \neq \mathbf{0}$*, then* $n = \mathsf{S}m$ *for some* $m \in \mathbb{N}$.

Remark. The predecessor is, of course, not asserted to be unique.

Proof. By induction on x we prove that $x \in \mathbb{N} \to x \neq 0 \to \exists y \in \mathbb{N}\,(\mathsf{S}y = x)$. The base case and induction step are both immediate.

Lemma 3.10. $\forall n \in \mathbb{N}\,(n = \mathbf{0} \;\vee\; n \neq \mathbf{0})$.

Proof. By induction on n, which is legal since the formula is stratified. The base case is immediate; and the induction step is immediate from Theorem 3.8. That completes the proof of the lemma.

Lemma 3.11. *Suppose* $f : X \to X$*, and* $f \in \mathsf{FUNC}$ *and* $Rel(f)$*, and* $dom(f) \subseteq X$*. Let* $n \in \mathbb{N}$ *and suppose* $n \neq \mathbf{0}$*. Then* $dom(nf) \subseteq X$*.*

Remark. When $n = \mathbf{0}$, nf is the identity function, whose domain is $\mathbb{V}$. Hence the restriction $n \neq \mathbf{0}$ is necessary.

Proof. By induction on n, which is legal since the formula is stratified. Base case: there is nothing to prove because of the hypothesis $n \neq \mathbf{0}$.

Induction step: Assume $\mathsf{S}n \neq \mathbf{0}$. By Lemma 3.10, $n = \mathbf{0} \;\vee\; n \neq \mathbf{0}$. We argue by cases accordingly.

Case 1, $n = \mathbf{0}$. We have to show $dom(\mathsf{S}\mathbf{0}f) \subseteq X$. Suppose $x \in dom(\mathsf{S}nf)$. It suffices to show $x \in X$. By Lemma 2.14, $\mathsf{S}\mathbf{0}f = f$. Therefore $x \in dom(f)$. Since $dom(f) \subseteq X$, we have $x \in X$ as desired. That completes Case 1.

Case 2, $n \neq \mathbf{0}$. By Lemma 3.4, we have $nf \in \mathsf{FUNC}$ and $Rel(nf)$, and also $\mathsf{S}nf \in \mathsf{FUNC}$ and $Rel(\mathsf{S}nf)$. Suppose $\langle x, y\rangle \in \mathsf{S}nf$. We must show $x \in X$. Since $\mathsf{S}nf \in \mathsf{FUNC}$, we have $y = (\mathsf{S}nf)x$. By Lemma 2.5, we have

$$x \in dom(\mathsf{S}nf) \leftrightarrow \exists w, t, q\, (t \in \mathsf{FUNC} \ \wedge \ \langle f, t\rangle \in n \ \wedge \ \langle x, q\rangle \in t \ \wedge \ \langle q, w\rangle \in f)$$

Suppose $x \in dom(\mathsf{S}nf)$. Then for some w, t, q we have

$$t \in \mathsf{FUNC} \ \wedge \ \langle f, t\rangle \in n \ \wedge \ \langle x, q\rangle \in t \ \wedge \ \langle q, w\rangle \in f$$

Then by Lemma 2.7 of [1], $t = nf$. By the induction hypothesis, $dom(nf) \subseteq X$. Since $\langle x, q\rangle \in t$ and $t = nf$, we have $x \in dom(nf)$ and hence $x \in X$. That completes Case 2. That completes the induction step. That completes the proof of the lemma.

Lemma 3.12. *Suppose $f \in \mathsf{FUNC}$ and $Rel(f)$, and $f : X \to X$ and $m \in \mathbb{N}$ and mf is one-to-one from X to X, and $dom(f) \subseteq X$. Then $\mathsf{S}mf : X \to X$, and $\mathsf{S}mf$ is one-to-one.*

Proof. Suppose $\mathsf{S}mx = \mathsf{S}mz$. I say $x = z$. We have

$$\begin{aligned} \mathsf{S}mfx &= f(mfx)) && \text{by Theorem 3.6}\\ \mathsf{S}mfz &= f(mfz)) && \text{Theorem 3.6}\\ f(mfx) &= f(mfz) && \text{by the preceding two lines}\\ x &= z && \text{since } mf \text{ is one-to-one} \end{aligned}$$

Technically, however, the definition of one-to-one involves more than just $x = z$. We have

$$\mathsf{S}mf \in \mathsf{FUNC} \qquad \text{by Lemma 3.4}$$

We also have to show that mf is a relation, that its domain is a subset of X, and that its range is a subset of X. These verifications require about 100 proof steps (here omitted), using for example Lemmas 2.20 and 2.20 and 3.11. That completes the proof of the lemma.

Lemma 3.13. *Let X be any set, and let $f : X \to X$ be a permutation. Let $m \in \mathbb{N}$. Then $mf : X \to X$ for $m \neq \mathbf{0}$, mf is a permutation.*

Remark. When $m = \mathbf{0}$, mf is the identity function, which has domain $\mathbb{V}$, so it is not a permutation of X (unless $X = \mathbb{V}$).

Proof. By induction on m. The formula is stratified, as we have already checked that "one-to-one" and "$f : X \to X$" are stratified.

Base case, when $m = \mathbf{0}$ we have $mf = \mathsf{id}$, by definition of $\mathbf{0}$, and the identity function maps X to X, and the identity function is one-to-one. That completes the base case.

Induction step. Suppose $mf : X \to X$ is one-to-one, and

$$m \neq \mathbf{0} \to range(mf) \subseteq X.$$

We must prove $\mathsf{S}mf : X \to X$ and $\mathsf{S}m$ is one-to-one. We have $m = \mathbf{0} \ \vee \ m \neq \mathbf{0}$, by Lemma 3.10. We argue by cases.

Case 1: $m = \mathbf{0}$. Then $mf = f$, so by hypothesis, mf is a permutation of X.

Case 2: $m \neq \mathbf{0}$. Assume $x \in X$. Then by Lemma 3.12, $\mathsf{S}mf : X \to X$ and $\mathsf{S}mf$ is one-to-one. That completes Case 2. That completes the induction step. That completes the proof of the lemma.

4. Definition of addition on $\mathbb{N}$

In this section we define addition on $\mathbb{N}$ and prove some of its properties. To define the graph of a binary function we use ordered triples, which are defined in Definition 2.2 of [1].

Lemma 4.1. INF *can define a set* Sum *such that for* $x, n, y \in \mathbb{N}$

(i) $\langle x, 0, x\rangle \in Sum$*, and*

(ii) $\langle x, n, y\rangle \in Sum \to \langle x, \mathsf{S}n, \mathsf{S}y\rangle \in Sum$*, and*

(iii) Sum *is the intersection of all sets* X *satisfying those two conditions;*

Proof. Sum is the intersection of sets X satisfying conditions (i) and (ii) with Sum replaced by X. Specifically those conditions are

$$\begin{aligned} x \in \mathbb{N} \quad &\to \quad \langle x, 0, x\rangle \in X \\ x \in X \wedge y \in \mathbb{N} \wedge n \in \mathbb{N} \quad &\to \quad (\langle x, n, y\rangle \in X \to \langle x, \mathsf{S}n, \mathsf{S}y\rangle \in X) \end{aligned}$$

These formulas can be stratified by assigning x, y, and n all index 0, $\mathbb{N}$ index 1, and X index 5.

Then the conjunction of these two conditions, preceded by $\forall X$, is also stratifiable, and it defines Sum.

Now we must prove that Sum so defined satisfies the three conditions itself. Suppose $x \in \mathbb{N}$. Then $\langle x, 0, x\rangle$ belongs to every X satisfying the conditions. Hence it belongs to Sum. Hence Sum satisfies the first condition.

Suppose $x \in \mathbb{N}$ and $y \in \mathbb{N}$ and $n \in \mathbb{N}$. Suppose $\langle x, n, y\rangle \in Sum$. Then for every X satisfying the conditions, $\langle x, n, y\rangle \in X$. Then for every X satisfying the conditions, $\langle x, \mathsf{S}n, \mathsf{S}y\rangle \in X$. Then $\langle x, \mathsf{S}n, \mathsf{S}y\rangle \in Sum$. That verifies that Sum satisfies the second condition. That completes the proof of the lemma.

Lemma 4.2. INF *proves that for each* $x, n \in \mathbb{N}$*, there is a unique* $y \in N$ *such that* $\langle x, n, y\rangle \in Sum$*.*

Proof. (Holmes) First, by induction on n, there is some y such that $\langle x, n, y\rangle \in Sum$; the clauses (i) and (ii) in the definition yield the base case and induction steps, respectively. So it suffices to prove by induction on x that

$$\forall y \in \mathbb{N}\,(\langle x, y, z\rangle \in Sum \wedge \langle x, y, w\rangle \in Sum \to z = w).$$

Base case: Since $\langle 0, y, y\rangle \in Sum$, it suffices to prove that $\langle 0, y, z\rangle \in Sum$ implies $z = y$. To that end define

$$X = \{\langle x, y, z\rangle : x = 0 \to y = z\}.$$

That is legal as the formula is stratifiable. I say that X satisfies the closure conditions in the definition of Sum. Ad (i): We have $\langle x, 0, x\rangle \in X$, since $x = 0 \to 0 = x$. Ad (ii): Suppose $\langle x, y, z\rangle \in X$. We must show $\langle x, \mathsf{S}y, \mathsf{S}z\rangle \in X$. Since $\langle x, y, z\rangle \in X$, we have $x = 0 \to y = z$. Then also $x = 0 \to \mathsf{S}y = \mathsf{S}z$. Therefore $\langle x, \mathsf{S}y, \mathsf{S}z\rangle \in X$. Therefore X satisfies both closure conditions. Therefore Sum is a subset of X. Therefore $\langle 0, y, z\rangle \in Sum$ implies $y = z$, as desired. That completes the base case.

Induction step: The induction hypothesis is that (with x fixed) for every $y \in \mathbb{N}$, there is a unique $p \in \mathbb{N}$ such that $\langle x, y, p\rangle \in Sum$. We denote that unique p by $x \oplus y$. Suppose that

$$\langle \mathsf{S}x, y, z\rangle \in Sum \tag{3}$$

$$\langle \mathsf{S}x, y, w\rangle \in Sum \tag{4}$$

We must prove $z = w$.

We define a set X (depending on x, which is now fixed until we finish the induction step):

$$X = \{\langle u, v, z\rangle : u = \mathsf{S}x \to z = \mathsf{S}(x \oplus v)\}.$$

That formula is stratifiable, as "$z = \mathsf{S}(x \oplus v)$" can be replaced by $\exists p\,(Sum(x, v, p) \wedge \mathsf{S}p = z$", and all the variables can be given the same type. Hence the definition of X is legal. I say that X satisfies the closure conditions in the definition of Sum. Ad (i): We must show $\langle x, 0, x\rangle \in X$. That holds if and only if $x = \mathsf{S}x \to x = \mathsf{S}(x \oplus 0)$. But $x \oplus 0 = 0$, so the condition is $x = \mathsf{S}x \to x = \mathsf{S}x$, which is indeed valid.

Ad (ii): Suppose $\langle u, v, z\rangle \in X$. We must show $\langle u, \mathsf{S}v, \mathsf{S}z\rangle \in X$. We have

$$u = \mathsf{S}x \to z = \mathsf{S}(x \oplus v) \qquad\qquad \text{since } \langle u, v, z\rangle \in X$$

By the definition of Sum we have $\mathsf{S}(x \oplus v) = x \oplus \mathsf{S}v$. Therefore

$$u = \mathsf{S}x \to z = x \oplus \mathsf{S}v.$$

Taking the successor of both sides of the equation after the implication,

$$u = \mathsf{S}x \to \mathsf{S}z = \mathsf{S}(x \oplus \mathsf{S}v).$$

By the definition of X, this is equivalent to

$$\langle u, \mathsf{S}v, \mathsf{S}z\rangle \in X.$$

That completes the verification that X satisfies (ii). Hence Sum is a subset of X. Then $\langle u, v, z\rangle \in Sum$ implies $\langle u, v, z\rangle \in X$. Take $u = \mathsf{S}x$. Then by definition of X, we have

$$\langle \mathsf{S}x, v, z\rangle \in Sum \to z = x \oplus v.$$

Applying this to (3) and (4) we have $z = x \oplus v$ and $w = x \oplus v$. Therefore $z = w$ as desired. That completes the induction step. That completes the proof of the lemma.

Lemma 4.2 allows us to make the following definition.

Definition 4.3. *We henceforth write $x \oplus n = y$ instead of $\langle x, n, y\rangle \in Sum$, and when $x, n \in \mathbb{N}$, we write $x \oplus n$ for the unique y such that $x \oplus n = y$.*

Remark. We already used "$x + y$" for addition of Frege numerals in [1]. While we never need addition of Frege numerals in this paper, we have chosen to keep the notation consistent between the two papers, by using a different symbol for addition of Church numbers.

Lemma 4.4. $\forall x \in \mathbb{N}\,(x \oplus 0 = x)$.

Proof. By Definition 4.3, this formula can be expressed in terms of Sum as $\langle x, 0, x\rangle \in Sum$, which is proved in Lemma 4.1.

Lemma 4.5. $\forall x, n \in \mathbb{N}\,(x \oplus \mathsf{S}n = \mathsf{S}(x \oplus n))$.

Proof. By Definition 4.3, this formula can be expressed in terms of Sum as $\langle x, n, y\rangle \in Sum \to \langle x, \mathsf{S}n, \mathsf{S}y\rangle \in Sum$, which is proved in Lemma 4.1.

5. Alternate definitions of addition

In this section we discuss two definitions that we do not use, and the reasons we do not use them.

5.1. Addition as iterated successor. We could consider defining addition by

$$x \oplus y \quad := \quad y\mathsf{S}x \tag{5}$$

Technically we have defined the "add y" function $y\mathsf{S}$, which takes an argument x and adds y to it.

This definition of addition as iterated successor makes it immediate that addition is single-valued, but the defining formula (5) cannot be stratified giving x and y the same type, for if we give x index 0, then s has index 3 and y has to get index 6. So this definition does not make addition a function of the ordered pair $\langle x, y\rangle$.

The laws of addition follow from the definition of successor:

$$\begin{aligned} x \oplus \mathsf{S}y &= (\mathsf{S}y)\mathsf{S}x \\ &= \mathsf{S}y\mathsf{S}x \\ &= \mathsf{S}(y\mathsf{S}x) \qquad \text{by definition of } \mathsf{S} \\ &= \mathsf{S}(x \oplus y) \qquad \text{by (5)} \end{aligned}$$

$$\begin{aligned} x \oplus 0 &= 0\mathsf{S}x \\ &= 0 \qquad \text{by definition of } 0 \end{aligned}$$

With this definition of addition, the formula $x \oplus y = z$ is $y\mathsf{S}x = z$, which is stratified since it has only one occurrence of each variable, but not homogeneous. For example the formula $0 \oplus x = x$ is $x\mathsf{S}0 = x$, which is not stratified. Hence, with this definition, we would not see how to prove $0 \oplus x = x$. Similarly, the formula asserting the equivalence of the two definitions is

$$x \oplus y = y\mathsf{S}x,$$

where $\oplus$ means the first definition. This is not a stratified formula, since y on the right must get a greater index than on the left. Hence we cannot prove, at least not by induction on y, that the two definitions are equivalent. This gives us a second reason not to use this definition.

5.2. Addition via composition. Church and Kleene (in [2] and [5]) define addition to satisfy this formula:

$$(x \oplus y)fz \quad = \quad xf(yfz) \tag{6}$$

This formula is stratified giving z index 0, x and y both index 6, and f index 3, so it is possible to give this definition in INF. The set-theoretical definition of addition given in Definition 4.3 produces an addition function defined only on the Church numbers; the more general definition here can add any two functions mapping some set into itself, not just mapping $\mathbb{N}$ into $\mathbb{N}$.

Unlike the definition of addition by iterated successor, there is no compelling reason not to use the Church-Kleene definition. But there are several details to attend to in translating from the λ-calculus to NF, for example, just to go from the definition above to the set of ordered triples that is really the function $\oplus$. We wrote out all the details required to reach the basic properties of addition, and found it required twice as much space as the set-theoretic details using Definition 4.3. We shall see in Lemma 7.6 that (6) is satisfied by the addition of Definition 4.3.

From (6) and the equation for successor we find $\mathsf{S}(x \oplus y) = \mathsf{S}x \oplus y$ and $0 \oplus y = y$. From these we can prove the equivalence of this definition to the one given in Definition 4.3, when restricted to Church numbers x and y.

6. Stratification

Let L be the fragment of the language of Peano arithmetic that does not involve the symbol for multiplication; thus L has a constant 0 and function symbols for successor and addition, from which compound terms can be built up.

Now that we have defined addition on $\mathbb{N}$, it is possible to define an interpretation of (the language of) L into NF (which does not have terms, constant symbols, or function symbols). Namely, for each term t in L with free variables x there is a formula of NF with free variables x and one additional variable y expressing $t = y$. This formula contains many fresh existentially quantified variables; rather than give a recursive definition, or a program for computing it, we illustrate with an example. If t is $x \oplus s(z)$, then the formula in question is

$$\exists u, v\, (\langle x, u, y\rangle \in \mathit{Sum} \wedge \langle z, u\rangle \in \mathsf{S})$$

where $w \in \mathsf{S}$ abbreviates the formula in Definition 2.2, and $w \in \mathit{Sum}$ stands for the formula defining Sum. Similarly, the formula $y = 0$ is expressed by the formula in Definition 2.2.

Lemma 6.1. *Any formula in the language of Peano arithmetic without multiplication is interpreted by a formula of NF that can be stratified by giving all the variables the same type.*

Proof. By induction on the complexity of the formula ϕ. Since all the variables are to be given the same type, no conflict can arise between different occurrences of a variable; hence we need consider only atomic formulae ϕ. These have the form $p = q$ for terms p and q. We can replace $p = q$ by $\exists u\, (p = u \wedge q = u)$, so we need only atomic formulae $p = u$. These we prove stratifiable by induction on the complexity of the term, which is either $q \oplus r$ or $\mathsf{S}(q)$ (often written q' in PA). We omit the details, which are technical but typical of interpretation proofs.

Examples. In the rest of this paper we have occasion to prove several theorems or lemmas by induction in NF. To prove something by induction in NF we have to check that the formula being proved is stratified. The theorems are all special cases of the preceding lemma. Some formulas to which we apply Lemma 6.1 to obtain these formulas are as follows:

$0 \oplus x = x$	Lemma 7.1
$\forall x\, (x \oplus \mathsf{S}(n) = \mathsf{S}(x) \oplus n)$	Lemma 7.2
$x \neq 0 \to 0 < x$	Lemma 8.5
$x < y \to \mathsf{S}x < y \ \vee\ \mathsf{S}x = y$	Lemma 8.6

7. Properties of addition

For the rest of the paper, it does not matter how addition was defined; we use only that it is defined by a stratified homogeneous formula and satisfies the two formulas in Lemmas 4.5 and 4.4, namely

$$\begin{array}{rcll} x \oplus 0 & = & x & \text{and} \\ x \oplus \mathsf{S}n & = & \mathsf{S}(x \oplus n). & \end{array}$$

Indeed one can easily prove that if $x \oplus y$ is another function satisfying these properties then $x \oplus y = x \oplus y$ on Church numbers x, y. Above we gave a set-theoretical definition of addition, in Definition 4.3; and a definition closer to λ-calculus in spirit, in §5.2. The former is defined only on Church numbers, while the latter can add any two functions; but as just remarked, they *necessarily* agree on Church numbers. In this section we develop further properties of addition, using only the two properties listed above.

Lemma 7.1. *For $x \in \mathbb{N}$, $0 \oplus x = x$.*

Proof. By induction on x. The base case is $0 \oplus 0 = 0$, which follows from $x \oplus 0 = 0$, which is Lemma 4.4 part (i). For the induction step, assume $0 \oplus x = x$. Applying successor to both sides, we have $\mathsf{S}(0 \oplus x) = \mathsf{S}x$. By Lemma 4.5 we have $\mathsf{S}(0 \oplus x) = 0 \oplus \mathsf{S}x$. Therefore $\mathsf{S}x = 0 \oplus \mathsf{S}x$. That completes the induction step, and that completes the proof of the lemma.

Lemma 7.2. *For $x, n \in \mathbb{N}$,*

$$x \oplus \mathsf{S}n = \mathsf{S}x \oplus n.$$

Proof. We quantify universally over Church numbers x, obtaining

$$\forall x \in \mathbb{N}\, (x \oplus \mathsf{S}n = \mathsf{S}x \oplus n),$$

and prove that by induction on n. The formula to be proved can be stratified by giving all variables type 0.

Base case: $x \oplus \mathsf{S}0 = \mathsf{S}x \oplus 0$.

$$\begin{array}{rcll} x \oplus \mathsf{S}0 & = & \mathsf{S}(x \oplus 0) & \text{by Lemma 4.5} \\ & = & sx & \text{by Lemma 4.4} \\ & = & \mathsf{S}(x) \oplus 0 & \text{by Lemma 4.4} \end{array}$$

That completes the base case.

Induction step:

$$\begin{array}{rcll} x \oplus \mathsf{SS}n & = & \mathsf{S}(x \oplus \mathsf{S}n) & \text{by Lemma 4.5} \\ & = & \mathsf{S}(\mathsf{S}x \oplus n) & \text{by the induction hypothesis} \\ & = & \mathsf{S}x \oplus \mathsf{S}n & \text{by Lemma 4.5, with } x \text{ replaced by } \mathsf{S}x \end{array}$$

The replacement of x by $\mathsf{S}x$ in the last step is legal, because the statement being proved by induction is universally quantified over x. That completes the proof of the theorem.

Lemma 7.3. $\forall x, y \in \mathbb{N}\ (x \oplus y \in \mathbb{N})$.

Proof. By induction on y, which is legal since the formula is stratified. We omit the straightforward proof.

Lemma 7.4 (Associativity)**.** $\forall x, y, z \in \mathbb{N}, ((x \oplus y) \oplus z = x \oplus (y \oplus z))$.

Proof. By induction on y, which is legal since the formula is stratified.

Base case: $(x \oplus 0) \oplus z = x \oplus z$ and $x \oplus (0 \oplus z) = x \oplus z$, by Lemma 7.1. Hence $(x \oplus 0) \oplus z = x \oplus (0 \oplus z)$, completing the base case.

Induction step:

$$\begin{aligned}
(x \oplus \mathsf{S}y) \oplus z &= \mathsf{S}(x \oplus y) \oplus z && \text{by Lemma 4.5} \\
&= (x \oplus y) \oplus \mathsf{S}z && \text{by Lemma 7.2} \\
&= \mathsf{S}((x \oplus y) \oplus z) && \text{by Lemmas 4.5 and 7.3} \\
&= \mathsf{S}(x \oplus (y \oplus z)) && \text{by the induction hypothesis} \\
&= x \oplus \mathsf{S}(y \oplus z) && \text{by Lemmas 7.2} \\
&= x \oplus (y \oplus \mathsf{S}z) && \text{by Lemma 4.5 and 7.3} \\
&= x \oplus (\mathsf{S}y \oplus z) && \text{by Lemma 7.2}
\end{aligned}$$

That completes the proof of the lemma.

Lemma 7.5 (Commutativity)**.** $\forall x, y \in \mathbb{N}\,(x \oplus y = y \oplus x)$.

Proof. By induction on y, which is legal since the formula is stratified.

Base case, $x \oplus \mathbf{0} = \mathbf{0} \oplus x$. We have

$$\begin{aligned}
x \oplus \mathbf{0} &= x && \text{by Lemma 4.4} \\
\mathbf{0} \oplus x &= x && \text{by Lemma 7.1} \\
x \oplus \mathbf{0} &= \mathbf{0} \oplus x && \text{by the previous two lines}
\end{aligned}$$

Induction step:

$$\begin{aligned}
x \oplus \mathsf{S}y &= \mathsf{S}(x \oplus y) && \text{by Lemma 4.5} \\
&= \mathsf{S}(y \oplus x) && \text{by the induction hypothesis} \\
&= y \oplus \mathsf{S}x && \text{by Lemma 4.5} \\
&= \mathsf{S}y \oplus x && \text{by Lemma 7.2}
\end{aligned}$$

That completes the induction step, and the proof of the lemma.

Lemma 7.6. *Let $f \in \mathsf{FUNC}$ and $f : X \to X$. Then for Church numbers j and ℓ, and $x \in X$, we have*

$$(jf)(\ell f x) = (j \oplus \ell) f x.$$

Proof. The formula to be proved is stratified, so we may prove it by induction on j. Base case:

$$\begin{aligned}
0f(\ell f x) &= \ell f x && \text{by definition of 0} \\
&= (0 \oplus \ell) f x && \text{by Lemma 7.1}
\end{aligned}$$

Induction step:

$$\begin{aligned}
(\mathsf{S}jf)(\ell f x) &= f(jf(\ell f x)) && \text{by Theorem 3.6} \\
&= f((j \oplus \ell) f x) && \text{by the induction hypothesis} \\
&= \mathsf{S}(j \oplus \ell) f x && \text{by Theorem 3.6} \\
&= (j \oplus \mathsf{S}\ell) f x && \text{by Lemma 4.5} \\
&= (\mathsf{S}j \oplus \ell) && \text{by Lemma 7.2}
\end{aligned}$$

That completes the proof of the lemma.

8. Order on $\mathbb{N}$

Definition 8.1. *Order on the Church numbers is defined by*

$$x < y \leftrightarrow \exists n \in \mathbb{N}\,(x \oplus \mathsf{S}n = y).$$

$$x \le y \leftrightarrow \exists n \in \mathbb{N}\,(x \oplus n = y).$$

These formulas are stratifiable, giving x, y, and n all index 0. ($\mathbb{N}$ is a parameter.) Therefore the relations $x < y$ and $x \le y$ are definable in INF as sets of ordered pairs.

Remark. We use the same symbols for these relations as are used in [1] for order on finite Frege cardinals; in our formalization, we used different symbols, but for human readers, we think it better not to introduce a new symbol.[5]

Lemma 8.2. *For all $x \in \mathbb{N}$, $x \not< \mathbf{0}$.*

Proof. Suppose $x \in \mathbb{N}$ and $x < \mathbf{0}$. Then

$$\begin{aligned} x \oplus \mathsf{S}n &= \mathbf{0} && \text{by definition of } < \\ \mathsf{S}(x \oplus n) &= \mathbf{0} && \text{by Lemma 7.2} \end{aligned}$$

But that contradicts Theorem 3.8, which says that $\mathbf{0}$ is not a successor.

Lemma 8.3. *For all x and y in $\mathbb{N}$,*

$$x = y \ \vee \ x < y \to x < \mathsf{S}y$$

Proof. Suppose $x = y \vee x < y$.

Case 1, $x = y$. We must prove $x < \mathsf{S}x$.

$$\begin{aligned} x \oplus \mathsf{S}0 &= \mathsf{S}x \oplus 0 && \text{by Lemma 4.5} \\ &= \mathsf{S}x && \text{by Lemma 4.4} \\ x \oplus \mathsf{S}0 &= \mathsf{S}x && \text{by the preceding two lines} \\ x &< \mathsf{S}x && \text{by Definition 8.1} \end{aligned}$$

That completes Case 1.

Case 2, $x < y$. We have to prove $x < \mathsf{S}y$.

$$\begin{aligned} x \oplus \mathsf{S}t &= y && \text{for some } t \in \mathbb{N}, \text{ by Definition 8.1} \\ \mathsf{S}(x \oplus \mathsf{S}t) &= \mathsf{S}y && \text{by the preceding line} \\ x \oplus \mathsf{S}(\mathsf{S}t) &= \mathsf{S}y && \text{by Lemma 4.5} \\ x &< \mathsf{S}y && \text{by Definition 8.1} \end{aligned}$$

That completes Case 2. That completes the proof of the lemma.

Corollary 8.4. *For all $x \in \mathbb{N}$, $x < \mathsf{S}x$.*

Remark. This does not guarantee $x \ne \mathsf{S}x$ since we do not have trichotomy.

Proof. Take $x = y$ in Lemma 8.3.

Lemma 8.5. *For all $x \in \mathbb{N}$, $x \ne \mathbf{0} \to \mathbf{0} < x$.*

[5] Life is short, but the alphabet is shorter. And the alphabet of binary ordering relations is even shorter, and we later need $\preceq$ and $\prec$ for something else.

Proof. By induction on x. The formula to be proved is stratifiable, by Lemma 6.1.

We proceed with the induction. The base case is immediate (since $\mathbf{0} \neq \mathbf{0}$ implies anything). To prove the induction step, we have to prove $\mathsf{S}x \neq \mathbf{0} \to \mathbf{0} < \mathsf{S}x$. Suppose $\mathsf{S}x \neq \mathbf{0}$; we have to prove $\mathbf{0} < \mathsf{S}x$. By Lemma 8.3, it suffices to prove $\mathbf{0} < x \vee \mathbf{0} = x$. But that follows from the induction hypothesis $x \neq \mathbf{0} \to \mathbf{0} < x$, even with intuitionistic logic, because by Lemma 3.10, $x \neq \mathbf{0} \vee x = \mathbf{0}$, and if $x \neq \mathbf{0}$ then $\mathbf{0} < x$, while if $x = \mathbf{0}$ then $\mathbf{0} = x$. That completes the proof of the lemma.

Lemma 8.6. *For all $x, y \in \mathbb{N}$,*

$$x < y \to \mathsf{S}x < y \ \vee \ \mathsf{S}x = y$$

Proof.

$$\begin{array}{rl} x < y & \text{assumption} \\ x \oplus \mathsf{S}p = y & \text{for some } p \in \mathbb{N}\text{, by definition of } < \\ x \oplus \mathsf{S}p = \mathsf{S}x \oplus p = y & \text{by Lemma 7.2} \\ p = \mathbf{0} \ \vee \ p \neq \mathbf{0} & \text{by Lemma 3.10} \end{array}$$

If $p = \mathbf{0}$ then $\mathsf{S}x = y$ and we are done. If $p \neq \mathbf{0}$ then

$$\begin{array}{rl} p = \mathsf{S}\ell & \text{for some } \ell \in \mathbb{N}\text{, by Lemma 3.9} \\ x \oplus \mathsf{S}(\mathsf{S}\ell) = y & \text{since } x \oplus \mathsf{S}p = y \\ \mathsf{S}x \oplus \mathsf{S}\ell = y & \text{by Lemma 7.2} \\ \mathsf{S}x < y & \text{by definition of } < \end{array}$$

That completes the proof of the lemma.

Lemma 8.7. *For $x, y \in \mathbb{N}$, if $x \leq y$ and $x \neq y$ then $x < y$.*

Proof. Suppose $x, y \in \mathbb{N}$ and $x \leq y$. Then for some m we have $x \oplus m = y$. If $m = \mathbf{0}$ then $x = y$, by Lemma 4.4. Hence $m \neq \mathbf{0}$. Then by Lemma 3.9, $m = \mathsf{S}r$ for some $r \in \mathbb{N}$. Then $x \oplus \mathsf{S}r = y$. Then by definition of $<$, we have $x < y$. That completes the proof of the lemma.

Lemma 8.8. *For $x, y \in \mathbb{N}$,*

$$x \leq y \leftrightarrow x < y \ \vee \ x = y.$$

Proof. Left to right: Suppose $x \leq y$. Then $x \oplus m = y$ for some $m \in \mathbb{N}$. By Lemma 3.10, $m = \mathbf{0} \ \vee \ m \neq \mathbf{0}$. If $m = \mathbf{0}$, then by Lemma 4.4, $x = y$. If $m \neq \mathbf{0}$, then by Lemma 3.9, $m = \mathsf{S}r$ for some $r \in \mathbb{N}$. Then $x < y$ by the definition of $<$.

Right to left. Suppose $x < y \vee x = y$. If $x < y$ then $x \oplus \mathsf{S}m = y$ for some $m \in \mathbb{N}$. Then $\mathsf{S}m \in \mathbb{N}$ by Lemma 2.19, so $x \leq y$ by definition of $\leq$. If $x = y$ then $x \oplus \mathbf{0} = y$, by Lemma 4.4, so $x \leq y$. That completes the proof of the lemma.

Lemma 8.9 (transitivity). *$x < y$ is a transitive relation. That is, for $x, y, z \in \mathbb{N}$,*

$$x < y \wedge y < z \to x < z.$$

Proof. Suppose $x < y$ and $y < z$. Then for some p, q we have $x \oplus p = y$ and $y \oplus q = z$. Then $(x \oplus p) \oplus q = z$. By the associativity of addition we have $x \oplus (p \oplus q) = z$. Then $x < z$. That completes the proof of the lemma.

Lemma 8.10. *For $x, y \in \mathbb{N}$,*

$$x < y \ \vee \ x = y \ \vee \ y < x$$

Remark. We do not claim that exactly one of the three alternatives holds.

Proof. We proceed by induction on x. When $x = \mathbf{0}$ we have to prove

$$\mathbf{0} < y \ \vee \ \mathbf{0} = y \ \vee \ y < \mathbf{0}.$$

We have

$$y = \mathbf{0} \ \vee \ y \neq \mathbf{0} \qquad \text{by Lemma 3.10}$$

If $y = \mathbf{0}$, we are done. If $y \neq \mathbf{0}$ then

$$\mathbf{0} < y \vee \mathbf{0} = y \qquad \text{by Lemma 8.5}$$

That completes the base case.

For the induction step, we assume

$$x < y \ \vee \ x = y \ \vee \ y < x$$

and must prove

$$\mathsf{S}x < y \ \vee \ \mathsf{S}x = y \ \vee \ y < \mathsf{S}x.$$

We argue by cases.

Case 1, $x < y$. Then by Lemma 8.6, $\mathsf{S}x < y$ or $\mathsf{S}x = y$. That completes Case 1.

Case 2, $x = y$. Then by Corollary 8.4, $y < \mathsf{S}x$. That completes Case 2.

Case 3, $y < x$. Then

$$x < \mathsf{S}x \qquad \text{by Corollary 8.4}$$
$$y < \mathsf{S}x \qquad \text{by Lemma 8.9}$$

That completes Case 3. That completes the proof of the lemma.

9. Structure of ℕ under successor: The picture

In this and the following sections, we explore the consequences of the assumption that Church successor is not one to one. We first attempt to convey an intuitive picture of the situation.

Figure 2. The stem STEM, the loop $\mathcal{L}$, and unique double successor

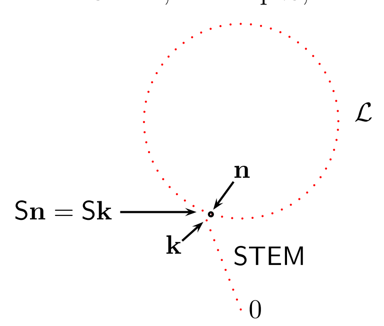


Figure 2 (already shown in the introduction, but reprinted here for convenience) illustrates the structure of ℕ under successor. To arrive at this figure, imagine coloring $\mathbf{0}$ red, and at each stage where you have just colored x red, then color $\mathsf{S}x$ red unless $\mathsf{S}(\mathsf{S}x)$ is already red. Then stop. Let $\mathbf{n}$ be the last number you encountered. You will have colored every integer red except $\mathbf{n}$ (shown black in the figure). The reason you did not color $\mathbf{n}$ is that $\mathsf{S}\mathbf{n} = \mathsf{S}\mathbf{k}$, where $\mathbf{k}$ is some number that you already colored red. We call $\mathsf{S}n$ a "double successor."

We emphasize that at this point we have not proved that this figure is accurate. There might be many more double successors not shown; imagine a gray spiderweb of mysterious Church numbers, merging at different places into the red part of the figure. But the red part, if it could be defined, contains 0 and is closed under successor, so it intuitively should be all of $\mathbb{N}$. We shall prove in Theorem 13.3 below that, at least if $\mathbb{N}$ is assumed to be finite, this picture is an accurate one. The part that you colored before reaching $\mathbf{k}$ (and including $\mathbf{k}$) is called the "stem". The rest of the red numbers (plus $\mathbf{n}$) comprise "the loop." The next several sections will show in detail that this picture is correct.

Definition 9.1. *p is not a double successor if*

$$\forall a, b\, (a \in \mathbb{N} \ \wedge \ b \in \mathbb{N} \ \wedge \mathsf{S}a = \mathsf{S}b = p \rightarrow \ a = b).$$

It might seem more natural to define the concept this way: p is a double successor if there exists $a, b \in \mathbb{N}$ with $a \neq b$ and $\mathsf{S}a = \mathsf{S}b = p$. But negating this introduces a double negation, which we prefer not to have. Hence the definition above. Soon we will be working under the hypothesis that $\mathbb{N}$ is finite, which implies that $\mathbb{N}$ has decidable equality, making this double negation irrelevant. Also, we could strengthen the notion by dropping the condition $b \in \mathbb{N}$; we will do that in one place below.

Lemma 9.2. *If $x, y \in \mathbb{N}$ and $\mathsf{S}x$ is not a double successor, then*

$$y < \mathsf{S}x \leftrightarrow y < x \vee y = x.$$

Explicitly this means

$$\forall x, y \in \mathbb{N}\, ((\forall u \in \mathbb{N}\, (\mathsf{S}u = \mathsf{S}x \rightarrow u = x)) \rightarrow y < \mathsf{S}x \leftrightarrow y < x \vee y = x).$$

Proof. Left to right:

$y < \mathsf{S}x$	assumption
$y \oplus \mathsf{S}p = \mathsf{S}x$	for some $p \in \mathbb{N}$, by definition of $<$
$\mathsf{S}(y \oplus p) = \mathsf{S}x$	by Lemma 4.5
$y \oplus p = x$	since $\mathsf{S}x$ is not a double successor
$p = \mathbf{0} \ \vee \ p \neq \mathbf{0}$	by Lemma 3.10

Case 1, $p = \mathbf{0}$. Then $y = x$. That completes Case 1.

Case 2, $p \neq \mathbf{0}$. Then

$p = \mathsf{S}m$	for some $m \in \mathbb{N}$, by Lemma 3.9
$y \oplus \mathsf{S}m = x$	since $y \oplus p = x$
$y < x$	by definition of $<$

That completes Case 2. That completes the left-to-right implication.

Right-to-left: Suppose $y < x \vee y = x$, and $\mathsf{S}x$ is not a double successor. We have to prove $y < \mathsf{S}x$. We argue by cases.

Case 1, $y < x$. Then

$x < \mathsf{S}x$	by Corollary 8.4
$y < \mathsf{S}x$	by transitivity

That completes Case 1.

Case 2, $y = x$. Then $y < \mathsf{S}x$ by Corollary 8.4. That completes Case 2. That completes the right-to-left direction. That completes the proof of the lemma.

10. Structure of $\mathbb{N}$ under successor: The stem

Definition 10.1. *The set* STEM *is the intersection of all subsets of* $\mathbb{N}$ *containing 0 and closed under successors that are not double successors. More precisely,* STEM *is the intersection of* $\mathbb{N}$ *and all* X *such that*

$$0 \in X \ \wedge\ \forall u \in \mathbb{N}\,(u \in X \ \wedge\ \forall v \in \mathbb{N}\,(\mathsf{S}v = \mathsf{S}u \to v = u) \to \mathsf{S}u \in X).$$

The intention of the definition is that STEM should contain everything from $\mathbf{0}$ up to but not including the first double successor.

Lemma 10.2. $\mathsf{STEM} \subseteq \mathbb{N}$.

Proof. Immediate from the definition of STEM as the intersection of $\mathbb{N}$ with some other sets.

Lemma 10.3. STEM *is one of the sets used to define* STEM*. That is,*

$$\mathbf{0} \in \mathsf{STEM} \ \wedge\ \forall u \in \mathbb{N}\,(u \in \mathsf{STEM} \wedge \forall v \in \mathbb{N}\,(\mathsf{S}v = \mathsf{S}u \to v = u) \to \mathsf{S}u \in \mathsf{STEM}).$$

Proof. Let X satisfy the formula in the lemma (with STEM replaced by X). Then $\mathbf{0} \in X$. Since X was arbitrary, $\mathbf{0} \in \mathsf{STEM}$. Now suppose $u \in \mathbb{N}$ and $u \in \mathsf{STEM}$ and $\forall v \in \mathbb{N}\,(\mathsf{S}v = \mathsf{S}u \to v = u)$. Then $\mathsf{S}u \in X$. Since X was arbitrary, $\mathsf{S}u \in \mathsf{STEM}$, by Definition 10.1. That completes the proof of the lemma.

Lemma 10.4. *Church successor is one-to-one on* STEM*. What is more,*

$$\forall u \in \mathsf{STEM}\,(\mathsf{S}u \in \mathsf{STEM} \to \forall v \in \mathbb{N}\,(\mathsf{S}u = \mathsf{S}v \to u = v)).$$

That is, there are no double successors in STEM*.*

Remark. "What is more" because v is not required to be in STEM.

Proof. Define X to be

$$X := \{p \in \mathbb{N} : \forall u, v \in \mathbb{N}\,(p = \mathsf{S}u \to \mathsf{S}u = \mathsf{S}v \to u = v)\}. \tag{7}$$

The formula is stratified, giving all the variables index 0; $\mathbb{N}$ is a parameter. Hence the definition can be given in INF. Then $X \subseteq \mathbb{N}$. By Theorem 3.8, $\mathbf{0} \in X$. X is closed under successors except double successors; that is, if $x \in X$ and $\forall v \in \mathbb{N}\,(\mathsf{S}x = \mathsf{S}v \to x = v)$, then $\mathsf{S}x \in X$, as we see by putting $p = \mathsf{S}x$ in the definition of X. (By the hypothesis $x \in X$, we have $x \in \mathbb{N}$.) Therefore, by the definition of STEM, we have $\mathsf{STEM} \subseteq X$.

Suppose $Su \in \mathsf{STEM}$ and $\mathsf{S}u = \mathsf{S}v$. Then $\mathsf{S}u \in X$, since $\mathsf{STEM} \subseteq X$. Therefore $u = v$. That completes the proof of the lemma.

Lemma 10.5. *If* $y \in \mathbb{N}$ *and* $\mathsf{S}y \in \mathsf{STEM}$*, then* $y \in \mathsf{STEM}$*.*

Proof. By Lemma 10.4 there are no double successors in STEM, so it suffices to show that every nonzero element of STEM is the successor of something in STEM. Let X be the set of elements of STEM that are equal to $\mathbf{0}$ or are successors of something in STEM. Explicitly

$$X = \{x : x \in \mathsf{STEM} \ \wedge\ x = \mathbf{0} \ \vee\ \exists y\,(\mathsf{S}y = x \ \wedge\ y \in \mathsf{STEM})\}.$$

The formula is stratified, giving x and y index 0, with STEM as a parameter. I say that X is closed under successors that are not double successors. Let $x \in X$ and suppose

$$\forall v \in \mathbb{N}\,(\mathsf{S}x = \mathsf{S}v \to x = v) \tag{8}$$

(informally, $\mathsf{S}x$ is not a double successor). We must show $\mathsf{S}x \in X$. Since $x \in X$, $x \in \mathsf{STEM}$. To show $\mathsf{S}x \in X$ we must show two things:

$$\mathsf{S}x \in \mathsf{STEM} \tag{9}$$

$$\exists y\,(\mathsf{S}y = \mathsf{S}x \;\wedge\; y \in \mathsf{STEM}) \tag{10}$$

(10) is immediate, taking $y = x$. To verify (9) we use that $x \in \mathsf{STEM}$ and $\mathsf{S}x$ is not a double successor (8). By Lemma 10.3, STEM is closed under successors except double successors, so $\mathsf{S}x \in \mathsf{STEM}$ as desired. That completes the proof that X is closed under successors except double successors. Then by the definition of STEM, we have $\mathsf{STEM} \subseteq X$.

Now suppose $\mathsf{S}x \in \mathsf{STEM}$ and $x \in \mathbb{N}$; we must prove $x \in \mathsf{STEM}$. Since $\mathsf{STEM} \subseteq X$, we have $\mathsf{S}x \in X$. By definition of X,

$$\mathsf{S}x = \mathbf{0} \;\vee\; \exists y\,(y \in \mathsf{STEM} \;\wedge\; \mathsf{S}y = \mathsf{S}x).$$

By Theorem 3.8, and the hypothesis $x \in \mathbb{N}$, we have $\mathsf{S}x \neq \mathbf{0}$. Therefore, for some $y \in \mathsf{STEM}$, we have $\mathsf{S}y = \mathsf{S}x$. By Lemma 10.4, we have $y = x$. Since $y \in \mathsf{STEM}$ and $y = x$, we have $x \in \mathsf{STEM}$ as desired. That completes the proof of the lemma.

Lemma 10.6. STEM *has decidable equality. In fact,*

$$\forall x \in \mathbb{N}\,\forall y\,(x \in \mathsf{STEM} \to y \in \mathbb{N} \to x = y \;\vee\; x \neq y).$$

Remark. It is not necessary to assume $y \in \mathsf{STEM}$.

Proof. We prove by induction on x that

$$\forall y(x \in \mathsf{STEM} \to y \in \mathbb{N} \to x = y \;\vee\; x \neq y). \tag{11}$$

That formula is stratified, so it is legal to prove it by induction. The base case follows from Lemma 3.10. For the induction step, suppose $\mathsf{S}x \in \mathsf{STEM}$ and $y \in \mathbb{N}$; we have to prove $\mathsf{S}x = y \;\vee\; \mathsf{S}x \neq y$. By Lemma 3.10, we may argue by cases according as $y = \mathbf{0}$ or not. If $y = \mathbf{0}$, we are done by Lemma 3.10. If $y \neq \mathbf{0}$, then $y = \mathsf{S}q$ for some q. Then

$$\begin{aligned} x &\in \mathsf{STEM} && \text{by Lemma 10.5} \\ \mathsf{S}x = y \;\vee \mathsf{S}x \neq y &\leftrightarrow \mathsf{S}x = \mathsf{S}q \vee \mathsf{S}x \neq \mathsf{S}q && \text{since } y = \mathsf{S}q \\ &\leftrightarrow x = q \;\vee x \neq q && \text{by Lemma 10.4, since } \mathsf{S}x \in \mathsf{STEM} \end{aligned}$$

and that follows from the induction hypothesis (11). That completes the proof of the lemma.

Lemma 10.7. *Suppose* $y \in \mathsf{STEM}$ *and* $x \in \mathbb{N}$ *and* $x < y$. *Then* $x \in \mathsf{STEM}$.

Proof. By induction on y we prove

$$y \in \mathbb{N} \to y \in \mathsf{STEM} \to \forall x \in \mathbb{N}\,(x < y \to x \in \mathsf{STEM}).$$

That formula is stratified, so induction is legal.

Base case: When $y = \mathbf{0}$, it is impossible that $x < y$, by Lemma 8.2. Therefore $x < \mathbf{0} \to x \in \mathsf{STEM}$. That completes the base case.

Induction step: Suppose $\mathsf{S}y \in \mathbb{N}$ and $\mathsf{S}y \in \mathsf{STEM}$ and $x < \mathsf{S}y$. We must prove $x \in \mathsf{STEM}$. We have

$y \in \mathsf{STEM}$	by Lemma 10.5
$\mathsf{S}y \in \mathsf{STEM}$	by hypothesis
$\mathsf{S}y$ is not a double successor	by Lemma 10.4
$x < y \ \vee \ x = y$	by Lemma 9.2

If $x < y$, then by the induction hypothesis, $x \in \mathsf{STEM}$. If $x = y$ then $x \in \mathsf{STEM}$ because $y \in \mathsf{STEM}$. That completes the induction step. That completes the proof of the lemma.

Lemma 10.8. *Suppose* $\mathsf{S}k = \mathsf{S}n$ *with* $k \in \mathsf{STEM}$ *and* $n \in \mathbb{N}$ *and* $k \neq n$. *Then* k *is a maximal element of* STEM*; more precisely,*

$$\mathsf{STEM} = \{x \in \mathbb{N} : x < k \ \vee \ x = k\}.$$

Proof. Define

$$Z = \{x \in \mathsf{STEM} : x < k \ \vee \ x = k\}.$$

The formula is stratified, since $<$ is definable as a relation in INF. I say that Z contains $\mathbf{0}$ and is closed under successor except double successors.

To prove $\mathbf{0} \in Z$:

$\mathbf{0} \in \mathsf{STEM}$	by Lemma 10.3
$k = \mathbf{0} = k \ \vee \ k \neq \mathbf{0}$	by Lemma 3.10

We argue by cases.

Case 1, $k = \mathbf{0}$. Then $\mathbf{0} \in Z$, by definition of Z.

Case 2, $\mathbf{k} \neq \mathbf{0}$. Then

$k = \mathsf{S}m$	for some $m \in \mathbb{N}$, by Lemma 3.9
$\mathbf{0} \oplus \mathsf{S}m = \mathsf{S}m$	by Lemma 7.1
$\mathbf{0} \oplus \mathsf{S}m = k$	since $k = \mathsf{S}m$
$\mathbf{0} < k$	by definition of $<$

To prove Z is closed under successor except double successor: Suppose $x \in Z$ and $\mathsf{S}x$ is not a double successor. Since $x \in Z$, $x < k \ \vee \ x = k$. But $\mathsf{S}k$ is a double successor, so $x \neq k$. Therefore $x < k$. Then $\mathsf{S}x = k \vee \mathsf{S}x < k$, by Lemma 8.6. Hence $\mathsf{S}x \in Z$. Therefore Z contains $\mathbf{0}$ and is closed under successor except double successors. Therefore $\mathsf{STEM} \subseteq Z$. Now I say

$$\mathsf{STEM} = \{x \in \mathbb{N} : x < k \vee x = k\}.$$

It suffices to prove

$$x \in \mathsf{STEM} \leftrightarrow x \in \mathbb{N} \ \wedge \ (x < k \vee x = k).$$

Left to right: Suppose $x \in \mathsf{STEM}$. By Lemma 10.2, $\mathsf{STEM} \subseteq \mathbb{N}$, so $x \in \mathbb{N}$. Since $\mathsf{STEM} \subseteq Z$, we have $x \in Z$. Then $x < k \vee x = k$, by definition of Z.

Right to left: Suppose $x \in \mathbb{N} \ \wedge \ (x < k \vee x = k)$. Since $k \in \mathsf{STEM}$, we have $x \in \mathsf{STEM}$ by Lemma 10.7. That completes the proof of the lemma.

Lemma 10.9. *Let P be any subset of $\mathbb{N}$ satisfying the following two conditions:*

(i) $\forall x \in \mathbb{N}\,(Sx \in P \to x \in P)$.

(ii) $\forall x, y \in P(y < \mathsf{S}x \leftrightarrow y < x \vee y = x)$.

Then trichotomy holds on P. That is, for $x, y \in P$, exactly one of $x < y$, $x = y$, or $y < x$ holds.

Proof. Assume (i) and (ii). By Lemma 8.10, at least one of the three alternatives (of trichotomy) holds. We prove by induction on y that

$$y \in P \to \forall x \in P\,(\neg(x < y \ \wedge\ y < x) \ \wedge\ x \not< x).$$

The formula is stratified, giving x and y index 0 and P index 1, so we may proceed by induction.

Base case, $y = \mathbf{0}$. Suppose $x \in P$ and $\mathbf{0} \in P$. We do not have $x < \mathbf{0}$, by Lemma 8.2. Suppose $x = \mathbf{0} \wedge \mathbf{0} < x$. Then $\mathbf{0} < \mathbf{0}$, contradicting Lemma 8.2. That completes the base case.

Induction step: Suppose $\mathsf{S}y \in P$. Assume $x \in P$. We have to prove

$$\neg\,(x < \mathsf{S}y \ \wedge \mathsf{S}y < x) \ \wedge\ \mathsf{S}y \not< \mathsf{S}y.$$

We have

$$\begin{array}{rl}
y \in P & \text{by (i), since } \mathsf{S}y \in P \\
x < \mathsf{S}y & \text{assumption} \\
x < y \vee x = y & \text{by (ii), with } x \text{ and } y \text{ switched} \\
x < y \to x \oplus j = y & \text{for some } j \in \mathbb{N}, \text{ by the definition of } < \\
x = y \to x \oplus j = y & \text{for } j = \mathbf{0}, \text{ by Lemma 4.4} \\
x \oplus j = y & \text{for some } j \in \mathbb{N}, \text{ by the preceding three lines}
\end{array}$$

Now assume that also $\mathsf{S}y < x$. Then arguing as above, but switching x and y, we have

$$\begin{array}{rl}
\mathsf{S}y \oplus \ell = x & \text{for some } \ell \in \mathbb{N} \\
\mathsf{S}y \oplus \ell \oplus j = x \oplus j & \text{by the preceding line} \\
\mathsf{S}y \oplus \ell \oplus j = y & \text{since } x \oplus j = y \\
y \oplus \mathsf{S}(\ell \oplus j) = y & \text{by Lemma 7.2} \\
y < y & \text{by the definition of } <
\end{array}$$

But that contradicts the induction hypothesis, since $y \in P$. We have now proved the first half of (12), namely

$$\neg\,(x < \mathsf{S}y \ \wedge \mathsf{S}y < x).$$

Then by Lemma 8.10 we have $\mathsf{S}y = x$. It remains to prove $\mathsf{S}y \not< \mathsf{S}y$. Suppose $\mathsf{S}y < \mathsf{S}y$. Then

$$\begin{array}{rl}
y < \mathsf{S}y & \text{by Corollary 8.4} \\
\mathsf{S}y \in P & \text{by hypothesis} \\
\mathsf{S}y < y \ \vee\ \mathsf{S}y = y & \text{by hypothesis (ii)}
\end{array}$$

We argue by cases accordingly.

Case 1, $\mathsf{S}y < y$. Since $y < \mathsf{S}y$ we have $y < y$ by transitivity, contradicting the induction hypothesis.

Case 2, $\mathsf{S}y = y$. Then since $y < \mathsf{S}y$ we again have $y < y$, contradicting the induction hypothesis. That completes the proof of (12. That completes the induction step. That completes the proof of the lemma.

Lemma 10.10. *Suppose there is a double successor* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *with* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \neq \mathbf{k}$. *Then* $\mathbf{k} \not< \mathbf{k}$.

Proof. Let

$$X := \mathsf{STEM} - \{x \in \mathbb{N} : \mathbf{k} < x\}.$$

I say that X is closed under non-double successors. Suppose $x \in X$ and $\mathsf{S}x$ is not a double successor. Then

$$\begin{array}{rl} \mathsf{S}x \in \mathsf{STEM} & \text{by Lemma 10.3} \\ \mathbf{k} \not< x & \text{since } x \in X \end{array}$$

I say $\mathbf{k} \not< \mathsf{S}x$. Suppose $\mathbf{k} < \mathsf{S}x$. Then by Lemma 9.2, we have $\mathbf{k} < x \ \vee \ \mathbf{k} = x$. We do not have $\mathbf{k} = x$, since $\mathsf{S}\mathbf{k}$ is a double successor but $\mathsf{S}x$ is not. Therefore $\mathbf{k} < x$, contradiction. Therefore X is closed under non-double successors, as claimed. Therefore $\mathsf{STEM} \subseteq X$, by definition of STEM. But $\mathbf{k} < \mathbf{k}$ implies $\mathbf{k} \notin X$, while by hypothesis, $\mathbf{k} \in \mathsf{STEM}$. That completes the proof of the lemma.

Lemma 10.11. *Suppose there is a double successor* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *with* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \neq \mathbf{k}$. *Let* $x \in \mathsf{STEM}$ *with* $x \neq \mathbf{k}$. *Then* $\mathsf{S}x$ *is not a double successor; that is,* $\forall u \in \mathbb{N}(\mathsf{S}u = \mathsf{S}x \to u = x)$.

Proof. Suppose $\mathsf{S}\mathbf{k}$ is a double successor, and $x \in \mathsf{STEM}$ and $x \neq \mathbf{k}$. Then by Lemma 10.8, we have $x < \mathbf{k}$. If $\mathsf{S}x$ is a double successor, then by Lemma 10.8, $\mathbf{k} < x$. Then by Lemma 8.9, $\mathbf{k} < \mathbf{k}$. But that contradicts Lemma 10.10. Hence, $\mathsf{S}x$ is not a double successor. That is,

$$\neg\exists u \in \mathbb{N}\,(\mathsf{S}u = \mathsf{S}x \ \wedge \ u \neq x).$$

By logic,

$$\forall u \in \mathbb{N}\,(\mathsf{S}u = \mathsf{S}x \to \neg\neg\,(u = x).$$

Since $x \in \mathsf{STEM}$ and $y \in \mathbb{N}$, we have $\neg\neg\, u = x \to u = x$, by Lemma 10.6. Therefore we can drop the double negation:

$$\forall u \in \mathbb{N}\,(\mathsf{S}u = \mathsf{S}u \to u = x).$$

That completes the proof of the lemma.

Lemma 10.12. *Suppose there is a double successor* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *with* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \neq \mathbf{k}$. *Then for* $y \in \mathsf{STEM}$, *we have* $\neg(x < y \ \wedge y < x) \ \wedge \ \neg\,(y < y)$.

Proof. We intend to apply Lemma 10.9, with P replaced by STEM. To do that, it suffices to verify the hypotheses of Lemma 10.9, namely

$$\begin{array}{ll} (i) & x \in \mathbb{N} \to \mathsf{S}x \in \mathsf{STEM} \to x \in \mathsf{STEM} \\ (ii) & x, y \in \mathsf{STEM} \to (y < \mathsf{S}x \leftrightarrow y < x \vee y = x) \end{array}$$

Ad (i): This is Lemma 10.5.

Ad (ii): Assume $x, y \in \mathsf{STEM}$. By Lemma 10.6, we have $x = \mathbf{k} \ \vee \ x \neq \mathbf{k}$. We argue by cases.

Case 1, $x = \mathbf{k}$. We have to prove $y < \mathsf{S}\mathbf{k} \leftrightarrow y < \mathbf{k} \ \vee \ y = \mathbf{k}$.

Left to right: By Lemma 10.8, the right side is equivalent to $y \in \mathsf{STEM}$, which we have assumed.

Right to left: Assume $y < \mathbf{k} \vee y = \mathbf{k}$; we have to prove $y < \mathsf{S}\mathbf{k}$. We have $\mathbf{k} < \mathsf{S}\mathbf{k}$ by Lemma 8.4. If $y = \mathbf{k}$ we are done; if $y < \mathbf{k}$ then by transitivity (Lemma 8.9) we have $y < \mathsf{S}\mathbf{k}$. That completes Case 1.

Case 2, $x \neq \mathbf{k}$. By Lemma 10.11, x is not a double successor. Then by Lemma 9.2, we have (ii). That completes Case 2. That completes the proof of the lemma.

Lemma 10.13. *Suppose there is a double successor* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *with* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \neq \mathbf{k}$. *Then* $\mathbf{n} \neq \mathbf{0}$.

Proof. Assume $\mathbf{n} = \mathbf{0}$. Then $\mathbf{n} \in \mathsf{STEM}$, by Lemma 10.3. By Lemma 10.8, $\mathbf{0}$ is the maximal element of STEM. Then $\mathbf{0}$ is the only element of STEM, by Lemma 8.2. Then $\mathbf{k} = \mathbf{0}$, since $\mathbf{k} \in \mathsf{STEM}$. But that contradicts $\mathbf{n} \neq \mathbf{k}$. That completes the proof of the lemma.

11. Structure of $\mathbb{N}$ under successor: the loop

Definition 11.1. *Suppose there is a double successor* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *with* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \neq \mathbf{k}$. *Then the* **loop** $\mathcal{L}(\mathbf{n})$ *is the intersection of all sets* X *containing* $\mathbf{n}$ *and closed under successor.*

The formula is stratified, giving $\mathbf{n}$ and $\mathbf{k}$ both index 0. STEM is a parameter. Hence the definition is legal in INF.

Lemma 11.2. *Suppose there is a double successor* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *with* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \neq \mathbf{k}$. *Then* $\mathbf{n} \in \mathcal{L}(\mathbf{n})$ *and* $\mathcal{L}(\mathbf{n})$ *is closed under Church successor.*

Proof. Follows from the definition of $\mathcal{L}(\mathbf{n})$ as the intersection of all sets w that contain $\mathbf{n}$ and are closed under successor. Since $\mathbf{n}$ belongs to every such w, it belongs to their intersection. Suppose $x \in \mathcal{L}(\mathbf{n})$; then $x \in w$, so $\mathsf{S}x \in w$. Then $\mathsf{S}x$ belongs to the intersection of all such w, i.e., $\mathsf{S}x \in \mathcal{L}(\mathbf{n})$. That completes the proof of the lemma.

Lemma 11.3. *Suppose there is a double successor* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *with* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \neq \mathbf{k}$. *Then* $\mathcal{L}(\mathbf{n}) \subseteq \mathbb{N}$.

Proof. $\mathbf{n} \in \mathcal{L}n$ by Lemma 11.2. Then $\mathbb{N}$ is a set containing $\mathbf{n}$ and closed under successor. Then by definition of $\mathcal{L}(\mathbf{n})$, $\mathcal{L}(\mathbf{n}) \subseteq \mathbb{N}$. That completes the proof of the lemma.

Lemma 11.4. *Suppose there is a double successor* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *with* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \neq \mathbf{k}$. *Then* $\mathcal{L}(\mathbf{n}) \cap \mathsf{STEM} = \phi$.

Proof. Assume $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ and $\mathbf{k} \in \mathsf{STEM}$ and $\mathbf{n} \neq \mathbf{k}$. We will prove by induction on j that

$$j \in \mathsf{STEM} \to j \notin \mathcal{L}(\mathbf{n}).$$

The formula is stratified, giving j index 0; STEM and $\mathcal{L}(\mathbf{n})$ are parameters.

Base case: We must show $0 \notin \mathcal{L}$. Let $Z = \mathcal{L}(\mathbf{n}) - \{0\}$. Then Z is closed under successor, by Theorem 3.8. And Z contains $\mathbf{n}$, since $\mathbf{n} \neq 0$ by Lemma 10.13. Therefore $\mathcal{L}(\mathbf{n}) \subseteq Z$. Therefore $0 \notin \mathcal{L}$, as desired.

Induction step: Suppose $\mathsf{S}j \in \mathsf{STEM}$. We have $j \in \mathsf{STEM}$ by Lemma 10.5. By Lemma 10.4, $\mathsf{S}j$ is not a double successor. Therefore, if $\mathsf{S}j = \mathsf{S}\mathbf{n}$, $j = \mathbf{n}$. But $j \neq \mathbf{n}$, since $\mathbf{n} \in \mathcal{L}(\mathbf{n})$ by definition of $\mathcal{L}(\mathbf{n})$, but $j \notin \mathcal{L}$ by the induction hypothesis. Therefore, $\mathsf{S}j \neq \mathsf{S}\mathbf{n}$.

Define $Z = \mathcal{L}(\mathbf{n}) - \{\mathsf{S}j\}$. I say Z is closed under successor. Let $x \in Z$; then $x \in \mathcal{L}(\mathbf{n})$, so $\mathsf{S}x \in \mathcal{L}$. By induction hypothesis $j \notin \mathcal{L}(\mathbf{n})$, but $x \in \mathcal{L}$; therefore $x \neq j$. If $\mathsf{S}x = \mathsf{S}j$ then $\mathsf{S}j$ is a double successor, contradicting Lemma 10.4, since $\mathsf{S}j \in \mathsf{STEM}$. Hence $\mathsf{S}x \in Z$ as claimed.

Now I say $\mathbf{n} \in Z$. Since $\mathbf{n} \in \mathcal{L}(\mathbf{n})$ it suffices to show that $\mathbf{n} \neq \mathsf{S}j$. Suppose to the contrary that $\mathbf{n} = \mathsf{S}j$. Then $\mathbf{n} \in \mathsf{STEM}$, since $\mathsf{S}j \in \mathsf{STEM}$. Since $\mathsf{S}\mathbf{n}$ is a double successor, by Lemma 10.8, $\mathbf{n}$ is the maximal element of STEM. But $\mathbf{k}$ is the maximal element of STEM, by definition of $\mathbf{k}$. Therefore $\mathbf{k} = \mathbf{n}$, contradiction. Hence $\mathbf{n} \neq \mathsf{S}j$. Hence $\mathbf{n} \in Z$, as claimed.

Therefore Z satisfies the conditions defining $\mathcal{L}(\mathbf{n})$. Therefore $\mathcal{L}(\mathbf{n}) \subseteq Z$. Therefore $\mathsf{S}j \notin \mathcal{L}(\mathbf{n})$, as desired. That completes the induction step. That completes the proof of the lemma.

Lemma 11.5. *Suppose there is a double successor* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *with* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \neq \mathbf{k}$. *Then* $\mathbb{N} = \mathcal{L}(\mathbf{n}) \cup \mathsf{STEM}$.

Proof. Assume $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ and $\mathbf{k} \in \mathsf{STEM}$ and $\mathbf{n} \neq \mathbf{k}$. We will prove by induction on x that

$$x \in \mathbb{N} \to x \in \mathcal{L}(\mathbf{n}) \cup \mathsf{STEM} \tag{12}$$

The formula is stratified, giving x index 0; $\mathcal{L}(\mathbf{n})$ is a parameter.

Base case: $\mathbf{0} \in \mathsf{STEM}$, by Lemma 10.2. Therefore $\mathbf{0} \in \mathcal{L}(\mathbf{n}) \cup \mathsf{STEM}$. That completes the base case.

Induction step: Let $x \in \mathcal{L}(\mathbf{n}) \cup \mathsf{STEM}$. Then $x \in \mathcal{L}(\mathbf{n}) \;\vee\; x \in \mathsf{STEM}$.

Case 1: $x \in \mathcal{L}(\mathbf{n})$. Then by Lemma 11.2, $\mathsf{S}x \in \mathcal{L}(\mathbf{n})$, so $\mathsf{S}x \in \mathcal{L}(\mathbf{n}) \cup \mathsf{STEM}$.

Case 2: $x \in \mathsf{STEM}$. We have

$$\begin{array}{rl} \mathbf{k} \in \mathsf{STEM} & \text{by hypothesis} \\ \mathbf{k} \in \mathbb{N} & \text{by Lemma 10.2} \\ x = \mathbf{k} \vee x \neq \mathbf{k} & \text{by Lemma 10.6} \end{array}$$

Therefore we may argue by cases according as $x = \mathbf{k}$ or not.

Case 2a: $x \neq \mathbf{k}$. Then

$$\begin{array}{rl} \forall u\,(u \in \mathbb{N} \to \mathsf{S}u = \mathsf{S}x \to u = x) & \text{by Lemma 10.11} \\ \mathsf{S}x \in \mathsf{STEM} & \text{by Lemma 10.3} \\ x \in \mathcal{L}(\mathbf{n}) \cup \mathsf{STEM} & \text{by definition of union} \end{array}$$

Case 2b: $x = \mathbf{k}$. Then

$$\begin{array}{rl} \mathbf{n} \in \mathbb{N} & \text{by Lemma 11.3} \\ \mathsf{S}\mathbf{n} \in \mathcal{L}(\mathbf{n}) & \text{by Lemma11.2} \\ \mathsf{S}x = \mathsf{S}\mathbf{k} = \mathsf{S}n & \text{by hypothesis} \\ \mathsf{S}x \in \mathsf{STEM} \cup \mathcal{L}(\mathbf{n}) & \text{by definition of union} \end{array}$$

That completes the induction step. That completes the proof of (12).

By (12), $\mathbb{N} \subseteq \mathcal{L}(\mathbf{n}) \cup \mathsf{STEM}$. It remains to prove $\mathcal{L}(\mathbf{n}) \cup \mathsf{STEM} \subseteq \mathbb{N}$. Suppose $x \in \mathcal{L}(\mathbf{n}) \cup \mathsf{STEM}$. Then $x \in \mathcal{L}(n)$ or $x \in \mathsf{STEM}$. If $x \in \mathcal{L}(n)$, then $x \in \mathbb{N}$ by Lemma 11.3. If $x \in \mathsf{STEM}$, then $x \in \mathbb{N}$ by Lemma 10.2. That completes the proof of the lemma.

Lemma 11.6. *Suppose there is a double successor* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *with* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \neq \mathbf{k}$. *Then* $\mathcal{L}(\mathbf{n}) = \mathbb{N} - \mathsf{STEM}$. *Consequently* $\mathcal{L}(n)$ *does not depend on the choice of* $\mathbf{n}$.

Remark. This lemma is never used; we include it only to clarify why we keep writing in English "the loop", while in formulas we keep writing $\mathcal{L}(\mathbf{n})$ as if "the loop" depended on $\mathbf{n}$.

Proof. By Lemma 11.5, we have $\mathbb{N} = \mathcal{L}(\mathbf{n}) \cup \mathsf{STEM}$. Therefore it suffices to prove

$$\mathcal{L}(\mathbf{n}) = (\mathcal{L}(n) \cup \mathsf{STEM}) - \mathsf{STEM} \tag{13}$$

Left to right: Suppose $t \in \mathcal{L}(\mathbf{n})$. By Lemma 11.4, $t \notin \mathsf{STEM}$. Therefore $t \in (\mathcal{L}(n) \cup \mathsf{STEM}) - \mathsf{STEM}$, as desired.

Right to left: Suppose $t \in (\mathcal{L}(n) \cup \mathsf{STEM}) - \mathsf{STEM}$. Then $t \in \mathcal{L}(\mathbf{n})$. That completes the proof of the lemma.

Lemma 11.7. *Suppose there is a double successor* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *with* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \neq \mathbf{k}$. *Then* $\exists p \in \mathbb{N}\, (p \in \mathcal{L}(\mathbf{n}) \ \wedge\ \mathsf{S}p = \mathbf{n})$.

Proof. We have

$$\begin{array}{rl}
\mathbf{n} \notin \mathsf{STEM} & \text{by Lemma 10.11} \\
\mathbf{0} \in \mathsf{STEM} & \text{by Lemma 10.3} \\
\mathbf{n} \neq \mathbf{0} & \text{by the preceding two lines} \\
\mathbf{n} = \mathsf{S}p & \text{for some } p\text{, by Lemma 3.9}
\end{array}$$

By Lemma 11.5, $p \in \mathcal{L}(\mathbf{n}) \ \vee\ p \in \mathsf{STEM}$. We argue by cases accordingly.

Case 1, $p \in \mathcal{L}(\mathbf{n})$. Then we use p to instantiatiate $\exists p$. That completes Case 1.

Case 2, $p \in \mathsf{STEM}$. Since we have decidable equality on STEM. By Lemma 10.6, we have $p = \mathbf{k} \ \vee\ p \neq \mathbf{k}$. We argue by cases accordingly.

Case 2a, $p = \mathbf{k}$. Then $\mathbf{n} = \mathsf{S}p = \mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$, so $\mathbf{n} = \mathsf{S}\mathbf{n}$. We use n to instantiate $\exists p$. We have $\mathbf{n} \in \mathcal{L}(\mathbf{n})$ by Lemma 11.2. That completes Case 2a.

Case 2b, $p \neq \mathbf{k}$. Then

$$\begin{array}{rl}
p < \mathbf{k} & \text{by Lemma 10.8} \\
\mathsf{S}p \in \mathsf{STEM} & \text{by Lemma 8.6} \\
\mathsf{STEM} \cap \mathcal{L}(\mathbf{n}) = \Lambda & \text{by Lemma 11.4} \\
\mathbf{n} \in \mathcal{L}(\mathbf{n}) & \text{by Lemma 11.2} \\
\mathsf{S}p \in \mathcal{L}(\mathbf{n}) & \text{since } \mathsf{S}p = \mathbf{n} \\
\mathsf{S}p \notin \mathsf{STEM} & \text{since } \mathsf{STEM} \cap \mathcal{L}(\mathbf{n}) = \phi
\end{array}$$

But that contradicts $\mathsf{S}p \in \mathsf{STEM}$. That completes Case 2b. That completes the proof of the lemma.

Theorem 11.8. *Suppose there is a double successor* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *with* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \neq \mathbf{k}$. *Then* $\mathsf{S} : \mathcal{L}(\mathbf{n}) \to \mathcal{L}(n)$ *is onto.*

Proof. By Lemma 11.2, $\mathcal{L}(\mathbf{n})$ is closed under successor, so $\mathsf{S} : \mathcal{L}(\mathbf{n}) \to \mathcal{L}(n)$. Define

$$Z := \{x \in \mathcal{L}(\mathbf{n}) : \exists y\, (y \in \mathcal{L}(\mathbf{n}) \ \wedge \ \mathsf{S}y = x)\}.$$

The formula is stratified, giving x and y index 0; $\mathcal{L}(\mathbf{n})$ is a parameter. We have

$$\begin{array}{rl}
\mathbf{n} \in \mathcal{L}(\mathbf{n}) & \text{by Lemma 11.2} \\
\exists p \in \mathcal{L}(\mathbf{n})\, (\mathsf{S}p = \mathbf{n}) & \text{by Lemma 11.7} \\
\mathbf{n} \in Z & \text{by the definition of } Z
\end{array}$$

I say that Z is closed under successor. Suppose $x \in Z$. Then

$$\begin{array}{rl}
x \in \mathcal{L}(\mathbf{n}) & \text{by definition of } Z \\
\mathsf{S}x \in \mathcal{L}(\mathbf{n}) & \text{by Lemma 11.2} \\
\mathsf{S}x \in \mathbb{Z} & \text{by the definition of } \mathbb{Z}
\end{array}$$

We have shown that Z contains $\mathbf{n}$ and is closed under successor. Then by the definition of $\mathcal{L}(\mathbf{n})$, we have $\mathcal{L}(n) \subseteq Z$. That completes the proof of the theorem.

Lemma 11.9. *Suppose there is a double successor* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *with* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \neq \mathbf{k}$. *Then* $\mathbf{k} \in \mathbb{N}$.

Proof. We have $\mathsf{STEM} \subseteq \mathbb{N}$, since $\mathbb{N} = \mathsf{STEM} \ \cup \ \mathcal{L}(n)$ by Lemma 11.5. Since $\mathbf{k} \in \mathsf{STEM}$, we have $\mathbf{k} \in \mathbb{N}$. That completes the proof of the lemma.

12. The Annihilation Theorem

Theorem 12.1 (Annihilation Theorem)**.** *Suppose u and m are Church numbers such that $u \oplus m = u$. Let X be any set and let $f : X \to X$ be an injection. Then f, iterated m times, is the identity on X. In symbols, $mfx = x$ for all $x \in X$.*

Remarks. This theorem is proved for any set X, not just for any finite set, and we do not assume $\mathbb{N}$ is finite. Definition 3.2 defines "injection". We also do not need to know that there is only one double successor (and even if there is none, the theorem is still true, although then $m = 0$ is the only possibility.)

Proof. Let $f : X \to \mathbb{N}$, and assume $f \in \mathsf{FUNC}$ and $Rel(f)$. By Lemma 3.5, each iterate uf of f maps X to X and is also a functional relation. Moreover, by Lemma 3.13, each iterate of f is also one-to-one from X to X. Then

$$\begin{array}{rcll}
u & = & u \oplus m & \text{by hypothesis} \\
ufx & = & (u \oplus m)fx & \text{since } u,\ u \oplus m,\ uf, \text{ and } (u \oplus m)f \text{ are functions} \\
 & = & uf(mfx) & \text{by Lemma 7.6}
\end{array}$$

Since uf is one-to-one from X to X, this implies $x = mfx$. That completes the proof of the theorem.

Remark. Nothing proved up to now rules out the possibility that $\mathbf{n} = \mathsf{S}\mathbf{k}$ and $\mathsf{S}\mathbf{n} = \mathbf{n}$. That would make the loop $\mathcal{L}$ contain only one element, and $\mathbf{m}$ would be 1. The following corollary shows that $\mathbf{m}$ is much greater.

Corollary 12.2. *Suppose $x = x \oplus m$ for some $x, m \in \mathbb{N}$. Then m is not equal to 1, 2, 3, …, where by* 1 *we mean* $\mathsf{S}\mathbf{0}$*, etc.*

Remark. Formally, this is a different theorem for each value of m. We formalized the cases $m = 1$ and $m = 2$ in Lean, which was sufficient for our application.

Proof. If there is a finite set X with a permutation f that is not the identity on X, but df is the identity on X, then $\mathbf{m} \neq d$. (Here d is not a variable, but a specific named integer, with a different proof for each d.) For example, when $d = \mathsf{S}\mathbf{0}$, we have $\mathbf{0} \neq \mathsf{S}\mathbf{0}$ by Theorem 3.8. We can define a permutation f of $\{\mathbf{0}, \mathsf{S}\mathbf{0}\}$ that interchanges $\mathbf{0}$ and $\mathsf{S}\mathbf{0}$. (It takes about 400 steps to verify that formally, as the definition of permutation has several clauses.) Therefore $\mathbf{m} \neq \mathsf{S}\mathbf{0}$.

Therefore there are at least three elements in $\mathbb{N}$, namely $\mathbf{0}$, $\mathbf{n}$, and $\mathsf{S}\mathbf{n}$. I say these are distinct elements. We have $\mathsf{S}\mathbf{n} \neq \mathbf{n}$ since we have just shown $\mathbf{m} \neq \mathbf{0}$. We have $\mathsf{S}n \neq \mathbf{0}$ by Theorem 3.8. And we have $\mathbf{n} \neq \mathbf{0}$ by Lemma 10.13. We can then construct a permutation f of $\mathbb{N}$ such that jf is not the identity for $j = \mathsf{S}\mathbf{0}$ or $j = \mathsf{S}(\mathsf{S}\mathbf{0})$. Therefore $\mathbf{m} \neq \mathsf{S}(\mathsf{S}\mathbf{0})$. Then one can show that there are three distinct members of $\mathcal{L}(\mathbf{n})$, so there are four distinct members of $\mathbf{n}$, and we can construct a permutation of those members to show that $\mathbf{m} \neq \mathsf{S}(\mathsf{S}(\mathsf{S}\mathbf{0}))$. Similarly we can continue through any particular value of $\mathbf{m}$. That is, $\mathbf{m}$ is not equal to any integer with a name, as for such d we can construct the required permutation.

Corollary 12.3. *Nothing is its own successor. That is, for $x \in \mathbb{N}$, we have $\mathsf{S}x \neq x$.*

Remark. This corollary shows that the loop does not degenerate to a singleton, in that $\mathsf{S}\mathbf{n} \neq \mathbf{n}$, but it applies more generally to any Church number x. Thanks to Albert Visser for pointing out that we can obtain this corollary immediately for any x, not just for $\mathbf{n}$. In fact we do not even need to assume that there is a double successor.

Proof. We have $\mathsf{S}x = x \oplus \mathsf{S}0 = x \oplus 1$. Then if $\mathsf{S}x = x$ we have $x = x \oplus m$ with $m = 1$, contradicting Corollary 12.2. That completes the proof.

Corollary 12.4. *For $x \in \mathbb{N}$, we have $\mathsf{S}(\mathsf{S}x) \neq x$.*

Remark. To formalize this result, we have to formalize Lemma 12.2 for $\mathbf{m} = 2$, or more precisely, $\mathbf{m} = \mathsf{S}(\mathsf{S}\mathbf{0})$), which involves constructing a permutation of three elements. We define $X = \{a, b, c\}$ where $a = \mathbf{0}$, $b = \mathsf{S}a$, and $c = \mathsf{S}b$. Those three elements are distinct, by Lemma 12.3 and Theorem 3.8. To prove that there is a permutation of X requires about 700 steps, which we omit here. (There are several arguments by cases with nine cases.) Somewhat surprisingly, one does not need to first prove X is finite.

Proof. Suppose $\mathsf{S}(\mathsf{S}x) = x$. Then

$$\begin{aligned}
x &= x \oplus \mathbf{0} && \text{by Lemma 4.4} \\
\mathsf{S}x &= \mathsf{S}(x \oplus \mathbf{0}) && \text{by the previous line} \\
&= x \oplus \mathsf{S}\mathbf{0} && \text{by Lemma 7.2} \\
\mathsf{S}(\mathsf{S}x) &= \mathsf{S}(x \oplus \mathsf{S}\mathbf{0}) && \text{by the previous line} \\
&= x \oplus \mathsf{S}(\mathsf{S}\mathbf{0}) && \text{by Lemma 7.2} \\
x &= x \oplus \mathsf{S}(\mathsf{S}\mathbf{0}) && \text{since } \mathsf{S}(\mathsf{S}x) = x
\end{aligned}$$

But that contradicts Lemma 12.2. That completes the proof.

Corollary 12.5. *If $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ with $\mathbf{k} \in \mathsf{STEM}$ and $\mathbf{n} \in \mathbb{N}$ and $\mathbf{k} \neq \mathbf{n}$, then $\mathbf{k} < \mathbf{n}$. That is, there exists $m \in \mathbb{N}$ such that $\mathbf{n} = \mathbf{k} \oplus m$.*

Proof. Define

$$Z = \{x \in \mathsf{STEM} : x \leq \mathbf{n}\}.$$

I say that Z contains 0 and is closed under successor except double successors. We have

$$\begin{array}{rl} \mathbf{0} \in \mathsf{STEM} & \text{by Lemma 10.3} \\ \mathbf{0} \oplus \mathbf{n} = \mathbf{n} & \text{by Lemma 7.1} \\ \mathbf{0} \leq \mathbf{n} & \text{by definition of } < \\ \mathbf{0} \in Z & \text{by definition of } Z \end{array}$$

Now suppose $x \in Z$ and $\mathsf{S}x$ is not a double successor. We must show $\mathsf{S}x \in Z$. We have

$$\begin{array}{rl} x \in \mathsf{STEM} \ \wedge \ x \leq \mathbf{n} & \text{by the definition of } Z \\ \mathsf{S}x \in \mathsf{STEM} & \text{by Lemma 10.3} \\ x \neq \mathbf{n} & \text{by Lemma 10.11, since } \mathsf{S}x \text{ is not a double successor} \\ x < \mathbf{n} & \text{by Lemma 8.7} \\ \mathsf{S}x \leq \mathbf{n} & \text{by Lemma 8.8} \end{array}$$

Hence $\mathsf{STEM} \subseteq Z$. Then $\mathbf{k} \in Z$. Therefore $\mathbf{k} \leq \mathbf{n}$. Since $\mathbf{k} \neq \mathbf{n}$ we have $\mathbf{k} < \mathbf{n}$, by Lemma 8.7. By definition of $<$, there exists $m \in \mathbb{N}$ such that $\mathbf{n} = \mathbf{k} \oplus m$. That completes the proof of the corollary.

Remarks. m is not asserted to be unique. We do not know if m has to be in the loop or has to be in the stem.

In order to apply the Annihilation Theorem (Theorem 12.1), we need to know that the iterates of f still map X to X. That is the content of the next lemma.

Lemma 12.6. *Let X be any set. Let $f : X \to X$, and suppose $f \in \mathsf{FUNC}$ and $Rel(f)$. Then*

$$q \in \mathbb{N} \to x \in X \to qfx \in X.$$

Proof. The formula is stratified, giving x index 0, f index 3, and q index 6. Therefore we may proceed by induction on q.

Base case, $q = \mathbf{0}$. Then

$$\begin{array}{rl} x \in X & \text{by hypothesis} \\ \mathbf{0}fx = x & \text{by Lemma 2.13} \end{array}$$

That completes the base case.

Induction step.

$$\begin{array}{rl} qfx \in X & \text{by the induction hypothesis} \\ \mathsf{S}(qfx) \in X & \text{since } f : X \to X \\ \mathsf{S}qfx = \mathsf{S}(qfx) & \text{by Theorem 3.6} \\ \mathsf{S}qfx \in X & \text{by the preceding two lines} \end{array}$$

That completes the induction step. That completes the proof of the lemma.

13. Some consequences of assuming $\mathbb{N}$ is finite

We take this opportunity to point out that "$\mathbb{N}$ is not finite" is, on the face of it at least, a weaker assertion than "$\mathbb{N}$ is infinite", where the latter is taken in Dedekind's sense, that the Church successor function is one-to-one. Thus "$\mathbb{N}$ is finite" is a stronger assumption than "$\mathbb{N}$ is not infinite". In this section we show that under the assumption that $\mathbb{N}$ is finite, we rather quickly reach several important results: $\mathbb{N}$ has decidable equality, successor is one-to-one on the loop $\mathcal{L}$, and there is a unique double successor.

That $\mathbb{N}$ has decidable equality is immediate if we assume $\mathbb{N}$ is finite, since according to Lemma 3.3 of [1], every finite set has decidable equality.

Lemma 13.1. *If $\mathbb{N}$ is finite, and there is a double successor $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ with $\mathbf{k} \in \mathsf{STEM}$, then $\mathcal{L}(\mathbf{n})$ is finite.*

Proof. Assume $\mathbb{N}$ is finite and there is a double successor $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ with $\mathbf{k} \in \mathsf{STEM}$. I say that $\mathcal{L}(\mathbf{n})$ is a separable subset of $\mathbb{N}$. By Definition 3.16 of [1], that means that $\mathbb{N} = \mathcal{L} \cup (\mathbb{N} - \mathcal{L})$. By Lemma 11.5, $\mathbb{N} - \mathcal{L} = \mathsf{STEM}$, and $\mathbb{N} = \mathcal{L} \cup \mathsf{STEM}$, so $\mathcal{L}$ is a separable subset of $\mathbb{N}$, as claimed. Then by Lemma 3.19 of [1], $\mathcal{L}$ is finite. That completes the proof of the lemma.

Theorem 13.2. *If $\mathbb{N}$ is finite, and there is a double successor $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ with $\mathbf{k} \in \mathsf{STEM}$, then Church successor restricted to $\mathcal{L}(\mathbf{n})$ is one-to-one.*

Proof. Assume $\mathbb{N}$ is finite and there is a double successor $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ with $\mathbf{k} \in \mathsf{STEM}$. By Lemma 13.1, $\mathcal{L}(n) \in \mathsf{FINITE}$. By Theorem 11.8, successor is onto as a map from $\mathcal{L}(\mathbf{n})$ to $\mathcal{L}(\mathbf{n})$. By Theorem 13.8 of [1], successor is one-to-one as a map from $\mathcal{L}$ to $\mathcal{L}$. That completes the proof of the theorem.

Theorem 13.3. *Suppose $\mathbb{N}$ is finite and there is a double successor $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ with $\mathbf{k} \neq \mathbf{n}$ and $\mathbf{n} \in \mathbb{N}$ and $\mathbf{k} \in \mathsf{STEM}$. Then there is exactly one double successor. More precisely, if $j, \ell \in \mathbb{N}$ and $j \neq \ell$ and $j < \ell$ and $\mathsf{S}j = \mathsf{S}\ell$, then $j = \mathbf{k}$ and $\ell = \mathbf{n}$.*

Proof. Suppose $\mathbb{N}$ is finite and $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ with $\mathbf{k} \neq \mathbf{n}$ and $\mathbf{k} \in \mathsf{STEM}$. Suppose $\mathsf{S}j = \mathsf{S}\ell$ with $j < \ell$. We have to prove $\ell = \mathbf{n}$.

By Theorem 13.2, successor is one-to-one on $\mathcal{L}$, so not both j and ℓ can belong to $\mathcal{L}(\mathbf{n})$. By Lemma 11.5, each of them belongs to $\mathcal{L}(\mathbf{n})$ or to STEM, and by Lemma 11.4, $\mathcal{L}(n)$ and STEM are disjoint. I say that

$$\ell \in \mathsf{STEM} \rightarrow j \in \mathsf{STEM} \ \wedge \ \mathsf{S}j \in \mathsf{STEM} \tag{14}$$

To prove that, assume $\ell \in \mathsf{STEM}$. Then

$\ell \in \mathsf{STEM}$	by assumption
$j \in \mathsf{STEM}$	by Lemma 10.7, since $j < \ell$

By Lemma 10.3, to prove $\mathsf{S}j \in \mathsf{STEM}$ it suffices to prove that $\mathsf{S}j$ is not a double successor. To that end, assume $\mathsf{S}j = \mathsf{S}v$; we must prove $j = v$. I say that $j \neq \mathbf{k}$.

Here is the proof:

$$\begin{array}{rl}
j = \mathbf{k} & \text{assumption} \\
\ell < \mathbf{k} \ \vee \ \ell = \mathbf{k} & \text{by Lemma 10.8, since } \ell \in \mathsf{STEM} \\
\ell < \mathbf{k} & \text{since } \mathbf{k} \neq \ell \\
\mathbf{k} < \mathbf{k} & \text{by transitivity, since } \mathbf{k} < \ell \\
\mathbf{k} \not< \mathbf{k} & \text{by Lemma 10.10}
\end{array}$$

That contradiction completes the proof that $j \neq \mathbf{k}$. Then by Lemma 10.11, we have $v = j$ as desired. That completes the proof of (14).

Now I say that $\ell \notin \mathsf{STEM}$. To prove that:

$$\begin{array}{rl}
\ell \in \mathsf{STEM} & \text{by assumption} \\
j \in \mathsf{STEM} & \text{by (14)} \\
\mathsf{S}j \in \mathsf{STEM} & \text{by (14)} \\
j = \ell & \text{by Lemma 10.4} \\
j \neq \ell & \text{by Lemma 10.12, since } j < \ell
\end{array}$$

That contradiction completes the proof that $\ell \notin \mathsf{STEM}$.

Then

$$\begin{array}{rl}
\ell \in \mathcal{L}(\mathbf{n}) & \text{by Lemma 11.5, since } \ell \notin \mathsf{STEM} \\
j \in \mathcal{L}(\mathbf{n}) \rightarrow j = \ell & \text{by Theorem 13.2} \\
j \notin \mathcal{L}(\mathbf{n}) & \text{since } j \neq \ell \\
j \in \mathsf{STEM} & \text{by Lemmas 11.5 and 11.4} \\
\mathsf{STEM} = \{x \in \mathbb{N} : x < \mathbf{k} \vee x = \mathbf{k}\} & \text{by Lemma 10.8} \\
\mathsf{S}\mathbf{k} \notin \mathsf{STEM} & \text{by Lemma 10.4 applied to } \mathbf{k}, \mathbf{n} \\
\mathbf{k} \neq \mathsf{S}\mathbf{k} & \text{since } \mathbf{k} \in \mathsf{STEM} \text{ but } \mathsf{S}\mathbf{k} \notin \mathsf{STEM} \\
\mathbf{k} \in \mathbb{N} & \text{by Lemma 11.9} \\
j = \mathbf{k} \ \vee \ j \neq \mathbf{k} & \text{by Lemma 3.3 of [1], since } \mathbb{N} \in \mathsf{FINITE}
\end{array}$$

We argue by cases accordingly.

Case 1, $j = \mathbf{k}$. Then

$$\begin{array}{rl}
\mathsf{S}\mathbf{k} = \mathsf{S}\ell & \text{since } \mathsf{S}\mathbf{k} = \mathsf{S}j = \mathsf{S}\ell \\
\mathsf{S}\mathbf{n} = \mathsf{S}\ell & \text{since } \mathsf{S}\mathbf{k} = \mathsf{S}n \\
\ell \in \mathcal{L}(\mathbf{n}) & \text{by Lemma 11.5} \\
\mathsf{S}\ell \in \mathcal{L}(\mathbf{n}) & \text{by Lemma 11.2} \\
\mathsf{S}\mathbf{n} \in \mathcal{L}(\mathbf{n}) & \text{by Lemma 11.2} \\
\mathbf{n} = \ell & \text{by Theorem 13.2}
\end{array}$$

That completes Case 1.

Case 2, $j \neq \mathbf{k}$. Then

$$\begin{array}{rl} \mathsf{S}j \text{ is not a double successor} & \text{by Lemma 10.11} \\ \mathsf{S}j \in \mathsf{STEM} & \text{by Lemma 10.3, since } j \in \mathsf{STEM} \\ j = \ell & \text{by Lemma 10.4} \\ j \neq \ell & \text{by hypothesis} \end{array}$$

That contradiction completes Case 2. That completes the proof of the theorem.

Corollary 13.4. *Suppose $\mathbb{N}$ is finite and there is a double successor $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ with $\mathbf{k} \neq \mathbf{n}$ and $\mathbf{n} \in \mathbb{N}$ and $\mathbf{k} \in \mathsf{STEM}$. Suppose $j, \ell \in \mathbb{N}$ and $j \neq \ell$ and $\mathsf{S}j = \mathsf{S}\ell$. Then $\{j, \ell\} = \{\mathbf{k}, \mathbf{n}\}$, i.e., j and ℓ are $\mathbf{n}$ and $\mathbf{k}$ or $\mathbf{k}$ and $\mathbf{n}$.*

Proof. By Lemma 8.10, $j < \ell \ \vee \ell < j$. If $j < \ell$ then by Theorem 13.3 we have $j = \mathbf{k}$ and $\ell = \mathbf{n}$. If $\ell < j$ then (applying Theorem 13.3 to ℓ and j instead of to j and ℓ), we have $\ell = \mathbf{k}$ and $j = \mathbf{n}$. That completes the proof of the corollary.

14. A linear order on $\mathbb{N}$

In this section we introduce a certain linear ordering on $\mathbb{N}$, which we write as $x \preceq y$, or in its strict version, $x \prec y$. The definition of $x \preceq y$ will be given in such a way that it does not presume that $\mathbb{N}$ is finite or that there is a double successor, because we need it under those conditions near the end of the paper, after we have proved $\mathbb{N}$ is not finite but still need to prove $\mathbb{N}$ is infinite.

The intuitive meaning of $x \preceq y$ is that we come to x before y as we trace out the stem and then the loop (also allowing $x = y$).

Definition 14.1. *For $X \subseteq \mathbb{N}$, we say "X is closed under successors except greater double successors" to mean*

$$\forall u\, (u \in X \to \forall v \in \mathbb{N}\, (v < u \to \mathsf{S}u = \mathsf{S}v \to u = v) \to \mathsf{S}u \in X)).$$

Remark. $\mathbf{n}$ does not actually appear in the definition of "closed under successors except greater double successors," but the following lemma shows that, if there is a double successor, it really means "closed under successors except $\mathbf{n}$." However, the definition does not *assume* that there is a double successor.

Lemma 14.2. *Suppose $\mathbb{N}$ is finite, and $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ with $\mathbf{k} \in \mathsf{STEM}$ and $\mathbf{n} \neq \mathbf{k}$. Let $X \subseteq \mathbb{N}$. Then*

$$\forall u\, (u \in X \to \forall v \in \mathbb{N}\, (v < u \to \mathsf{S}u = \mathsf{S}v \to u = v) \to \mathsf{S}u \in X))$$

(which is the formula in the preceding definition) is equivalent to

$$\forall u\, (u \in X \to u \neq \mathbf{n} \to \mathsf{S}u \in X).$$

Proof. Let $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ with $\mathbf{k} \in \mathsf{STEM}$ and $\mathbf{n} \neq \mathbf{k}$, and let X be any set. We have to prove

$$\begin{array}{rl} & \forall u\, (u \in X \to \forall v \in \mathbb{N}\, (v < u \to (\mathsf{S}u = \mathsf{S}v \to u = v) \to \mathsf{S}u \in X)) \\ \leftrightarrow & \forall u\, (u \in X \to u \neq \mathbf{n} \to \mathsf{S}u \in X). \end{array}$$

Left to right: Assume $u \in X$ and $u \neq \mathbf{n}$. Instantiating the left side to u, we see that it suffices to prove

$$\forall v \in \mathbb{N}\, (v < u \to \mathsf{S}u = \mathsf{S}v \to u = v).$$

Suppose $v \in \mathbb{N}$ and $v < u$ and $\mathsf{S}u = \mathsf{S}v$. Since $u \in X$ and $X \subseteq \mathbb{N}$, we have $u \in \mathbb{N}$. Since $\mathbb{N}$ is finite, it has decidable equality, by Lemma 3.3 of [1]. Therefore $u = v \ \vee \ u \neq v$. If $u = v$, the desired conclusion is immediate, so we may assume $u \neq v$. Then by Theorem 13.3, since $u \neq \mathbf{n}$, we have $u = v$ as desired. That completes the left-to-right direction.

Right to left: Assume

$$\forall u \, (u \in X \to u \neq \mathbf{n} \to \mathsf{S}u \in X)) \tag{15}$$

and suppose $u \in X$ and

$$\forall v < u \, (\mathsf{S}u = \mathsf{S}v \to u = v). \tag{16}$$

We must prove $\mathsf{S}u \in X$. We have

$$\begin{array}{ll} \mathbf{k} \in \mathbb{N} & \text{by Lemma 11.9} \\ \mathbf{k} < \mathbf{n} & \text{by Corollary 12.5} \end{array}$$

We have $u \neq \mathbf{n}$, since if $u = \mathbf{n}$ then taking $u = \mathbf{n}$ and $v = \mathbf{k}$ in (16) we have $\mathsf{S}u = \mathsf{S}v$, so $u = v$, i.e., $\mathbf{n} = \mathbf{k}$, contradiction. Then by (15), we have $\mathsf{S}u \in X$, as desired. That completes the right-to-left direction. That completes the proof of the lemma.

Definition 14.3. *The relation $x \preceq y$, means that $x \in \mathbb{N}$ and $y \in \mathbb{N}$ and y belongs to every separable subset of $\mathbb{N}$ containing x and closed under successors except greater double successors.*

Explicitly,

$$\begin{aligned} &x \preceq y \leftrightarrow \forall X \, (\mathbb{N} = X \cup (\mathbb{N} - X) \to x \in X \\ &\quad \to \forall u \, (u \in X \to \forall v \in \mathbb{N} \, (v < u \to (\mathsf{S}u = \mathsf{S}v \to u = v) \to \mathsf{S}u \in X) \to y \in X. \end{aligned}$$

The definition is stratified, giving x and y index 0 and X index 1. $\mathbb{N}$ is a parameter. Since x and y get the same index, the relation $x \preceq y$ is definable in INF.

Lemma 14.4. *Suppose $\mathbb{N} \in \mathsf{FINITE}$ and $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ and $\mathbf{k} \neq \mathbf{n}$ and $\mathbf{k} \in \mathsf{STEM}$ and $\mathbf{n} \in \mathbb{N}$. Then for all $x, y \in \mathbb{N}$, we have $x \preceq y$ if and only if*

$$\forall w \, (\mathbb{N} = X \cup (\mathbb{N} - X) \to x \in w \to (\forall u \, (u \in w \to u \neq \mathbf{n} \to \mathsf{S}u \in w) \to y \in w).$$

Remark. Although $\mathbf{n}$ appears in this lemma, $\mathbf{n}$ does not appear in the definition of $\preceq$. We can use therefore use this lemma to express $\preceq$ in terms of any (hypothesized) double successor, without it depending on the particular double successor.

Proof. Using Lemma 14.2 (in the right-to-left direction) to rewrite the closure condition in the lemma, we see that it suffices to prove

$$\begin{aligned} x \preceq y \leftrightarrow \forall w \, (\mathbb{N} = X \cup (\mathbb{N} - X) \to x \in w \to \\ \forall u \, (u \in w \to \forall v \in \mathbb{N} \, (v < u \to \mathsf{S}u = \mathsf{S}v \to u = v) \to \mathsf{S}u \in w) \\ \to y \in w) \end{aligned}$$

But that is just Definition 14.3 (up to renaming a bound variable). That completes the proof of the lemma.

Definition 14.5. *We define*

$$x \prec y \leftrightarrow x \preceq y \ \wedge x \ \neq y.$$

Lemma 14.6 (Transitivity of $\preceq$)**.** *For $x, y, z \in \mathbb{N}$ we have*

$$x \preceq y \to y \preceq z \to x \preceq z.$$

Proof. Suppose $x \preceq y$ and $y \preceq z$. Let X be a separable subset of $\mathbb{N}$ closed under successors except greater double successors. Suppose $x \in X$. Since $x \preceq y$ we have $y \in X$. Since $y \preceq z$, we have $z \in X$. Then by the definition of $\preceq$, we have $x \preceq z$. That completes the proof of the lemma.

Lemma 14.7. *For $x \in \mathbb{N}$ we have $x \preceq x$.*

Proof. x belongs to every separable set X containing x and satisfying some condition; putting in the particular condition from the definition of $\preceq$ we have the desired result. That completes the proof of the lemma.

Lemma 14.8. *Suppose $x \in \mathbb{N}$ and $x \preceq \mathbf{0}$. Then $x = \mathbf{0}$.*

Proof. By Theorem 3.8, $Z := \mathbb{N} - \{\mathbf{0}\}$ is closed under successor. By Lemma 3.10, $x = \mathbf{0} \ \vee \ x \neq \mathbf{0}$. Therefore Z is a separable subset of $\mathbb{N}$. If $x \neq \mathbf{0}$, then $x \in Z$. Since $x \preceq \mathbf{0}$, then $\mathbf{0} \in Z$. But $\mathbf{0} \notin Z$. Therefore $x = \mathbf{0}$. That completes the proof of the lemma.

Lemma 14.9. *For $x \in \mathbb{N}$, we have $\neg\,(x \prec \mathbf{0})$.*

Proof. Suppose $x \in \mathbb{N}$ and $x \prec \mathbf{0}$. By definition of $\prec$, $x \preceq \mathbf{0}$ and $x \neq \mathbf{0}$. By Lemma 14.8, $x = \mathbf{0}$, contradiction. That completes the proof of the lemma.

Lemma 14.10. *Suppose $\mathbb{N} \in \mathsf{FINITE}$ and $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ and $\mathbf{k} \neq \mathbf{n}$ and $\mathbf{k} \in \mathsf{STEM}$ and $\mathbf{n} \in \mathbb{N}$. Then for $x, y \in \mathbb{N}$ we have*

$$y \neq \mathbf{n} \to x \preceq \mathsf{S}y \leftrightarrow x \preceq y \ \vee \ x = \mathsf{S}y.$$

Remark. The reader should refer to Fig. 1 to see why the condition $y \neq \mathbf{n}$ is needed.

Proof. Suppose $y \neq \mathbf{n}$. Left to right: suppose $x \preceq \mathsf{S}y$. Since $\mathbb{N}$ is finite, it has decidable equality, so $x = \mathsf{S}y \ \vee \ x \neq \mathsf{S}y$. If $x = \mathsf{S}y$ we are done, so we may suppose $x \neq \mathsf{S}y$. We have to prove $x \preceq y$. Let X be a separable subset of $\mathbb{N}$ closed under successor except $\mathbf{n}$ and containing x. We have to prove $y \in X$. Since X is a separable subset of $\mathbb{N}$, we have $y \in X \ \vee \ y \notin X$. If $y \in X$, we are done, so we may assume $y \notin X$. Define $Z := X - \{\mathsf{S}y\}$. Since X is a separable subset of $\mathbb{N}$ and $\mathbb{N}$ has decidable equality, Z is a separable subset of $\mathbb{N}$ (80 steps omitted). Since $x \neq \mathsf{S}y$, we have $x \in Z$.

I say that Z is closed under successor except $\mathbf{n}$. To prove that, suppose $u \in \mathbb{Z}$ and $u \neq \mathbf{n}$; we must prove $\mathsf{S}u \in \mathbb{Z}$. We have $\mathsf{S}u \in X$ since X is closed under successor except $\mathbf{n}$. Since $Z = X - \{\mathsf{S}y\}$, it suffices to prove $\mathsf{S}u \neq \mathsf{S}y$. Suppose that $\mathsf{S}u = \mathsf{S}y$; we must derive a contradiction.

$u = y$	by Corollary 13.4, since $u \neq \mathbf{n}$ and $y \neq \mathbf{n}$
$u \notin X$	since $y \notin X$ and $u = y$
$u \in X$	since $u \in Z = X - \{\mathsf{S}y\}$

That completes the proof that Z is closed under successor except $\mathbf{n}$. Since $x \in Z$ and $x \preceq \mathsf{S}y$, we have $\mathsf{S}y \in Z$. But that is a contradiction. That completes the proof of the left-to-right direction of the lemma.

Right to left: Suppose $y \neq \mathbf{n}$ and $x \preceq y \ \vee \ x = \mathsf{S}y$. We must prove $x \preceq \mathsf{S}y$. Let X be a separable subset of $\mathbb{N}$ closed under successor except $\mathbf{n}$ and containing x; we must prove $\mathsf{S}y \in X$. Since $x \preceq y \ \vee \ x = \mathsf{S}y$, we may argue by cases.

Case 1, $x \preceq y$. Since $x \in X$ and $y \neq \mathbf{n}$, we have $\mathsf{S}y \in X$. That completes case 1.

Case 2, $x = \mathsf{S}y$. Since $x \in X$ we have $\mathsf{S}y \in X$. That completes Case 2. That completes the proof of the lemma.

Corollary 14.11. *Suppose* $\mathbb{N} \in \mathsf{FINITE}$ *and* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *and* $\mathbf{k} \neq \mathbf{n}$ *and* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \in \mathbb{N}$*. Then for* $x, y \in \mathbb{N}$ *we have*

$$x \neq \mathbf{n} \rightarrow x \preceq \mathsf{S}x.$$

Proof. By Lemma 14.7, we have $x \preceq x$. Taking $y = x$ in Lemma 14.10, we have $x \preceq \mathsf{S}x$ as desired. That completes the proof of the corollary.

Corollary 14.12. *Suppose* $\mathbb{N} \in \mathsf{FINITE}$ *and* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *and* $\mathbf{k} \neq \mathbf{n}$ *and* $\mathbf{k} \in \mathsf{STEM}$*. Then for all* $x \in \mathbb{N}$*, we have*

$$x \neq \mathbf{n} \rightarrow x \prec \mathsf{S}x.$$

Proof. Suppose $x \neq \mathbf{n}$ and $x \in \mathbb{N}$. We have

$$\begin{array}{ll} x \preceq \mathsf{S}x & \text{by Lemma 14.11} \\ x \neq \mathsf{S}x & \text{by Lemma 12.3} \\ x \prec \mathsf{S}x & \text{by definition of } \prec \end{array}$$

That completes the proof of the lemma.

Lemma 14.13. *Suppose* $\mathbb{N} \in \mathsf{FINITE}$ *and* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *and* $\mathbf{k} \neq \mathbf{n}$ *and* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \in \mathbb{N}$*. Then for* $x, y \in \mathbb{N}$ *we have*

$$x \prec y \rightarrow \mathsf{S}x \preceq y.$$

Proof. Suppose $x \prec y$. By definition of $\prec$, $x \preceq y$ and $x \neq y$. We must prove $\mathsf{S}x \preceq y$. By Lemma 14.4, it suffices to show that for every separable subset X of $\mathbb{N}$ that contains $\mathsf{S}x$ and is closed under successor except $\mathbf{n}$, we have $y \in X$. Let X be such a set, and define

$$Z := X \cup \{x\} \tag{17}$$

Since $\mathbb{N}$ is finite, it has decidable equality; hence Z is a separable subset of $\mathbb{N}$. Since $\mathsf{S}x \in X$, we have $\mathsf{S}x \in Z$, so Z is closed under successor except $\mathbf{n}$. We have $x \in Z$ by (17). Since $x \preceq y$, we have $y \in Z$ by Lemma 14.4. Since $x \neq y$, we have $y \in X$ by (17). That completes the proof of the lemma.

Lemma 14.14. *Suppose* $\mathbb{N} \in \mathsf{FINITE}$ *and* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *and* $\mathbf{k} \neq \mathbf{n}$ *and* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \in \mathbb{N}$*. Then for all* $x \in \mathbb{N}$ *we have* $x \preceq \mathbf{n}$*.*

Proof. Suppose $\mathbb{N} \in \mathsf{FINITE}$ and $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ and $\mathbf{k} \neq \mathbf{n}$ and $\mathbf{k} \in \mathsf{STEM}$ and $\mathbf{n} \in \mathbb{N}$. We begin by proving

$$\mathsf{S}\mathbf{k} \preceq \mathbf{n} \tag{18}$$

To prove that, let X be a separable subset of $\mathbb{N}$ containing $\mathsf{S}\mathbf{k}$ and closed under successor except $\mathbf{n}$. We must prove $\mathbf{n} \in X$.

Define $Z := X \cup \{\mathbf{n}\}$. I say that Z is closed under successor. To prove that: if $x \in Z$ then $x \in X \ \vee \ x = \mathbf{n}$. If $x \in X$ and $x \neq \mathbf{n}$, then $\mathsf{S}x \in X$, since X is closed under successor except $\mathbf{n}$. But if $x = \mathbf{n}$ then $\mathsf{S}x = \mathsf{S}\mathbf{n} = \mathsf{S}k$, which is in X by hypothesis, and hence in Z. Since $\mathbb{N}$ is finite, it has decidable equality, so these cases are exhaustive. Hence Z is closed under successor, as claimed.

Now we can prove $\mathbf{n} \in X$:

$\mathcal{L}(n) \subseteq Z$	by the definition of $\mathcal{L}(\mathbf{n})$
$\mathbf{n} \in \mathcal{L}(\mathbf{n})$	by Lemma 11.2
$\mathbf{0} \in \mathsf{STEM}$	by Lemma 10.3
$\mathcal{L}(n) \cap \mathsf{STEM} = \Lambda$	by Lemma 11.4
$\mathbf{n} \neq \mathbf{0}$	by the preceding lines
$\mathbf{n} = \mathsf{S}r$	for some $r \in \mathcal{L}(\mathbf{n})$, by Theorem 11.8
$r \in Z$	since $\mathcal{L}(\mathbf{n}) \subseteq Z$
$r \neq n$	by Lemma 12.3
$r \in X$	since $Z = X \cup \{n\}$
$\mathsf{S}r \in X$	since X is closed under successor except $\mathbf{n}$, and $r \neq \mathbf{n}$
$\mathbf{n} \in X$	since $\mathsf{S}r = \mathbf{n}$

That completes the proof that $\mathbf{n} \in X$. That completes the proof of (18)

We must prove

$$\forall x \in \mathbb{N}\,(x \preceq \mathbf{n}).$$

We will prove this by induction on x. The formula to be proved is stratified, giving $x, \mathbf{k}, \mathbf{n}$ all index 0, since $\preceq$ is a definable relation, appearing here as a parameter. Therefore we may proceed by induction on x.

Base case. $\mathbf{0} \preceq \mathbf{n}$ by Lemma 14.8.

Induction step. The induction hypothesis is $x \preceq \mathbf{n}$. We have to prove $\mathsf{S}x \preceq n$. Since $\mathbb{N}$ is finite, it has decidable equality, so we have $x = \mathbf{n} \ \vee \ x \neq \mathbf{n}$. If $x = \mathbf{n}$, we are done by (18), since $\mathsf{S}\mathbf{n} = \mathsf{S}\mathbf{k}$. Therefore we may assume $x \neq \mathbf{n}$. Then

$x \prec \mathbf{n}$	by definition of $\prec$
$\mathsf{S}x \preceq \mathbf{n}$	by Lemma 14.13 with $\mathbf{n}$ for y

That completes the induction step. That completes the proof of the lemma.

Lemma 14.15 (Finite induction)**.** *Suppose* $\mathbb{N} \in \mathsf{FINITE}$ *and* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *and* $\mathbf{k} \neq \mathbf{n}$ *and* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \in \mathbb{N}$. *Suppose* $\mathbf{0} \in X$ *and* $\forall u\,(u \in X \to u \neq \mathbf{n} \to \mathsf{S}u \in X)$. *Then* $\mathbb{N} \subseteq X$.

Proof. We will prove by induction on z that

$$\forall x \in \mathbb{N}\,(x \preceq z \to x \in X). \tag{19}$$

The formula is stratified, giving x and z index 0, since $\preceq$ is a definable relation, so we may proceed by induction.

Base case, $z = \mathbf{0}$. We must show $x \preceq \mathbf{0} \to x \in X$. Suppose $x \preceq \mathbf{0}$. By Lemma 14.8, $x = \mathbf{0}$. Then $x \in X$ by hypothesis. That completes the base case.

Induction step. Suppose

$$\forall x \in \mathbb{N}\,(x \preceq z \to x \in X) \tag{20}$$

and suppose $x \preceq \mathsf{S}z$. We must prove $x \in X$.

$$\begin{array}{rl} \mathbb{N} \in \mathsf{DECIDABLE} & \text{by Lemma 3.3 of [1]} \\ z = \mathbf{n} \ \vee \ z \neq \mathbf{n} & \text{since } \mathbb{N} \in \mathsf{DECIDABLE} \end{array}$$

We argue by cases.

Case 1, $z = \mathbf{n}$. Then

$$\begin{array}{rl} \mathsf{S}z = \mathsf{S}\mathbf{n} = \mathsf{S}\mathbf{k} & \text{since } z = \mathbf{n} \text{ and } \mathsf{S}\mathbf{n} = \mathsf{S}\mathbf{k} \\ x \preceq \mathbf{n} \to x \in X & \text{by (20)} \\ x \preceq \mathbf{n} & \text{by Lemma 14.14} \\ x \in X & \text{by the preceding two lines} \end{array}$$

That completes Case 1.

Case 2. $z \neq \mathbf{n}$.

$$\begin{array}{rl} x \preceq \mathsf{S}z & \text{by hypothesis} \\ x \preceq z \ \vee \ x = \mathsf{S}z & \text{by Lemma 14.10, since } z \neq \mathbf{n} \end{array}$$

If $x \preceq z$, we are done by (20), so we can assume $x = \mathsf{S}z$. Since X is closed under successor except $\mathbf{n}$, and $z \neq \mathbf{n}$, we have $x \in X$. That completes the induction step. That completes the proof of (19).

Now under the assumptions of the lemma, we have to prove $\mathbb{N} \subseteq X$. It suffices to prove that for all z, $z \in \mathbb{N} \to z \in X$. Assume $z \in \mathbb{N}$. Substituting z for the bound variable x in (19), we have $z \preceq z \to z \in X$. By Lemma 14.7, we have $z \preceq z$. Hence $z \in X$ as desired. That completes the proof of the lemma.

Theorem 14.16. *Suppose* $\mathbb{N} \in \mathsf{FINITE}$ *and* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *and* $\mathbf{k} \neq \mathbf{n}$ *and* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \in \mathbb{N}$. *Then for* $x, y \in \mathbb{N}$ *we have*

$$x \prec y \ \vee \ x = y \ \vee \ y \prec x.$$

Proof. We will prove by finite induction on x that

$$\forall y \in \mathbb{N} \, (x \preceq y \ \vee \ \ y \preceq x) \tag{21}$$

Since $\mathbb{N}$ is finite, it has decidable equality, so $x \preceq y \leftrightarrow x \prec y \ \vee \ x = y$. Therefore (21) is equivalent to the lemma as stated.

The formula is stratified, giving x and y both index 0, since $\preceq$ is a definable relation. Hence induction is legal.

Base case. By Lemma 14.8, we have $\mathbf{0} \preceq y$. That completes the base case.

Induction step. The induction hypothesis is (21). Let y be given. We must prove

$$\mathsf{S}x \preceq y \ \vee \ y \preceq \mathsf{S}x \tag{22}$$

Since we are using finite induction on x (Lemma 14.15), we may assume

$$x \neq \mathbf{n} \tag{23}$$

By (21) we have $x \preceq y \ \vee \ y \preceq x$. We argue by cases accordingly.

Case 1: $x \preceq y$. By decidable equality and the definition of $\prec$, we have $x \prec y$ or $x = y$. If $x \prec y$, then $\mathsf{S}x \preceq y$, by Lemma 14.13. If $x = y$ then $y \preceq \mathsf{S}x$, by Lemma 14.10. That completes Case 1.

Case 2: $y \preceq x$. Then $y \preceq \mathsf{S}x$, by Lemma 14.10 and (23). That completes Case 2. That completes the proof of the lemma.

Lemma 14.17. *Suppose* $\mathbb{N} \in \mathsf{FINITE}$ *and* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *and* $\mathbf{k} \neq \mathbf{n}$ *and* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \in \mathbb{N}$. *Then for* $x, y \in \mathbb{N}$ *we have*

$$y \neq \mathbf{n} \to \mathsf{S}y \prec x \to y \preceq x.$$

Proof. By finite induction on x.

Base case. We must prove $\mathsf{S}y \prec \mathbf{0} \to y \preceq \mathbf{0}$. But $\mathsf{S}y \prec \mathbf{0}$ can never hold, by Lemma 14.9. That completes the base case.

Induction step. Suppose $\mathsf{S}y \prec \mathsf{S}x$ and $x \neq \mathbf{n}$. We have to prove $y \preceq \mathsf{S}x$. We have

$\mathsf{S}y \preceq \mathsf{S}x \;\wedge\; \mathsf{S}y \neq \mathsf{S}x$	by definition of $\prec$
$y \neq \mathbf{n}$	by hypothesis
$\mathsf{S}y \preceq x$	by Lemma 14.10, since $y \neq \mathbf{n}$
$y \preceq \mathsf{S}y$	by Lemma 14.10
$y \preceq x$	by Lemma 14.6 and the preceding two lines
$y \preceq \mathsf{S}x$	by Lemma 14.10

That completes the induction step. That completes the proof of the lemma.

Lemma 14.18. *Suppose* $\mathbb{N} \in \mathsf{FINITE}$ *and* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *and* $\mathbf{k} \neq \mathbf{n}$ *and* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \in \mathbb{N}$. *Then for* $x \in \mathbb{N}$ *we have*

$$x \neq \mathbf{n} \to \neg\,(\mathsf{S}x \preceq x).$$

Proof. Suppose $x \in \mathbb{N}$ and $x \neq \mathbf{n}$ and

$$\mathsf{S}x \preceq x. \tag{24}$$

We must derive a contradiction. Define

$$Z := \{u \in \mathbb{N} : \neg\,(\mathsf{S}x \preceq u \;\wedge\; u \preceq x)\}.$$

The formula is stratified, giving x and u index 0, so the definition can be given in INF.

I say that $\mathbb{N} \subseteq Z$. By the definition of $\subseteq$, that is equivalent to

$$\forall u \in \mathbb{N}\,(u \in Z) \tag{25}$$

We will prove that by finite induction.

Base case, $\mathbf{0} \in Z$. We have to prove $\neg\,(\mathsf{S}x \preceq \mathbf{0} \;\wedge\; \mathbf{0} \preceq x)$. It suffices to prove $\neg\,(\mathsf{S}x \preceq \mathbf{0})$. Suppose $\mathsf{S}x \preceq \mathbf{0}$. Then by Lemma 14.8, $\mathsf{S}x = \mathbf{0}$. But that contradicts Theorem 3.8. That completes the base case.

Induction step. We have to prove that

$$u \in Z \to u \neq \mathbf{n} \to \mathsf{S}u \in Z.$$

Using the definition of Z, that becomes

$$\neg\,(\mathsf{S}x \preceq u \;\wedge\; u \preceq x) \to u \neq \mathbf{n} \to \neg\,(\mathsf{S}x \preceq \mathsf{S}u \;\wedge\; \mathsf{S}u \preceq x).$$

It suffices to prove, assuming $u \neq \mathbf{n}$, that

$$\mathsf{S}x \preceq \mathsf{S}u \;\wedge\; \mathsf{S}u \preceq x \to \mathsf{S}x \preceq u \;\wedge\; u \preceq x.$$

Suppose

$$u \neq \mathbf{n} \tag{26}$$

$$\mathsf{S}x \preceq \mathsf{S}u \ \wedge \ \mathsf{S}u \preceq x. \tag{27}$$

We must prove

$$\mathsf{S}x \preceq u \ \wedge \ u \preceq x \tag{28}$$

We have

$$\mathsf{S}x \preceq u \ \vee \ \mathsf{S}x = \mathsf{S}u \qquad \text{by Lemma 14.10 and (27) and (26)}$$

We argue by cases accordingly to prove (28).

Case 1, $\mathsf{S}x \preceq u$. That is already the first half of (28); it remains to prove $u \preceq x$. We have

$$\begin{array}{rl} \mathsf{S}u \preceq x & \text{by (27)} \\ u \preceq u & \text{by Lemma 14.7} \\ u \preceq \mathsf{S}u & \text{by Lemma 14.10, since } u \neq \mathbf{n} \\ u \preceq x & \text{by Lemma 14.6} \end{array}$$

That completes Case 1.

Case 2, $\mathsf{S}x = \mathsf{S}u$. Since $\mathbb{N}$ has decidable equality, we have $x = u \ \vee \ x \neq u$. We argue by cases.

Case 2a, $x = u$. Then (28) becomes $\mathsf{S}x \preceq x \ \wedge \ x \preceq x$, which follows from (24) and Lemma 14.7.

Case 2b. $x \neq u$. Then $\mathsf{S}x = \mathsf{S}u$ is a double successor. Then

$$\begin{array}{rl} \{x, u\} = \{\mathbf{k}, \mathbf{n}\} & \text{by Corollary 13.4} \\ x = \mathbf{n} \ \wedge \ u = \mathbf{k} & \text{since } u \neq \mathbf{n} \text{ by (26)} \\ x \neq \mathbf{n} & \text{by hypothesis} \end{array}$$

The last two lines are contradictory. That contradiction completes the proof of (28). That completes the proof that $\mathbb{N} \subseteq Z$.

Therefore $x \in Z$. But by hypothesis we have $\mathsf{S}x \preceq x$, and by Lemma 14.7 we have $x \preceq x$. Hence $x \notin Z$. That contradiction completes the proof of the lemma.

Lemma 14.19. *Suppose* $\mathbb{N} \in \mathsf{FINITE}$ *and* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *and* $\mathbf{k} \neq \mathbf{n}$ *and* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \in \mathbb{N}$. *Let* $x \in \mathbb{N}$ *with* $x \neq \mathbf{0}$. *Then there exists an* $r \in \mathbb{N}$ *with* $\mathsf{S}r = x$ *and* $r \neq \mathbf{n}$.

Proof. Let $x \in \mathbb{N}$ be nonzero. By Lemma 3.9, there exists $u \in \mathbb{N}$ with $\mathsf{S}u = x$. Since $\mathbb{N}$ is finite, it has decidable equality, so $u = \mathbf{n} \ \vee \ u \neq \mathbf{n}$. If $u \neq \mathbf{n}$, we may take $r = u$, and then we are done. If $u = \mathbf{n}$, then $x = \mathsf{S}\mathbf{n} = \mathsf{S}\mathbf{k}$. Since $\mathbf{k} \neq \mathbf{n}$ we may take $r = \mathbf{k}$. That completes the proof of the lemma.

Theorem 14.20. *Suppose* $\mathbb{N} \in \mathsf{FINITE}$ *and* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *and* $\mathbf{k} \neq \mathbf{n}$ *and* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \in \mathbb{N}$. *Then for* $x, y \in \mathbb{N}$ *we have*

$$x \preceq y \to y \preceq x \to x = y.$$

Proof. Since $\mathbb{N}$ is finite, it has decidable equality. Therefore the lemma as stated is equivalent to

$$x \neq y \to \neg(x \preceq y \ \wedge \ y \preceq x).$$

That formula is stratified, since $\preceq$ and $\prec$ are definable relations. We will prove it by finite induction on y.

Base case, $x \neq \mathbf{0} \rightarrow \neg(x \preceq \mathbf{0} \wedge \mathbf{0} \preceq x)$. is immediate from Lemma 14.8.

Induction step. Suppose $y \neq \mathbf{n}$ and $x \neq \mathsf{S}y$. We must prove

$$\neg(x \preceq \mathsf{S}y \ \wedge\ \mathsf{S}y \preceq x). \tag{29}$$

To prove that, we must derive a contradiction from

$$x \preceq \mathsf{S}y \tag{30}$$

$$\mathsf{S}y \preceq x \tag{31}$$

We have

(32)	$x \preceq y$	by Lemma 14.10 and (30) and $y \neq \mathbf{n}$ and $x \neq \mathsf{S}y$
	$\mathsf{S}y \prec x$	by (31) and $x \neq \mathsf{S}y$ and the definition of $\prec$
	$x \neq y$	by Lemma 14.18 and (31)
(33)	$y \preceq x$	by Lemma 14.17
	$\neg(x \preceq y \ \wedge\ y \preceq x)$	by (33) and the induction hypothesis

But that is contradicted by (32) together with (33). That completes the induction step. That completes the proof of the lemma.

Theorem 14.21. *Suppose* $\mathbb{N} \in \mathsf{FINITE}$ *and* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *and* $\mathbf{k} \neq \mathbf{n}$ *and* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \in \mathbb{N}$. *Then for* $x, y \in \mathbb{N}$ *we have*

$$\neg(x \prec y \ \wedge\ y \prec x).$$

Proof. Suppose $x \prec y$ and $y \prec x$. Then we have

$x \preceq y$	by definition of $\prec$
$y \preceq x$	by definition of $\prec$
$x = y$	by Theorem 14.20
$x \prec x$	since $x \prec y$ and $x = y$
$x \neq x$	by definition of $\prec$

That contradiction completes the proof of the theorem.

Lemma 14.22. *Suppose* $\mathbb{N} \in \mathsf{FINITE}$ *and* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *and* $\mathbf{k} \neq \mathbf{n}$ *and* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \in \mathbb{N}$. *Let* $x \in \mathbb{N}$. *Then* $\neg(\mathbf{n} \prec x)$.

Proof. Suppose $x \in \mathbb{N}$. Then

$x \preceq n$	by Lemma 14.14
$\mathbf{n} \prec x$	assumption, for proof by contradiction
$\mathbf{n} \preceq x \ \wedge\ n \neq x$	by definition of $\prec$
$x = \mathbf{n}$	by Theorem 14.21

That contradiction completes the proof of the lemma.

Lemma 14.23. *Suppose* $\mathbb{N} \in \mathsf{FINITE}$ *and* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *and* $\mathbf{k} \neq \mathbf{n}$ *and* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \in \mathbb{N}$. *Let* X *be a finite nonempty subset of* $\mathbb{N}$. *Then* X *has a* $\preceq$*-least element. More formally,*

$$\forall X \in \mathsf{FINITE}(X \subseteq \mathbb{N} \wedge X \neq \Lambda \rightarrow \exists p \in X\, \forall q \in X\, (p \preceq q)).$$

Proof. The formula to be proved is stratified, giving p and q both index 0 and X index 1. Therefore we can proceed by induction on finite sets X. Because of the hypothesis that $X \neq \Lambda$, the base case is immediate. For the induction step, suppose $X = Y \cup \{b\}$ with $b \notin Y$ and Y a finite set, and $X \subseteq \mathbb{N}$. Then also $Y \subseteq \mathbb{N}$. By Lemma 3.4 of [1], Y is empty or inhabited. If $Y = \Lambda$, then b is the only element of X, and hence the least element of X. So we may assume Y is inhabited. Then, by the induction hypothesis, Y has a $\preceq$-least element r. By Theorem 14.16, we have $r \preceq b \ \vee \ b \preceq r$. We argue by cases.

Case 1: $r \preceq b$. Then r is the desired $\preceq$-least member of X.

Case 2: $b \preceq r$. Then b is the desired $\preceq$-least member of X, by Lemma 8.9. That completes the proof of the lemma.

Lemma 14.24 (Transitivity of $\prec$)**.** *Suppose* $\mathbb{N} \in \mathsf{FINITE}$ *and* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *and* $\mathbf{k} \neq \mathbf{n}$ *and* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \in \mathbb{N}$*. Then for* $x, y, z \in \mathbb{N}$ *we have*

$$x \prec y \to y \prec z \to x \prec z.$$

Proof. Suppose $x \prec y$ and $y \prec z$. Then

$$\begin{array}{rl}
x \preceq y & \text{by the definition of } \prec \\
y \preceq z & \text{by the definition of } \prec \\
x \preceq z & \text{by Lemma 14.6} \\
x = z \to z \preceq y & \text{since } x \preceq y \\
x = z \to y = z & \text{by Theorem 14.20} \\
y \neq z & \text{by the definition of } y \prec z \\
x \neq z & \text{by the preceding two lines} \\
x \prec z & \text{by the definition of } \prec
\end{array}$$

That completes the proof of the lemma.

Lemma 14.25. *Suppose* $\mathbb{N} \in \mathsf{FINITE}$ *and* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *and* $\mathbf{k} \neq \mathbf{n}$ *and* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \in \mathbb{N}$*. Let* $x, y \in \mathbb{N}$ *with* $x \neq \mathbf{n}$*. Then* $\mathsf{S}x \preceq \mathsf{S}y \to x \preceq y$*.*

Proof. Assume all the hypotheses of the lemma, as well as $\mathsf{S}x \preceq \mathsf{S}y$. We must prove $x \preceq y$. Since $\mathbb{N}$ is finite, it has decidable equality. Therefore $y = \mathbf{n} \ \vee \ y \neq \mathbf{n}$. If $y = n$ then $x \preceq y$ by Lemma 14.14, and we are done. Therefore we may assume $y \neq \mathbf{n}$.

We have

$$\begin{array}{rl}
x \preceq \mathsf{S}x & \text{by Lemma 14.11} \\
x \neq \mathsf{S}x & \text{by Lemma 12.3} \\
\mathsf{S}x \preceq \mathsf{S}y & \text{by hypothesis} \\
x \preceq \mathsf{S}y & \text{by Lemma 14.6} \\
x \preceq \mathsf{S}y \leftrightarrow x \preceq y \ \vee x = \mathsf{S}y & \text{by Lemma 14.10, since } y \neq \mathbf{n} \\
x \preceq y \ \vee x = \mathsf{S}y & \text{by the preceding two lines}
\end{array}$$

If $x \preceq y$ we are finished; so we may assume $x = \mathsf{S}y$. Then $\mathsf{S}x \preceq \mathsf{S}y$ becomes $\mathsf{S}x \preceq x$. Then

$$\begin{array}{ll}
x = \mathsf{S}x & \text{by Theorem 14.20, since } x \preceq \mathsf{S}x \preceq x \\
x \neq \mathsf{S}x & \text{by Lemma 12.3}
\end{array}$$

That contradiction completes the proof of the lemma.

15. Multiplication of Church numbers

In this section we define multiplication $x \otimes y$ of Church numbers in such a way that it satisfies the "defining" laws $x \otimes \mathbf{0} = \mathbf{0}$ and $x \otimes \mathsf{S}y = x \otimes y \oplus x$. This requires knowing that either successor is one-to-on on $\mathbb{N}$, or that there is a double successor $\mathsf{S}\mathbf{n} = \mathsf{S}\mathbf{k}$ with $\mathbf{k} \neq \mathbf{n}$. Then the further laws of multiplication can be developed from those two, plus the decidability of equality on $\mathbb{N}$. Hence, all the results of this section will be valid when there is a double successor, and we use them later to show that $\mathbb{N}$ cannot be finite. But then, we still need multiplication to interpret HA, so we need these results also in the case when successor is one-to-one.

Lemma 15.1. *Multiplication $x \otimes y$ on $\mathbb{N} \times \mathbb{N}$ can be defined (as a function of two variables) in INF and satisfies the following laws for all $x, y \in \mathbb{N}$:*

(i) $x \otimes \mathbf{0} = \mathbf{0}$

(ii) $x \otimes \mathsf{S}y = x \otimes y \oplus x$.

Remark. The lemma does not assume that $\mathbb{N}$ is finite or that there is a double successor, or that there is no double successor. To prove it we have to give an "agnostic" definition of multiplication, that works without any assumption of that sort.

Proof. We define multiplication as the intersection of all sets Z of ordered triples $\langle x, y, z\rangle$ satisfying these conditions:

$$\forall y \in \mathbb{N}\,(\langle \mathbf{0}, y, \mathbf{0}\rangle \in Z)$$
$$\forall y \in \mathbb{N}\,(\langle x, y, z\rangle \in Z \wedge \neg\exists u\,(u \in \mathbb{N} \;\wedge\; u < y \;\wedge\; \mathsf{S}y = \mathsf{S}u) \to \langle x, \mathsf{S}y, z \oplus x\rangle \in Z)$$

These formulas are stratified, giving x, y, z index 0 and Z index 5, so the definition is legal in INF, and defines a relation, which we write $x \otimes y = z$. It remains to prove that this relation is a function. We will prove by induction on y that for each x there exists a unique z such that $x \otimes y = z$.

Base case: Existence: $x \otimes \mathbf{0} = \mathbf{0}$ by the first condition. Uniqueness: $x \otimes \mathbf{0} = z$ is only possibly by the first condition, by Theorem 3.8. That completes the base case.

Induction step: Existence: By the induction hypothesis, there exists z such that $x \otimes y = z$. Then by the second condition, $x \otimes \mathsf{S}y = z \oplus x$.

Uniqueness. Suppose $x \otimes \mathsf{S}y = z$ and $x \otimes \mathsf{S}y = w$. Then by the second condition, $z = x \otimes u \oplus x$ and $w = x \otimes v \oplus x$, where $\mathsf{S}u = \mathsf{S}v = \mathsf{S}y$. Then $\neg\,(u < v)$ and $\neg\,(v < u)$, by the second condition. Then by Lemma 8.10 we have $u = v$. Hence $z = x \otimes v \oplus x = x \otimes u \oplus x = w$ as desired. That completes the induction step. That completes the proof of the lemma.

Lemma 15.2. $\forall x, y \in \mathbb{N}\,(x \otimes y \in \mathbb{N})$.

Proof. The formula is stratified, so we can prove it by induction on y.

Base case. $x \otimes \mathbf{0} = \mathbf{0}$ by Lemma 15.1. $\mathbf{0} \in \mathbb{N}$ by Lemma 2.18. That completes the base case.

Induction step. Suppose

$$\forall x\,(x \otimes y \in \mathbb{N}) \tag{34}$$

We have to prove

$$\mathsf{S}y \in \mathbb{N} \to \forall x \in \mathbb{N}\, (x \otimes \mathsf{S}y \in \mathbb{N})$$

Suppose $y, x \in \mathbb{N}$. We have

$$\begin{array}{rl} x \otimes \mathsf{S}y = x \otimes y \oplus x & \text{By Lemma 15.1} \\ x \otimes y \in \mathbb{N} & \text{by (34)} \\ \mathsf{S}y \in & \text{by Lemma 2.19} \\ x \otimes y \oplus x \in \mathbb{N} & \text{by Lemma 7.3} \\ x \otimes \mathsf{S}y \in \mathbb{N} & \text{by the preceding lines} \end{array}$$

That completes the induction step. That completes the proof of the lemma.

Lemma 15.3. *For $y \in \mathbb{N}$ we have*

$$\mathbf{0} \otimes y = \mathbf{0}$$

Proof. By Lemma 15.1, multiplication is well-defined and satisfies the laws in Lemma 15.1. The formula is stratified, so we may use induction on y.

Base case, $\mathbf{0} \otimes \mathbf{0} = \mathbf{0}$ by Lemma 15.1.

Induction step,

$$\begin{array}{rl} \mathbf{0} \otimes \mathsf{S}y = \mathbf{0} \otimes y \oplus \mathbf{0} & \text{by Lemma 15.1} \\ = \mathbf{0} \otimes y & \text{since } z \oplus \mathbf{0} = z \\ = \mathbf{0} & \text{by the induction hypthesis} \end{array}$$

That completes the induction step. That completes the proof of the lemma.

Lemma 15.4. *For $x, y \in \mathbb{N}$ we have*

$$\mathsf{S}x \otimes y = x \otimes y \oplus y.$$

Proof. By Lemma 15.1, multiplication is well-defined and satisfies the laws in Lemma 15.1. The formula is stratified, so we may use induction on y.

Base case:

$$\begin{array}{rl} \mathsf{S}x \otimes \mathbf{0} = \mathbf{0} & \text{by Lemma 15.1} \\ \mathbf{0} = x \otimes \mathbf{0} & \text{by Lemma 15.1} \\ \mathbf{0} = x \otimes \mathbf{0} \oplus \mathbf{0} & \text{by Lemma 4.4} \end{array}$$

That completes the base case.

Induction step: Assume $\mathsf{S}x \otimes y = x \otimes y \oplus y$. We must prove

$$\mathsf{S}x \otimes \mathsf{S}y = x \otimes \mathsf{S}y \oplus \mathsf{S}y.$$

We have

$$\begin{array}{rcll} \mathsf{S}x \otimes \mathsf{S}y & = & \mathsf{S}x \otimes y \oplus \mathsf{S}x & \text{by definition of multiplication} \\ & = & x \otimes y \oplus y \oplus \mathsf{S}x & \text{by the induction hypothesis} \\ & = & x \otimes y \oplus (y \oplus \mathsf{S}x) & \text{by Lemma 7.4} \\ & = & x \otimes y \oplus (\mathsf{S}y \oplus x) & \text{by Lemma 7.2} \\ & = & x \otimes y \oplus (x \oplus \mathsf{S}y) & \text{by Lemma 7.5} \\ & = & x \otimes y \oplus x \oplus \mathsf{S}y & \text{by Lemma 7.4} \\ & = & x \otimes \mathsf{S}y \oplus \mathsf{S}y & \text{by Lemma 15.1} \end{array}$$

That completes the induction step. That completes the proof of the lemma.

Lemma 15.5. *For $x, y, z \in \mathbb{N}$ we have*

$$x \otimes (y \oplus z) \quad = \quad x \otimes y \oplus x \otimes z$$

Proof. By induction on x.

Base case.

$$\begin{array}{rl} y \oplus z \in \mathbb{N} & \text{by Lemma 7.3} \\ \mathbf{0} \otimes (y \oplus z) = \mathbf{0} & \text{by Lemma 15.3} \\ \mathbf{0} \otimes y = \mathbf{0} & \text{by Lemma 15.3} \\ \mathbf{0} \otimes z = \mathbf{0} & \text{by Lemma 15.3} \\ \mathbf{0} \otimes (y \oplus z) = \mathbf{0} \otimes y \oplus \mathbf{0} \otimes z & \text{since } \mathbf{0} \oplus \mathbf{0} = \mathbf{0} \end{array}$$

That completes the base case.

Induction step.

$$\begin{array}{rl} y \oplus z \in \mathbb{N} & \text{by Lemma 7.3} \\ x \otimes y \in \mathbb{N} & \text{by Lemma 15.2} \\ x \otimes z \in \mathbb{N} & \text{by Lemma 15.2} \\ \mathsf{S}x \otimes (y \oplus z) = x \otimes (y \oplus z) \oplus (y \oplus z) & \text{by Lemma 15.4} \\ = x \otimes y \oplus x \otimes z \oplus y \oplus z & \text{by the induction hypothesis} \\ = x \otimes y \oplus (x \otimes z \oplus y) \oplus z & \text{by Lemma 7.4} \\ = x \otimes y \oplus (y \oplus x \otimes z) \oplus z & \text{by Lemma 7.5} \\ = (x \otimes y \oplus y) \oplus (x \otimes z \oplus z) & \text{by Lemma 7.4} \\ = \mathsf{S}x \otimes y \oplus \mathsf{S}x \otimes z & \text{by Lemma 15.4} \end{array}$$

That completes the proof of the lemma.

Lemma 15.6. *Suppose there is a double successor $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ with $\mathbf{k} \in \mathsf{STEM}$ and $\mathbf{k} \neq \mathbf{n}$ and $\mathbf{n} \in \mathbb{N}$. Then for $x, y \in \mathbb{N}$ we have*

$$(x \oplus y) \otimes z \quad = \quad x \otimes z \oplus y \otimes z$$

Proof. By induction on z. The base case is immediate. For the induction step we have

$$\begin{array}{rcll} (x \oplus y) \otimes \mathsf{S}z & = & (x \oplus y) \otimes z \oplus (x \oplus y) & \text{by Lemma 15.1} \\ & = & x \otimes z \oplus y \otimes z \oplus (x \oplus y) & \text{by the induction hypothesis} \\ & = & (x \otimes z \oplus x) \oplus (y \otimes z \oplus y) & \text{by associativity and commutativity of } \oplus \\ & = & x \otimes \mathsf{S}z \oplus y \otimes \mathsf{S}z & \text{by Lemma 15.1} \end{array}$$

That completes the proof of the lemma.

Lemma 15.7 (Church multiplication associative)**.** *For $x, y, z \in \mathbb{N}$ we have*

$$x \otimes (y \otimes z) \quad = \quad (x \otimes y) \otimes z$$

Proof. By induction on y.

Base case:

$$\begin{aligned} x \otimes (\mathbf{0} \otimes z) &= x \otimes \mathbf{0} && \text{by Lemma 15.3} \\ &= \mathbf{0} && \text{by Lemma 15.1} \\ &= (x \otimes \mathbf{0}) \otimes \mathbf{0} && \text{by Lemma 15.1} \end{aligned}$$

That completes the base case.

Induction step:

$$\begin{aligned} x \otimes (\mathsf{S}y \otimes z) &= x \otimes (y \otimes z \oplus z) && \text{by Lemma 15.4} \\ &= x \otimes (y \otimes z) \oplus x \otimes z && \text{by Lemma 15.5} \\ &= (x \otimes y) \otimes z) \oplus x \otimes z && \text{by the induction hypothesis} \\ &= (x \otimes y \oplus x) \otimes z && \text{by Lemma 15.6} \\ &= (x \otimes \mathsf{S}y) \otimes z && \text{by Lemma 15.1} \end{aligned}$$

Lemma 15.8 (Church multiplication commutative)**.** *For* $x, y \in \mathbb{N}$ *we have*

$$x \otimes y \quad = \quad y \otimes x$$

Proof. By induction on y, which is legal since the formula is stratified.

Base case. We have

$$\begin{aligned} x \otimes \mathbf{0} = \mathbf{0} & && \text{by Lemma 15.1} \\ = \mathbf{0} \otimes x & && \text{by Lemma 15.3} \end{aligned}$$

That completes the base case.

Induction step. We have

$$\begin{aligned} \mathsf{S}x \otimes y &= x \otimes y \oplus y && \text{by Lemma 15.4} \\ &= y \otimes x \oplus y && \text{by the induction hypothesis} \\ &= y \otimes \mathsf{S}x. && \text{by Lemma 15.1} \end{aligned}$$

That completes the induction step. That completes the proof of the lemma.

16. Successor and addition on the loop

In this section we consider the map f on the loop, defined by restricting Church successor to the loop. We will show that f is a permutation of the loop; by the Annihilation Theorem then $\mathbf{m}f$ is the identity on the loop. We then consider solutions x of the equation $\mathbf{n} + x = \mathbf{n}$. There is a solution, and we show there is a $\preceq$-least solution $\mathbf{m}$. If $\mathbf{m}$ were the order of f, we could reach a contradiction, proving that $\mathbb{N}$ is not finite. We assumed the Church counting axiom to reach that conclusion; but in the last half of this section we prove, without the counting axiom, that the order of successor at least exists. That existence is not subsequently used, but we include it anyway.

Lemma 16.1. *Suppose* $\mathbb{N}$ *is finite and* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *and* $\mathbf{k} \neq \mathbf{n}$ *and* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \in \mathbb{N}$*. Then every element of* $\mathcal{L}(\mathbf{n})$ *has the form* $\mathbf{n} \oplus x$ *for some* $x \in \mathbb{N}$*.*

Proof. Let

$$X := \{\mathbf{n} \oplus x : x \in \mathbb{N}\}.$$

The formula is stratified, so the definition is legal. Then

$$\begin{array}{rl} \mathbf{n} \in X & \text{since } \mathbf{n} = \mathbf{n} \oplus \mathbf{0}\text{, by Lemma 4.4} \\ z \in X \to \mathsf{S}z \in X & \text{since } \mathsf{S}(n \oplus x) = \mathbf{n} \oplus \mathsf{S}x\text{, by Lemma 4.5} \\ \mathcal{L}(\mathbf{n}) \subseteq X & \text{by the definition of } \mathcal{L}(\mathbf{n}) \end{array}$$

That completes the proof of the lemma.

Lemma 16.2. *Suppose* $\mathbb{N} \in \mathsf{FINITE}$ *and* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *and* $\mathbf{k} \neq \mathbf{n}$ *and* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \in \mathbb{N}$*. Then there exists* $\mathbf{m} \in \mathbb{N}$ *such that* $\mathbf{n} = \mathbf{k} \oplus \mathbf{m}$*.*

Proof.

$$\begin{array}{rl} \mathbf{n} \in \mathcal{L}(\mathbf{n}) & \text{by Lemma 11.2} \\ \mathbf{n} = \mathsf{S}p & \text{for some } p \in \mathcal{L}(\mathbf{n}) \text{ by Theorem 11.8} \\ p = \mathbf{n} \oplus u & \text{for some } u \in \mathbb{N}\text{, by Lemma 16.1} \\ \mathsf{S}p = \mathsf{S}(n \oplus u) & \text{by the preceding line} \\ \mathbf{n} = \mathsf{S}(n \oplus u) & \text{since } \mathsf{S}p = \mathbf{n} \\ \mathbf{n} = \mathbf{n} \oplus \mathsf{S}u & \text{by Lemma 4.5} \\ \mathbf{n} = \mathsf{S}\mathbf{n} \oplus u & \text{by Lemma 7.2} \\ \mathbf{n} = \mathsf{S}\mathbf{k} \oplus u & \text{since } \mathsf{S}\mathbf{n} = \mathsf{S}\mathbf{k} \\ \mathbf{n} = \mathbf{k} \oplus \mathsf{S}u & \text{by Lemma 7.2} \end{array}$$

Setting $\mathbf{m} := \mathsf{S}u$ we have $\mathbf{n} = \mathbf{k} \oplus \mathbf{m}$. That completes the proof of the lemma.

Lemma 16.3. *Suppose* $\mathbb{N} \in \mathsf{FINITE}$ *and* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *and* $\mathbf{k} \neq \mathbf{n}$ *and* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \in \mathbb{N}$*. Then there exists* $\mathbf{m} \in \mathbb{N}$ *such that* $\mathbf{n} = \mathbf{k} \oplus \mathbf{m}$ *and* $\mathbf{m}$ *is the* $\preceq$*-least number with that property. Explicitly,*

$$\forall p \in \mathbb{N}\, (\mathbf{n} = \mathbf{k} \oplus p \to \mathbf{m} \preceq p).$$

Proof. Define

$$X = \{\ x : x \in \mathbb{N}\ \wedge\ \mathbf{n} = \mathbf{k} \oplus x\ \}.$$

By Lemma 16.2, X is inhabited. Since $\mathbb{N}$ is finite, it has decidable equality, by Lemma 3.3 of [1]. Therefore X is a separable subset of $\mathbb{N}$. By Lemma 3.19, $X \in \mathsf{FINITE}$. By Lemma 14.23, X has a $\preceq$-least element. That completes the proof of the lemma.

Lemma 16.4. *Suppose* $\mathbb{N} \in \mathsf{FINITE}$ *and* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *and* $\mathbf{k} \neq \mathbf{n}$ *and* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \in \mathbb{N}$*. Then* $x\mathsf{S} : \mathcal{L}(\mathbf{n}) \to \mathcal{L}(\mathbf{n})$*. That is,*

$$\forall x \in \mathbb{N}\, \forall y\, (y \in \mathcal{L}(\mathbf{n}) \to (x\mathsf{S}y \in \mathcal{L}(\mathbf{n})).$$

Proof. To stratify the formula, we give y index 0 and x index 6. Then $x\mathsf{S}y$ gets index 0, so the two occurrences of $\mathcal{L}(\mathbf{n})$ could get the same index, but since $\mathcal{L}(\mathbf{n})$ is a parameter we do not even have to assign $\mathcal{L}(\mathbf{n})$ an index. Since the formula is stratified, we may prove it by finite induction on x.

Base case, $x = \mathbf{0}$. Suppose $y \in \mathcal{L}(\mathbf{n})$. Then

$$\begin{array}{rl} y \in \mathbb{N} & \text{by Lemma 11.3} \\ \mathbf{0}\mathsf{S}y = y & \text{by Lemma 4.4} \\ \mathbf{0}\mathsf{S}y \in \mathcal{L}(\mathbf{n}) & \text{by the preceding two lines} \end{array}$$

That completes the base case.

Induction step. Suppose $x \neq \mathbf{n}$ and $x \in \mathbb{N}$ and $y \in \mathcal{L}(\mathbf{n})$. We must prove $(\mathsf{S}x)\mathsf{S}y \in \mathcal{L}(\mathbf{n})$. We have

$$\begin{array}{rl} x\mathsf{S}y \in \mathcal{L}(\mathbf{n}) & \text{by the induction hypothesis} \\ (\mathsf{S}x)\mathsf{S}y = \mathsf{S}(x\mathsf{S}y) & \text{by Theorem 3.6} \\ \mathsf{S}(x\mathsf{S}y) \in \mathcal{L}(\mathbf{n}) & \text{by Lemma 11.2} \\ (\mathsf{S}x)\mathsf{S}y \in \mathcal{L}(\mathbf{n}) & \text{by the preceding two lines} \end{array}$$

That completes the induction step. That completes the proof of the lemma.

Lemma 16.5 (Loop closed under addition)**.** *Suppose* $\mathbb{N}$ *is finite and* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *and* $\mathbf{k} \neq \mathbf{n}$ *and* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \in \mathbb{N}$. *Then*

$$x \in \mathcal{L}(\mathbf{n}) \to y \in \mathbb{N} \to x \oplus y \in \mathcal{L}(\mathbf{n}).$$

Proof. The displayed formula is stratified, giving x and $\mathbf{n}$ index 0, since $L(\mathbf{n})$ and $\mathbb{N}$ are parameters. So we may prove it by induction on y.

Base case, $y = \mathbf{0}$. Then

$$\begin{array}{rl} x \in \mathbb{N} & \text{by Lemma 11.3} \\ x \oplus \mathbf{0} = x & \text{by Lemma 4.4} \\ x \oplus y = x & \text{since } y = \mathbf{0} \\ x \oplus y \in \mathcal{L}(\mathbf{n}) & \text{since } x \in \mathbb{N} \end{array}$$

Induction step. Suppose $x \in \mathcal{L}(\mathbf{n})$ and $\mathsf{S}y \in \mathcal{L}(\mathbf{n})$ and $x \oplus y \in \mathcal{L}(\mathbf{n})$. We must prove $x \oplus \mathsf{S}y \in \mathcal{L}(\mathbf{n})$. We have

$$\begin{array}{rl} x \oplus y \in \mathcal{L}(\mathbf{n}) & \text{by the induction hypothesis} \\ \mathsf{S}(x \oplus y) \in \mathcal{L}(\mathbf{n}) & \text{by Lemma 11.2} \\ x \oplus \mathsf{S}y \in \mathcal{L}(\mathbf{n}) & \text{by Lemma 4.5} \end{array}$$

That completes the induction step. That completes the proof of the lemma.

Lemma 16.6. *Suppose* $\mathbb{N}$ *is finite and* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *and* $\mathbf{k} \neq \mathbf{n}$ *and* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \in \mathbb{N}$. *Suppose* $\mathbf{k} \oplus \mathbf{m} = \mathbf{n}$. *Then* $\mathbf{n} \oplus \mathbf{m} = \mathbf{n}$.

Proof. We have

$$\begin{array}{rl} \mathbf{k} \oplus \mathbf{m} = \mathbf{n} & \text{by hypothesis} \\ \mathsf{S}(\mathbf{k} \oplus \mathbf{m}) = \mathsf{S}\mathbf{n} & \text{by the previous line} \\ \mathbf{k} \in \mathbb{N} & \text{by Lemma 10.2} \\ \mathbf{k} \oplus \mathsf{S}\mathbf{m} = \mathsf{S}\mathbf{n} & \text{by Lemma 4.5} \\ \mathsf{S}\mathbf{k} \oplus \mathbf{m} = \mathsf{S}\mathbf{n} & \text{by Lemma 7.2} \\ \mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n} & \text{by hypothesis} \\ \mathsf{S}\mathbf{n} \oplus \mathbf{m} = \mathsf{S}\mathbf{n} & \text{by the preceding two lines} \\ \mathbf{n} \oplus \mathsf{S}\mathbf{m} = \mathsf{S}\mathbf{n} & \text{by Lemma 7.2} \\ \mathsf{S}(n \oplus \mathbf{m}) = \mathsf{S}\mathbf{n} & \text{by Lemma 4.5} \\ \mathbf{n} \oplus \mathbf{m} \in \mathcal{L}(\mathbf{n}) & \text{by Lemma 16.5} \\ \mathbf{n} \oplus \mathbf{m} = \mathbf{n} & \text{by Theorem 13.2} \end{array}$$

That completes the proof of the lemma.

Lemma 16.7. *Suppose* $\mathbb{N} \in \mathsf{FINITE}$ *and* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *and* $\mathbf{k} \neq \mathbf{n}$ *and* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \in \mathbb{N}$. *Then for all* $x \in \mathbb{N}$,

$$x \neq \mathbf{0} \rightarrow \mathbf{n} = \mathbf{n} \oplus x \rightarrow \mathbf{n} = \mathbf{k} \oplus x.$$

Proof. Suppose $\mathbf{n} = \mathbf{n} \oplus x$. Then

$$\begin{array}{rl}
\mathsf{S}\mathbf{n} = \mathsf{S}(\mathbf{n} \oplus x) & \text{since } \mathbf{n} = \mathbf{n} \oplus x \\
\mathsf{S}\mathbf{n} = \mathbf{n} \oplus \mathsf{S}x & \text{by Lemma 4.5} \\
\mathsf{S}\mathbf{n} = \mathsf{S}\mathbf{n} \oplus x & \text{by Lemma 7.2} \\
\mathsf{S}\mathbf{n} = \mathsf{S}\mathbf{k} \oplus x & \text{since } \mathsf{S}\mathbf{n} = \mathsf{S}\mathbf{k} \\
\mathbf{k} \in \mathbb{N} & \text{by Lemma 10.2, since } k \in \mathsf{STEM} \\
\mathsf{S}\mathbf{n} = \mathbf{k} \oplus \mathsf{S}x & \text{by Lemma 7.2} \\
\mathsf{S}\mathbf{n} = \mathsf{S}(\mathbf{k} \oplus x) & \text{by Lemma 4.5} \\
\mathbf{n} \in \mathcal{L}(\mathbf{n}) & \text{by Lemma 11.2} \\
\mathsf{S}\mathbf{n} \in \mathcal{L}(\mathbf{n}) & \text{by Lemma 11.2} \\
\mathsf{S}\mathbf{k} \in \mathcal{L}(\mathbf{n}) & \text{since } \mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n} \\
x \neq \mathbf{0} & \text{by hypothesis} \\
x = \mathsf{S}r & \text{for some } r \in \mathbb{N}, \text{ by Lemma 3.9} \\
\mathbf{k} \oplus x = \mathbf{k} \oplus \mathsf{S}r & \text{since } x = \mathsf{S}r \\
\mathbf{k} \oplus x = \mathsf{S}\mathbf{k} \oplus r & \text{by Lemma 7.2} \\
\mathsf{S}\mathbf{k} \oplus r \in \mathcal{L}(\mathbf{n}) & \text{by Lemma 16.5} \\
\mathbf{k} = \mathbf{n} \oplus x & \text{by Theorem 13.2, since } \mathsf{S}\mathbf{n} = \mathsf{S}(\mathbf{k} \oplus x)
\end{array}$$

That completes the proof of the lemma.

Definition 16.8. *Suppose* $\mathbb{N}$ *is finite and* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *and* $\mathbf{k} \neq \mathbf{n}$ *and* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \in \mathbb{N}$. *Then we define the* **order of successor on the loop** *to be the* $\preceq$*-least Church number* $\mathbf{q}$ *such that* $\mathbf{q}\mathsf{S}$ *is the identity on* $\mathcal{L}(\mathbf{n})$. *That is,*

$$\forall x \in \mathcal{L}(\mathbf{n})\,(\mathbf{q}\mathsf{S}x = x)$$
$$\forall r \in \mathbb{N}\,(r \prec \mathbf{q} \rightarrow \neg\forall x \in \mathcal{L}(\mathbf{n})\,(r\mathsf{S}x = x))$$

For short we call $\mathbf{q}$ *the "order of* $\mathcal{L}(\mathbf{n})$*" or the "order of the loop."*

We shall show below that there actually exists such a number $\mathbf{q}$. That, of course, requires a proof, not just a definition. Of course, assuming the Church counting axiom, it is easy to prove that $\mathbf{m}$ is the order of the loop, but we shall prove without the counting axiom that the order is well-defined.

Lemma 16.9. *Let* $x \in \mathbb{N}$ *and* $y \in \mathbb{N}$. *Then* $x\mathsf{S}y \in \mathbb{N}$.

Proof. The formula is stratified, giving x index 6 and y index 0, with $\mathbb{N}$ as parameter. Therefore we may prove it by induction on x.

Base case. We have

$$\begin{array}{rl}
\mathbf{0}\mathsf{S}y = y & \text{by Lemma 2.13} \\
\mathbf{0}\mathsf{S}y \in \mathbb{N} & \text{since } y \in \mathbb{N}
\end{array}$$

That completes the base case.

Induction step. We have

$$\begin{array}{rl} x\mathsf{S}y \in \mathbb{N} & \text{by the induction hypothesis} \\ x \in \mathsf{FUNC} & \text{by Lemma 2.20} \\ \mathsf{S}(x\mathsf{S}y) \in \mathbb{N} & \text{by Lemma 2.19, since } y \in \mathbb{N} \\ \mathsf{S}x\mathsf{S}y = \mathsf{S}(x\mathsf{S}y) & \text{by Theorem 3.6} \\ \mathsf{S}x\mathsf{S}y \in \mathbb{N} & \text{by the preceding two lines} \end{array}$$

That completes the induction step. That completes the proof of the theorem.

Lemma 16.10. *Let* $t \in \mathbb{N}$ *and* $q \in \mathbb{N}$. *Then*

$$q\mathsf{S}(\mathsf{S}t) = \mathsf{S}(q\mathsf{S}t).$$

Remark. Intuitively, both sides refer to successor applied q plus one times to t.

Proof. We have

$$\begin{array}{rl} \mathbf{0}\mathsf{S}t = t & \text{by Lemmas 2.13} \\ \mathsf{S}(\mathbf{0}\mathsf{S}t) = \mathsf{S}t & \text{by the preceding line} \\ q\mathsf{S}t \in \mathbb{N} & \text{by Lemma 16.9} \\ \mathsf{S}t \in \mathbb{N} & \text{by Lemma 2.19} \\ \mathsf{S}t \in \mathsf{FUNC} & \text{by Lemma 2.20} \\ Rel(\mathsf{S}t) & \text{by Lemma 2.21} \\ \mathsf{S}\mathbf{0}\mathsf{S}t = \mathsf{S}t & \text{by Lemma 2.14} \\ \mathsf{S}t = \mathsf{S}\mathbf{0}\mathsf{S}t & \text{by the preceding line} \\ q\mathsf{S}(\mathsf{S}t) = q\mathsf{S}(\mathsf{S}\mathbf{0}\mathsf{S}t) & \text{by the preceding line} \\ = (q \oplus \mathsf{S}\mathbf{0})\mathsf{S}t & \text{by Lemma 7.6 with } X = \mathbb{N} \text{ and } f = \mathsf{S} \\ = (\mathsf{S}q \oplus \mathbf{0})\mathsf{S}t & \text{by Lemma 7.2} \\ = \mathsf{S}q\mathsf{S}t & \text{by Lemma 4.4} \\ = \mathsf{S}(q\mathsf{S}t) & \text{by Theorem 3.6} \end{array}$$

That completes the proof of the lemma.

Lemma 16.11. *Suppose* $\mathbb{N}$ *is finite and* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *and* $\mathbf{k} \neq \mathbf{n}$ *and* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \in \mathbb{N}$. *Suppose* $q \in \mathbb{N}$ *and* $q \neq \mathbf{0}$ *and* $q\mathsf{S}\mathbf{n} = \mathbf{n}$. *Then* $q\mathsf{S}$ *is the identity on* $\mathcal{L}(\mathbf{n})$.

Proof. Define $X = \{x \in \mathcal{L}(n) : q\mathsf{S}x = x\}$ The formula is stratified, giving x index 0 and q index 6, so the definition is legal. By hypothesis, $\mathbf{n} \in X$. I say that X is closed under successor. Suppose $x \in X$. Then $x \in \mathcal{L}(\mathbf{n})$ and $q\mathsf{S}x = x$.

$$\begin{array}{rl} q\mathsf{S}(\mathsf{S}x) = \mathsf{S}(q\mathsf{S}x) & \text{by Lemma 16.10} \\ q\mathsf{S}(\mathsf{S}x) = \mathsf{S}x & \text{since } q\mathsf{S}x = x \\ \mathsf{S}x \in \mathcal{L}(\mathbf{n}) & \text{by Lemma 11.2} \\ \mathsf{S}x \in X & \text{by definition of } X \end{array}$$

That completes the proof that X is closed under successor. Then by definition of $\mathcal{L}(\mathbf{n})$, we have $\mathcal{L}(\mathbf{n}) \subseteq X$. That completes the proof of the lemma.

Lemma 16.12. *Suppose* $\mathbb{N}$ *is finite and* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *and* $\mathbf{k} \neq \mathbf{n}$ *and* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \in \mathbb{N}$*. Suppose* $q \in \mathbb{N}$ *and* $q \neq \mathbf{0}$ *and* $t \in \mathcal{L}(\mathbf{n})$ *and* $q\mathsf{S}t = t$*. Then* $q\mathsf{S}$ *is the identity on* $\mathcal{L}(\mathbf{n})$*. That is,*

$$\forall x \in \mathcal{L}(\mathbf{n})\,(q\mathsf{S}x = x).$$

Proof. The formula is stratified, giving x and t index 0 and q index 6. We can therefore prove it by "loop induction." That is, we show that the set of t for which the lemma holds contains $\mathbf{n}$ and is closed under successor. That set, explicitly, is

$$Z := \{\ t \in \mathcal{L}(\mathbf{n}) : q\mathsf{S}t = t \to \forall x \in \mathcal{L}(\mathbf{n})\,(q\mathsf{S}x = x)\ \}.$$

The formula defining Z is stratified, giving q index 6 and x and t index 0. $\mathcal{L}(\mathbf{n})$ is a parameter. Therefore Z can be defined in INF.

Z contains $\mathbf{n}$, by Lemma 16.11. It remains to show Z is closed under successor. Suppose $t \in Z$. We must show $\mathsf{S}t \in \mathbb{Z}$. Suppose $q\mathsf{S}(\mathsf{S}t) = \mathsf{S}t$, and let $x \in \mathcal{L}(\mathbf{n})$ be given. We must show $\mathbf{q}\mathsf{S}x = x$. We have

$q\mathsf{S}(\mathsf{S}t) = \mathsf{S}(q\mathsf{S}t)$	by Lemma 16.10
$\mathsf{S}(q\mathsf{S}t) = \mathsf{S}t$	since $q\mathsf{S}(\mathsf{S}t) = \mathsf{S}t$
$q\mathsf{S}t = t$	by Theorem 13.2
$\forall x \in \mathcal{L}(\mathbf{n})\,(qx = x)$	by the induction hypothesis

That completes the induction step. That completes the proof of the lemma.

Lemma 16.13. *Suppose* $\mathbb{N}$ *is finite and* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *and* $\mathbf{k} \neq \mathbf{n}$ *and* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \in \mathbb{N}$*. Let* f *be Church successor restricted to* $\mathcal{L}(\mathbf{n})$*. Then for every* $q \in \mathbb{N}$ *and* $x \in \mathcal{L}(\mathbf{n})$*,*

$$qfx = q\mathsf{S}x.$$

Proof. The displayed formula is stratified, giving x index 0, f index 3, and q index 6. Therefore we can prove it by induction on q.

Base case, $\mathbf{0}fx = x$ and $\mathbf{0}\mathsf{S}x = x$, by Lemma 2.13. Therefore $\mathbf{0}fx = \mathbf{0}\mathsf{S}x$. That completes the base case.

Induction step. We have

$f : \mathcal{L}(\mathbf{n}) \to \mathcal{L}(\mathbf{n})$	by Lemma 11.2
$Rel(f)\ \wedge\ f \in \mathsf{FUNC}$	since f is a subset of the graph of Church successor
$\mathsf{S}qfx = f(qfx)$	by Theorem 3.6
$\mathsf{S}qfx = f(q\mathsf{S}x)$	by the induction hypothesis, $qfx = q\mathsf{S}x$
$\mathsf{S}q\mathsf{S}x) = \mathsf{S}(q\mathsf{S}x)$	by Theorem 3.6
$q\mathsf{S}x \in \mathcal{L}(\mathbf{n})$	by Lemma 16.4
$f(q\mathsf{S}x) = \mathsf{S}(q\mathsf{S}x)$	since f is the restriction of S to $\mathcal{L}(\mathbf{n})$
$\mathsf{S}qfx = \mathsf{S}(q\mathsf{S}x)$	since $\mathsf{S}qfx = f(qfx)$
$\mathsf{S}qfx = \mathsf{S}q\mathsf{S}x$	since $\mathsf{S}q\mathsf{S}x) = \mathsf{S}(q\mathsf{S}x)$

That completes the induction step. That completes the proof of the lemma.

Lemma 16.14. *Suppose* $\mathbb{N}$ *is finite and* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *and* $\mathbf{k} \neq \mathbf{n}$ *and* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \in \mathbb{N}$*. Then the order of successor on the loop exists.*

Proof.

$$\begin{array}{rl} \mathbf{n} = \mathbf{k} \oplus \mathbf{m} & \text{for some } \mathbf{m} \in \mathbb{N}, \text{ by Lemma 16.3} \\ \mathbf{n} = \mathbf{n} \oplus \mathbf{m} & \text{by Lemma 16.6} \\ \mathbf{m}\mathsf{S} \text{ is the identity on } \mathcal{L}(\mathbf{n}) & \text{by the Annihilation Theorem} \\ \mathbf{m}\mathsf{S}\mathbf{n} = \mathbf{n} & \text{by the previous line} \end{array}$$

Define

$$X := \{q \in \mathbb{N} : q\mathsf{S}\mathbf{n} = \mathbf{n}\}.$$

The formula defining X is stratified, giving q index 6 and $\mathbf{n}$ index 0, so X can be defined in INF. Define f to be Church successor restricted to $\mathcal{L}(\mathbf{n})$. Then

$$\begin{array}{rl} f : \mathcal{L}(\mathbf{n}) \to \mathcal{L}(\mathbf{n}) & \text{by Lemma 11.2} \\ f \text{ is an injection} & \text{by Theorem 13.2} \\ \mathbf{m}f \text{ is the identity on } \mathcal{L}(\mathbf{n}) & \text{by the Annihilation Theorem} \\ x \in \mathcal{L}(\mathbf{n}) \to \mathbf{m}fx = \mathbf{m}\mathsf{S}x & \text{by Lemma 16.13} \\ \mathbf{m}\mathsf{S} \text{ is the identity on } \mathcal{L}(\mathbf{n}) & \text{by the preceding two lines} \\ \mathbf{m} \in X & \text{by the definition of } X \\ \mathbb{N} \in \mathsf{DECIDABLE} & \text{by Lemma 3.3 of [1]} \\ X \text{ is a separable subset of } \mathbb{N} & \text{by definition of separable} \\ X \in \mathsf{FINITE} & \text{by Lemma 3.19} \\ X \text{ has a } \preceq\text{-least element} & \text{by Lemma 14.23, since } \mathbf{m} \in X \end{array}$$

Let $\mathbf{q}$ be that element. By Lemma 16.11, $\mathbf{q}\mathsf{S}$ is the identity on $\mathcal{L}(\mathbf{n})$. Now let $r \prec q$, and suppose $r\mathsf{S}$ is the identity on $\mathcal{L}(\mathbf{n})$. Then $r \in X$, contradiction, since $\mathbf{q}$ is the $\preceq$-least element of X. Therefore $\mathbf{q}$ is the order of S on $\mathcal{L}(\mathbf{n})$, as claimed.

17. The Church counting axiom

The "Church counting axiom" expresses the idea that iterating the Church successor function j times starting from $\mathbf{0}$ leads to the Church number j. The formula expressing this fact is not stratified, since j as a function must get an index six higher than j as an "object." Hence if one wishes to use this principle, it must be assumed as a new axiom. Here is that axiom:

Definition 17.1. *The* **Church counting axiom** *is*

$$\forall j \in \mathbb{N}\,(j\mathsf{S}0 = j).$$

A similar axiom was introduced by Rosser [9]. Rosser's axiom is stated using the finite Frege cardinals. It says that $\{x \in \mathbb{F} : x < p\}$ belongs to the cardinal number p. In the last section of this paper, we will prove that the two counting axioms are equivalent. Orey proved [6] that the Rosser counting axiom is not provable in NF (unless, of course, NF is inconsistent). Therefore our result shows that the same is true of the Church counting axiom.

The main result of this paper is that INF plus the Church counting axiom proves that $\mathbb{N}$ is infinite and Church successor is one-to-one on $\mathbb{N}$. Whether this can be proved with intuitionistic logic and without the Church counting axiom we do not know. Our proof appears to require that the order of (successor on) the loop be $\mathbf{m}$, and we failed to prove that without the Church counting axiom. In this section, we present a proof of that fact using the Church counting axiom.

Lemma 17.2 (loop counting)**.** *Assume the Church counting axiom. Suppose* $\mathbb{N} \in \mathsf{FINITE}$ *and* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *and* $\mathbf{k} \neq \mathbf{n}$ *and* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \in \mathbb{N}$*. Let* $q \in \mathbb{N}$*. Then*

$$q\mathsf{S}\mathbf{n} = \mathbf{n} \oplus q.$$

Proof. We have

$$\begin{array}{rll}
\mathbf{n} = \mathbf{n}\mathsf{S}\mathbf{0} & & \text{by the Church counting axiom} \\
q\mathsf{S}\mathbf{n} = q\mathsf{S}(\mathbf{n}\mathsf{S}\mathbf{0}) & & \text{by the preceding line} \\
q\mathsf{S}\mathbf{n} = (q \oplus \mathbf{n})\mathsf{S}\mathbf{0} & & \text{by Lemma 7.6} \\
q\mathsf{S}\mathbf{n} = (\mathbf{n} \oplus q)\mathsf{S}\mathbf{0} & & \text{by Lemma 7.5} \\
\mathbf{n} \oplus q \in \mathbb{N} & & \text{by Lemma 7.3} \\
q\mathsf{S}\mathbf{n} = \mathbf{n} \oplus q & & \text{by the Church counting axiom}
\end{array}$$

Theorem 17.3 (Order of successor on the loop is $\mathbf{m}$)**.** *Assume the Church counting axiom. Suppose* $\mathbb{N} \in \mathsf{FINITE}$ *and* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *and* $\mathbf{k} \neq \mathbf{n}$ *and* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \in \mathbb{N}$*. Suppose* $\mathbf{m} \in \mathbb{N}$ *and* $\mathbf{n} = \mathbf{k} \oplus \mathbf{m}$*, and* $\mathbf{m}$ *is the* $\preceq$*-least solution of* $\mathbf{n} = \mathbf{k} \oplus \mathbf{m}$*. Suppose* $q \in \mathbb{N}$ *and* $q \neq \mathbf{0}$ *and* $q\mathsf{S}$ *is the identity on* $\mathcal{L}(\mathbf{n})$*. Then* $\mathbf{m} \preceq q$*.*

Proof. Suppose qs is the identity on $\mathcal{L}(\mathbf{n})$ and $q \neq \mathbf{0}$. We must show $\mathbf{m} \preceq q$. We have

$$\begin{array}{rll}
q\mathsf{S}\mathbf{n} = \mathbf{n} \oplus q & & \text{by Lemma 17.2 and the Church counting axiom} \\
q\mathsf{S}\mathbf{n} = \mathbf{n} & & \text{since } q\mathsf{S} \text{ is the identity on } \mathcal{L}(\mathbf{n}) \\
\mathbf{n} = \mathbf{n} \oplus q & & \text{by the preceding two lines} \\
\mathbf{n} = \mathbf{k} \oplus q & & \text{by Lemma 16.7} \\
\mathbf{m} \preceq q & & \text{since } \mathbf{m} \text{ is the least solution of } \mathbf{n} = \mathbf{k} \oplus \mathbf{m}
\end{array}$$

That completes the proof of the theorem.

18. Church counting implies $\mathbb{N}$ is not finite

Now we prove a series of lemmas under the hypothesis that $\mathbb{N}$ is finite. With only that hypothesis, results proved earlier under the additional hypothesis that there is a double successor are not applicable; without careful attention to the hypothesis, the reader might get a sense of *deja vu*.

Lemma 18.1. *Suppose* $\mathbb{N}$ *is finite and* $x \in \mathsf{STEM}$*. Then*

$$\exists y \in \mathbb{N}\,(\mathsf{S}y = \mathsf{S}x \ \wedge \ y \neq x) \ \vee \ \neg\exists y \in \mathbb{N}\,(\mathsf{S}y = \mathsf{S}x \ \wedge \ y \neq x).$$

Proof. Since $\mathbb{N}$ is finite, it has decidable equality, by Lemma 3.3 of [1]. Then define

$$R := \{\ \langle x, y\rangle \in \mathbb{N} \times \mathbb{N} : \mathsf{S}y = \mathsf{S}x \quad \wedge \ y \neq x\}.$$

The formula is stratified, giving x and y index 0, with $\mathbb{N} \times \mathbb{N}$ as a parameter. Since $\mathbb{N}$ has decidable equality, R is a decidable relation R on $\mathbb{N}$. The conclusion of the lemma then follows from Lemma 3.21 of [1].

Lemma 18.2. *Suppose* $\mathbb{N}$ *is finite. Then* STEM *is a separable subset of* $\mathbb{N}$*.*

Proof. We have to prove

$$\forall x \in \mathbb{N}\,(x \in \mathsf{STEM} \ \vee \ x \notin \mathsf{STEM}).$$

That formula is stratified, giving x index 0, with STEM a parameter. We can therefore proceed by induction on x.

Base case. $\mathbf{0} \in \mathsf{STEM}$, by Lemma 10.3. Hence $\mathbf{0} \in \mathsf{STEM} \ \vee \ \mathbf{0} \notin \mathsf{STEM}$. That completes the base case.

Induction step. We must prove

$$\mathsf{S}x \in \mathsf{STEM} \ \vee \ \mathsf{S}x \notin \mathsf{STEM}.$$

The induction hypothesis is $x \in \mathsf{STEM} \vee x \notin \mathsf{STEM}$. We argue by cases accordingly.

Case 1, $x \in \mathsf{STEM}$. By Lemma 18.1, we have

$$\exists y \in \mathbb{N}\,(\mathsf{S}y = \mathsf{S}x \ \wedge \ y \neq x) \ \vee \ \neg\exists y \in \mathbb{N}\,(\mathsf{S}y = \mathsf{S}x \ \wedge \ y \neq x).$$

We argue by cases accordingly.

Case 1a, $\exists y \in \mathbb{N}\,(\mathsf{S}y = \mathsf{S}x \ \wedge \ y \neq x)$. Then $\mathsf{S}x \notin \mathsf{STEM}$, by Lemma 10.4. That completes Case 1a.

Case 1b, $\neg\exists y \in \mathbb{N}\,(\mathsf{S}y = \mathsf{S}x \ \wedge \ y \neq x)$. Then $\mathsf{S}x \in \mathsf{STEM}$, by Lemma 10.3. That completes Case 1b. That completes Case 1.

Case 2, $x \notin \mathsf{STEM}$. Then $\mathsf{S}x \notin \mathsf{STEM}$, by Lemma 10.5. That completes Case 2. That completes the induction step. That completes the proof of the lemma.

Lemma 18.3. *Suppose* $\mathbb{N}$ *is finite. Then there exists a double successor* $\mathsf{S}\mathbf{k} = \mathsf{S}n$ *with* $\mathbf{k} \neq \mathbf{n}$ *and* $\mathbf{k} \in \mathsf{STEM}$.

Proof. We have

STEM is a separable subset of $\mathbb{N}$	by Lemma 18.2
$\mathbb{N} \in \mathsf{FINITE}$	by hypothesis
$\mathsf{STEM} \in \mathsf{FINITE}$	by Lemma 3.19 of [1]

We would like to identify $\mathbf{k}$ as the maximal element of the finite set STEM, but that is not a one-line proof, as we do not have a linear ordering on STEM without assuming $\mathbf{k} \in \mathsf{STEM}$, which is what we are trying to prove, so "maximal" makes no sense.

We avoid the need for a linear ordering as follows. Define

$$R := \{\ \langle y, x\rangle \in \mathbb{N} \times \mathbb{N} : x \in \mathsf{STEM} \ \wedge \ x \neq y \ \wedge \ \mathsf{S}x = \mathsf{S}y\ \}.$$

The formula is stratified, so the definition is legal. Then

STEM is a separable subset of $\mathbb{N}$	by Lemma 18.2
$\mathbb{N} \in \mathsf{DECIDABLE}$	by Lemma 3.3 of [1]
R is a decidable relation on $\mathbb{N}$	by the preceding lines

Define

$$Z := \{\ x \in \mathbb{N} : \exists y \in \mathbb{N}\,\langle y, x\rangle \in R\ \}.$$

Remark. Z is the set of $x \in \mathsf{STEM}$ such that $\mathsf{S}x$ is a double successor.

By Lemma 3.21, $Z \in \mathsf{FINITE}$. By Lemma 3.4 of [1], Z is empty or inhabited. We argue by cases accordingly.

Case 1, $Z = \Lambda$. Then there is no $x \in \mathsf{STEM}$ such that $\mathsf{S}x$ is a double successor. Then

$\mathbf{0} \in \mathsf{STEM}$	by Lemma 10.3

I say that STEM is closed under successor. Suppose $x \in \mathsf{STEM}$; we must show $\mathsf{S}x \in \mathsf{STEM}$. By Lemma 10.3, it suffices to show that $\mathsf{S}x$ is not a double successor; that is, it suffices to show that

$$\forall v \in \mathbb{N}\,(\mathsf{S}x = \mathsf{S}v \to x = v).$$

Let $v \in \mathbb{N}$ and $\mathsf{S}x = \mathsf{S}v$; we must show $x = v$. Since $\mathbb{N}$ has decidable equality, we may prove that by contradiction. Suppose $x \neq v$. Then $x \in \mathsf{STEM}$ and $\mathsf{S}x$ is a double successor, so $x \in Z$. But that contradicts the hypothesis $Z = \Lambda$ of Case 1. That completes the proof that STEM is closed under successor. Then

$\mathbb{N} \subseteq \mathsf{STEM}$	by the definition of $\mathbb{N}$
$\mathsf{STEM} \subseteq \mathbb{N}$	by Lemma 10.3
$\mathbb{N} = \mathsf{STEM}$	by the preceding two lines
Church successor is one-to-one on STEM	by Lemma 10.4
Church successor is one-to-one on $\mathbb{N}$	by the preceding two lines
ChurchSuccessor is not onto $\mathbb{N}$	by Theorem 3.8
$\mathbb{N}$ is infinite	by Definition 3.23 of [1]
$\neg\,\mathbb{N} \in \mathsf{FINITE}$	by Theorem 3.24 of [1]

But that contradicts the hypothesis that $\mathbb{N}$ is finite. That completes Case 1.

Case 2, Z is inhabited. Then there exists some $x \in \mathsf{STEM}$ such that $\mathsf{S}x$ is a double successor. That completes the proof of the lemma.

Lemma 18.4. *Suppose* $\mathbb{N} \in \mathsf{FINITE}$ *and* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *and* $\mathbf{k} \neq \mathbf{n}$ *and* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \in \mathbb{N}$. *Then*

$$\forall x \in \mathbb{N}\,(x \neq \mathbf{0} \to \mathbf{n} = \mathbf{k} \oplus x \to \mathbf{n} = \mathbf{n} \oplus x).$$

Proof. We have

$\mathbf{k} \in \mathbb{N}$	by Lemma 10.2, since $\mathbf{k} \in \mathsf{STEM}$
$\mathbf{n} = \mathbf{k} \oplus x$	by hypothesis
$\mathsf{S}\mathbf{n} = \mathsf{S}(\mathbf{k} \oplus x)$	by the previous line
$\mathsf{S}\mathbf{n} = \mathbf{k} \oplus \mathsf{S}x$	by Lemma 4.5
$\mathsf{S}\mathbf{n} = \mathsf{S}\mathbf{k} \oplus x$	by Lemma 7.2
$\mathsf{S}\mathbf{n} = \mathsf{S}\mathbf{n} \oplus x$	since $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$
$\mathsf{S}\mathbf{n} = \mathbf{n} \oplus \mathsf{S}x$	by Lemma 7.2
$\mathsf{S}\mathbf{n} = \mathsf{S}(\mathbf{n} \oplus x)$	by Lemma 4.5
$\mathbf{n} \in \mathcal{L}(\mathbf{n})$	by Lemma 11.2
$\mathbf{n} \oplus x \in \mathcal{L}(\mathbf{n})$	by Lemma 16.5
$\mathbf{n} \oplus x = \mathbf{n}$	by Theorem 13.2

That completes the proof of the lemma.

Lemma 18.5. *Suppose* $\mathbb{N} \in \mathsf{FINITE}$ *and* $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ *and* $\mathbf{k} \neq \mathbf{n}$ *and* $\mathbf{k} \in \mathsf{STEM}$ *and* $\mathbf{n} \in \mathbb{N}$. *Suppose* $\mathbf{m} \in \mathbb{N}$ *with* $\mathbf{n} = \mathbf{k} + \mathbf{m}$. *Then* $\mathbf{m}\mathsf{S}$ *is the identity on* $\mathcal{L}(\mathbf{n})$.

Remark. We want to say, "by the Annihilation Theorem." But the domain of successor is more than just the loop, so we must consider its restriction f to $\mathcal{L}(\mathbf{n})$, and verify that f satisfies the hypotheses of the Annihilation Theorem; and after the application, we still have to verify that the iterates of the restriction are the restrictions of the iterates.

Proof. We have

$$\begin{aligned}
\mathsf{S}\mathbf{n} &= \mathsf{S}(\mathbf{k}+\mathbf{m}) && \text{since } \mathbf{n} = \mathbf{k}+\mathbf{m} \\
&= \mathbf{k} + \mathsf{S}\mathbf{m} && \text{by Lemma 4.5} \\
&= \mathsf{S}\mathbf{k} + \mathbf{m} && \text{by Lemma 7.2} \\
&= \mathsf{S}\mathbf{n} + \mathbf{m} && \text{since } \mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}
\end{aligned}$$

Define f to be the restriction of Church successor to $\mathcal{L}(\mathbf{n})$ (which can be done by means of a stratified formula). One can verify that f is an injection from $\mathcal{L}(n)$ to $\mathcal{L}(\mathbf{n})$, in the sense of Definition 3.2. The most important step is that f is one-to-one, by Theorem 13.2. We omit the details of the verification (about 180 steps).

By Lemma 13.1, $\mathcal{L}(\mathbf{n})$ is finite. By Lemma 18.4 and the hypothesis that $\mathbf{n} = \mathbf{k}+\mathbf{m}$, we have $\mathbf{n} = \mathbf{k}+\mathbf{m}$. Since $f : \mathcal{L}(\mathbf{n}) \to \mathcal{L}(\mathbf{n})$ is an injection, we can apply the Annihilation Theorem to obtain

$$\forall x \in \mathcal{L}(\mathbf{n})\,(\mathbf{m} f x = x).$$

Then by Lemma 16.13, we have

$$\forall x \in \mathcal{L}(\mathbf{n})\,(\mathbf{m}\mathsf{S} x = x).$$

as desired. That completes the proof of the lemma.

Theorem 18.6. *The Church counting axiom implies that* $\mathbb{N}$ *is not finite.*

Proof. Assume the Church counting axiom, and suppose $\mathbb{N}$ is finite. By Lemma 18.3, there is a double successor $\mathsf{S}\mathbf{n} = \mathsf{S}\mathbf{k}$ with with $\mathbf{k} \neq \mathbf{n}$ and $\mathbf{k} \in \mathsf{STEM}$. Then by Lemma 16.3, there exists a $\preceq$-least $\mathbf{m} \in \mathbb{N}$ such that $\mathbf{n} = \mathbf{k}+\mathbf{m}$. Fix that $\mathbf{m}$. Then by Theorem 17.3, $\mathbf{m}$ is the order of successor restricted to $\mathcal{L}(\mathbf{n})$. Explicitly, we have

$$\forall q \in \mathbb{N}\,(q \neq \mathbf{0} \to q\mathsf{S}\mathbf{n} = \mathbf{n} \to \mathbf{m} \preceq q). \tag{35}$$

(This is where we use the Church counting axiom, since Theorem 17.3 requires it.)

We have

$$\begin{aligned}
\mathbf{n} &\neq \mathbf{0} && \text{by Lemma 10.13} \\
\mathbf{n} &\in \mathcal{L}(\mathbf{n}) && \text{by Lemma 11.2} \\
\mathbf{n} &= \mathsf{S}p && \text{for some } p \in \mathcal{L}(\mathbf{n}), \text{ by Theorem 11.8}
\end{aligned}$$

Now define

$$X := \mathcal{L}(\mathbf{n}) - \{\mathbf{n}\}.$$

and define f

$$f = (\{\langle x, \mathsf{S}x\rangle : x \in X\} - \{\langle p, \mathbf{n}\rangle\}) \cup \{\ \langle p, \mathsf{S}\mathbf{n}\rangle\}.$$

Informally, the idea of the definition of f is that $f(x) = \mathsf{S}x$ except when $x = p$, and $f(p) = \mathsf{S}\mathbf{n}$.

Our first observation about f is that

$$\langle x, \mathsf{S}\mathbf{n}\rangle \in f \to x = p \tag{36}$$

To prove that, suppose $\langle x, \mathsf{S}\mathbf{n}\rangle \in f$. Then

$$\begin{array}{rl} x \in \mathcal{L}(\mathbf{n}) & \text{by definition of } X \text{ and } f \\ \mathsf{S} \in \mathcal{L}(\mathbf{n}) & \text{by Lemma 11.2} \\ \mathsf{S}n \neq \mathbf{n} & \text{by Lemma 12.3} \\ \mathsf{S}x = \mathsf{S}n \to x = p & \text{by Theorem 13.2} \end{array}$$

Now (36) follows from the definition of f.

We have

$$\begin{array}{rl} Rel(f) & \text{by 17 omitted steps} \\ f \in \mathsf{FUNC} & \text{by 60 omitted steps} \\ \mathsf{S}\mathbf{n} \neq \mathbf{n} & \text{by Lemma 12.3} \\ dom(f) \subseteq X & \text{by the preceding line and 30 omitted steps} \\ range(f) \subseteq X & \text{by Theorem 13.2, Lemma 12.3, and 46 omitted steps} \\ f : X \to X & \text{by Theorem 13.2 and 82 omitted steps} \end{array}$$

I say that f is one-to-one. Suppose $\langle x, y\rangle \in f$ and $\langle u, y\rangle \in f$. We must prove $x = u$. Since $\mathbb{N}$ is finite, $\mathbb{N}$ has decidable equality, by Lemma 3.3 of [1]. Therefore

$$y = \mathsf{S}\mathbf{n} \ \vee \ y \neq \mathsf{S}\mathbf{n}.$$

Case 1, $y = \mathsf{S}\mathbf{n}$. Then

$$\begin{array}{ll} x = p & \text{by (36)} \\ u = p & \text{by (36)} \\ x = u & \text{by the preceding two lines} \end{array}$$

That completes Case 1.

Case 2, $y \neq \mathsf{S}\mathbf{n}$. Then $y = \mathsf{S}x$ and $y = \mathsf{S}u$. We have

$$\begin{array}{rl} x \in X \ \wedge \ u \in X & \text{since } dom(f) \subseteq X \\ x \in \mathcal{L}(\mathbf{n}) \ \wedge \ u \in \mathcal{L}(\mathbf{n}) & \text{since } X \subseteq \mathcal{L}(\mathbf{n}) \\ \mathsf{S}x \in \mathcal{L}(\mathbf{n}) & \text{by Lemma 11.2} \\ y \in \mathcal{L}(\mathbf{n}) & \text{since } y = \mathsf{S}x \\ x = u & \text{by Theorem 13.2} \end{array}$$

That completes Case 2. That completes the proof that f is one-to-one.

We have now proved that f is an injection, since by definition that means $f : X \to X$, f is one-to-one, $f \in \mathsf{FUNC}$ and $Rel(f)$, all of which we have verified. Hence we can apply the Annihilation Theorem to f and X to conclude that $\mathbf{m}f$ is the identity on X. Explicitly,

(37) $$\forall x \in X\, (\mathbf{m}fx = x)$$

In the rest of the proof, we will show that $\mathbf{m}f$ is not the identity on X, thus contradicting (37).

Let $\alpha := \mathsf{S}\mathbf{n}$. Then

$$\begin{array}{rl}
\mathsf{S}\mathbf{n} \neq \mathbf{n} & \text{by Lemma 12.3} \\
\mathbf{n} \in \mathcal{L}(\mathbf{n}) & \text{by Lemma 11.2} \\
\mathsf{S}\mathbf{n} \in L(\mathbf{n}) & \text{by Lemma 11.2} \\
\alpha \in \mathcal{L}(\mathbf{n}) & \text{since } \alpha = \mathsf{S}\mathbf{n} \text{ and } \mathbf{n} \in \mathcal{L}(\mathbf{n}) \\
\alpha \neq \mathbf{n} & \text{since } \alpha = \mathsf{S}\mathbf{n} \text{ and } \mathsf{S}\mathbf{n} \neq \mathbf{n} \\
\alpha \in X & \text{since } X = \mathcal{L}(\mathbf{n}) - \{\mathbf{n}\}
\end{array}$$

I say that

$$q \neq \mathbf{n} \to \mathsf{S}q \prec \mathbf{m} \to qf\alpha = q\mathsf{S}\alpha. \tag{38}$$

We prove this by finite induction on q. That is legal, since we can stratify that formula, giving q index 6 and α index 0. $\mathbf{m}$ occurs as a parameter, so we do not need to give it an index, but we could give it index 6. f gets index 3, since it contains pairs of objects of index 0; so q contains pairs of objects of index 3; those pairs have index 5, which is why q gets index 6.

Base case, $q = \mathbf{0}$. We have $\mathbf{0}f\alpha = \alpha = \mathbf{0}\mathsf{S}\alpha$, by Lemma 2.13. That completes the base case.

Induction step. Since we are using finite induction, we get to assume

$$q \neq \mathbf{n} \tag{39}$$

We also assume

$$\mathsf{S}q \neq \mathbf{n} \ \wedge \ \mathsf{S}(\mathsf{S}q) \prec \mathbf{m} \tag{40}$$

We have to prove

$$\mathsf{S}q\mathsf{S}\alpha = \mathsf{S}qf\alpha \tag{41}$$

We have

$$\begin{array}{rl}
\mathsf{S}(\mathsf{S}q) \neq \mathbf{n} & \text{by Lemma 14.22,since } \mathsf{S}(\mathsf{S}q) \prec \mathbf{m} \\
\mathsf{S}q \prec \mathsf{S}(\mathsf{S}q) & \text{by Corollary 14.12, since } \mathsf{S}q \neq \mathbf{n} \\
\mathsf{S}q \prec \mathbf{m} & \text{by Lemma 14.24, since } \mathsf{S}(\mathsf{S}\mathbf{q}) \prec \mathbf{m} \\
q\mathsf{S}\alpha \in \mathcal{L}(\mathbf{n}) & \text{by Lemma 16.4, since } \alpha \in \mathcal{L}(\mathbf{n}) \\
\mathcal{L}(\mathbf{n}) \subseteq \mathbb{N} & \text{by Lemma 11.2} \\
q\mathsf{S}\alpha \in \mathbb{N} & \text{by the preceding two lines} \\
p \in \mathbb{N} & \text{since } p \in \mathcal{L}(\mathbf{n}) \text{ and } \mathcal{L}(\mathbf{n}) \subseteq \mathbb{N}.
\end{array}$$

Since $\mathbb{N}$ is finite, it has decidable equality, by Lemma 3.3 of [1]. Since $p \in \mathcal{L}(\mathbf{n})$ and $q\mathsf{S}\alpha \in \mathbb{N}$, we have

$$\mathbf{q}\mathsf{S}\alpha = p \ \vee \ \mathbf{q}\mathsf{S}\alpha \neq p.$$

We argue by cases accordingly.

Case 1, $q\mathsf{S}\alpha = p$. Then

$$\begin{array}{rl}
\mathsf{S}(q\mathsf{S}\alpha) = \mathsf{S}p & \text{since } q\mathsf{S}\alpha = p \\
= \mathbf{n} & \text{since } \mathsf{S}p = \mathbf{n} \\
\mathsf{S}(\mathsf{S}(q\mathsf{S}\alpha)) = \mathsf{S}n & \text{by the previous line} \\
\mathsf{S}(\mathsf{S}(q\mathsf{S}\alpha)) = \alpha & \text{since } \mathsf{S}n = \alpha \\
\mathsf{S}(q\mathsf{S}\alpha) = \mathsf{S}q\mathsf{S}\alpha & \text{by Theorem 3.6} \\
\mathsf{S}(\mathsf{S}q\mathsf{S}\alpha) = \alpha & \text{by the preceding two lines} \\
\mathsf{S}(\mathsf{S}q)\mathsf{S}\alpha = \alpha & \text{by Theorem 3.6} \\
\mathsf{S}(\mathsf{S}q)\mathsf{S}x = x \ \text{ for all } x \in \mathcal{L}(\mathbf{n}) & \text{by Lemma 16.12} \\
\mathbf{m} \preceq \mathsf{S}(\mathsf{S}q) & \text{by Theorem 17.3 and (35)} \\
\mathsf{S}(\mathsf{S}q) \prec \mathbf{m} & \text{by (40)} \\
\mathsf{S}(\mathsf{S}q) \preceq \mathbf{m} \ \wedge \ \mathsf{S}(\mathsf{S}q) \neq \mathbf{m} & \text{by the definition of } \prec \\
\mathsf{S}(\mathsf{S}q) = \mathbf{m} & \text{by Theorem 14.21}
\end{array}$$

But the last two lines are contradictory. That shows that Case 1 is impossible.

Case 2, $q\mathsf{S}\alpha \neq p$. We have $\mathsf{S}q \neq \mathbf{n}$ and $\mathsf{S}(\mathsf{S}q) \prec \mathbf{m}$ by hypothesis, but in order to apply the induction hypothesis, we need $q \neq \mathbf{n}$ and $\mathsf{S}q \prec \mathbf{m}$. We have $q \neq \mathbf{n}$ by (39). Here is a proof that $\mathsf{S}q \prec \mathbf{m}$:

$$\begin{array}{rl}
\mathsf{S}q \prec \mathsf{S}(\mathsf{S}q) & \text{by Lemma 14.10, since } \mathsf{S}q \neq \mathbf{n} \\
\mathsf{S}(\mathsf{S}q) \prec \mathbf{m} & \text{by hypothesis} \\
\mathsf{S}q \prec \mathbf{m} & \text{by Lemma 14.24}
\end{array}$$

Now we can use the induction hypothesis. We proceed to the proof of the induction step.

$$\begin{array}{rl}
\mathsf{S}qf\alpha = f(qf\alpha) & \text{by Theorem 3.6} \\
qf\alpha \in X & \text{by Lemma 12.6, since } f : X \to X \\
\mathsf{S}qf\alpha = f(q\mathsf{S}\alpha) & \text{by the induction hypothesis} \\
= \mathsf{S}(q\mathsf{S}\alpha) & \text{since } q\mathsf{S}\alpha \neq p \text{, by definition of } f \\
= \mathsf{S}q\mathsf{S}\alpha & \text{by Theorem 3.6}
\end{array}$$

That completes Case 2. That completes the induction step. That completes the proof of (41); that is, it completes the induction step. That completes the proof of (38).

We have $\mathbf{m} \neq \mathbf{0}$, since if $\mathbf{m} = \mathbf{0}$ then $\mathbf{n} = \mathbf{k} + \mathbf{m} = \mathbf{k} + \mathbf{0} = \mathbf{k}$, contradiction. Then by Lemma 14.19, there exists m_1 such that

$$\begin{array}{r}
\mathsf{S}m_1 = \mathbf{m} \\
m_1 \in \mathbb{N} \ \wedge \ m_1 \neq \mathbf{n}
\end{array}$$

(The variable names m_1 and m_2 in this proof are meant to suggest $m-1$ and $m-2$, although subtraction has not been defined.) I say $m_1 \neq \mathbf{0}$. Here is the proof:

$$\begin{array}{rl}
m_1 = \mathbf{0} & \text{assumption} \\
\mathsf{S}m_1 = \mathsf{S}\mathbf{0} & \text{by the previous line} \\
\mathsf{S}m_1 = \mathbf{m} & \text{by construction of } m_1 \\
\mathbf{m} = \mathsf{S}\mathbf{0} & \text{by the preceding lines} \\
\mathbf{k} \oplus \mathsf{S}\mathbf{0} = \mathbf{n} & \text{since } \mathbf{k} + \mathbf{m} = \mathbf{n} \\
\mathsf{S}(\mathbf{k} \oplus \mathbf{0}) = \mathbf{n} & \text{by Lemma 4.5} \\
\mathsf{S}\mathbf{k} = \mathbf{n} & \text{by Lemma 4.4} \\
\mathsf{S}(\mathsf{S}\mathbf{k}) = \mathsf{S}\mathbf{n} & \text{by the previous line} \\
\mathsf{S}(\mathsf{S}\mathbf{k}) = \mathsf{S}\mathbf{k} & \text{since } \mathsf{S}\mathbf{n} = \mathsf{S}\mathbf{k} \\
\mathsf{S}(\mathsf{S}\mathbf{k}) \neq \mathsf{S}\mathbf{k} & \text{by Lemma 12.3}
\end{array}$$

That contradiction completes the proof that $m_1 \neq \mathbf{0}$.

Then by Lemma 14.19, there exists m_2 such that

$$\begin{array}{r}
\mathsf{S}m_2 = m_1 \\
m_2 \in \mathbb{N} \ \wedge \ m_2 \neq \mathbf{n}
\end{array}$$

Then

$$\begin{array}{rl}
m_1 \prec \mathsf{S}m_1 & \text{by Lemma 14.12, since } m_1 \neq \mathbf{n} \\
\mathsf{S}m_2 \prec \mathbf{m} & \text{since } \mathsf{S}m_2 = \mathbf{m}_1 \text{ and } \mathsf{S}m_1 = \mathbf{m}
\end{array}$$

Since $\mathsf{S}m_2 \prec \mathbf{m}$ and $m_2 \neq \mathbf{n}$, we have

$$m_2 f\alpha = m_2\mathsf{S}\alpha \qquad \text{by (38).} \tag{42}$$

We also have

$$\begin{array}{rl}
\mathsf{S}(\mathsf{S}(p)) = \mathsf{S}\mathbf{n} = \alpha & \text{by the definitions of } p \text{ and } \alpha \\
\mathbf{m}\mathsf{S}\alpha = \alpha & \text{by Lemma 18.5} \\
\mathsf{S}(\mathsf{S}m_2)\mathsf{S}\alpha = \alpha & \text{since } \mathsf{S}(\mathsf{S}m_2) = \mathbf{m} \\
\mathsf{S}(\mathsf{S}m_2)\mathsf{S}\alpha = \mathsf{S}\mathbf{n} & \text{since } \alpha = \mathsf{S}\mathbf{n} \\
\mathsf{S}(\mathsf{S}m_2\mathsf{S}\alpha) = \mathsf{S}\mathbf{n} & \text{by Theorem 3.6} \\
(\mathsf{S}m_2)\mathsf{S}\alpha \in \mathcal{L}(\mathbf{n}) & \text{by Lemma 16.4} \\
(\mathsf{S}m_2)\mathsf{S}\alpha = \mathbf{n} & \text{by Theorem 13.2} \\
(\mathsf{S}m_2)\mathsf{S}\alpha = \mathsf{S}p & \text{since } \mathbf{n} = \mathsf{S}p \\
\mathsf{S}(m_2\mathsf{S}\alpha) = \mathsf{S}p & \text{by Theorem 3.6} \\
m_s\mathsf{S}\alpha \in \mathcal{L}(\mathbf{n}) & \text{by Lemma 16.4}
\end{array}$$

$$m_2\mathsf{S}\alpha = p \qquad \text{by Theorem 13.2} \tag{43}$$

$m_2 f\alpha = p$	by (42) and (43)
$f(m_2 f\alpha) = f(p)$	applying f to both sides
$(\mathsf{S}m_2)f(\alpha) = f(p)$	by Theorem 3.6
$m_1 f\alpha = f(p)$	since $\mathsf{S}m_2 = m_1$
$f(p) = \alpha$	by the definition of f
$m_1 f\alpha = \alpha$	by the preceding two lines
$f(m_1 f\alpha) = f(\alpha)$	applying f to both sides
$(\mathsf{S}m_1)f\alpha = f(\alpha)$	by Theorem 3.6
$\mathbf{m}f\alpha = f(\alpha)$	since $\mathsf{S}m_1 = \mathbf{m}$
$\mathsf{S}(\mathsf{S}\mathbf{n}) \neq \mathbf{n}$	by Lemma 12.4
$\alpha = p \to \mathsf{S}(\mathsf{S}\mathbf{n}) = \mathbf{n}$	since $\mathsf{S}\mathbf{n} = \alpha$ and $\mathsf{S}p = \mathbf{n}$
$\alpha \neq p$	by the previous two lines
$f(\alpha) = \mathsf{S}\alpha$	by definition of f, since $\alpha \neq p$
$\mathbf{m}f\alpha = \mathsf{S}\alpha$	since $\mathbf{m}f\alpha = f(\alpha)$
$\mathsf{S}\alpha \neq \alpha$	by Lemma 12.3
$\mathbf{m}f(\alpha) \neq \alpha$	by the previous two lines
$\mathbf{m}f(\alpha) = \alpha$	by the Annihilation Theorem

That contradiction completes the proof of the theorem.

19. $\mathbb{N}$ NOT FINITE IMPLIES $\mathbb{N}$ IS INFINITE

In this section we will show that if $\mathbb{N}$ is not finite, then $\mathbb{N}$ is infinite, and indeed (what is more) Church successor is one-to-one on $\mathbb{N}$. Since we proved that the Church counting axiom implies $\mathbb{N}$ is not finite, it will follow that the Church counting axiom implies $\mathbb{N}$ is infinite and S is one-to-one.

That Church successor is one-to-one means $\mathsf{S}x = \mathsf{S}y \to x = y$. That it is weakly one-to-one means $x \neq y \to \mathsf{S}x \neq \mathsf{S}y$. One can check that if successor is weakly one-to-one, then $\mathbb{N}$ has decidable equality (by induction, with Lemma 3.10 as the base case). With decidable equality, weakly one-to-one implies one-to-one.

The idea of the proof can be explained simply. We start at $\mathbf{0}$ and make dots on our paper for $0, 1, 2, \ldots$. At any moment the set of dots so far written is finite. If we come to a double successor (as shown in Fig. 1), then we have a set that contains $\mathbf{0}$ and is closed under successor, so it is all of $\mathbb{N}$; but then $\mathbb{N}$ is finite, so that cannot happen. Instead we continue on indefinitely, i.e., successor is one-to-one.

To make that idea rigorous, we will define a relation $\mathbb{B}$, whose intended interpretation is that if $\langle \{x\}, y\rangle \in \mathbb{B}$, then y is the set of dots written down after x steps of the drawing process described above. We use $\{x\}$ instead of x to achieve stratification. The idea is to define $\mathbb{B}$ in such a way that $\mathbb{B}$ is the least relation such that

$$\langle \{\mathbf{0}\}, \{\mathbf{0}\}\rangle \in \mathbb{B}$$
$$\forall x, y \in \mathbb{N}\,(\langle \{x\}, y\rangle \in \mathbb{B} \to \mathsf{S}x \notin y \to \langle \mathsf{S}x, y \cup \{\mathsf{S}x\}\rangle \in \mathbb{B})$$

Of course, a proper definition cannot mention $\mathbb{B}$ on the right. Here is a proper definition:

Definition 19.1. *$\mathbb{B}$ is the set of all ordered pairs $\langle\{p\}, q\rangle$ with $p, q \in \mathbb{N}$ such that $\langle\{p\}, q\rangle$ belongs to every set w satisfying the following conditions:*

$$\begin{aligned}
&\langle\{\mathbf{0}\}, \{\mathbf{0}\}\rangle \in w \\
&\forall x, y \in \mathbb{N}\,(\langle\{x\}, y\rangle \in w \to \mathsf{S}x \notin y \to \langle\{\mathsf{S}x\}, y \cup \{\mathsf{S}x\}\rangle \in w)
\end{aligned}$$

The formula is stratified, giving x index 0, y index 1, so $\langle\{x\}, y\rangle$ gets index 3; then 2 gets index 4. $\mathbf{0}$ is a parameter, so does not need an index, but we could give it index 0. Either way, the formula is stratified, so the definition can be given in INF.

Lemma 19.2. $\langle\{\mathbf{0}\}, \{\mathbf{0}\}\rangle \in \mathbb{B}$.

Proof. Immediate from the definition of $\mathbb{B}$.

Lemma 19.3.

$$\langle\{x\}, y\rangle \in \mathbb{B} \to \mathsf{S}x \neq y \to \langle\{\mathsf{S}x\}, y \cup \{\mathsf{S}x\} \in \mathbb{B}.$$

Proof. Follows from Definition 19.1 in about 25 steps (omitted here).

Lemma 19.4. *Suppose $\langle\{x\}, y\rangle \in \mathbb{B}$. Then $y \in \mathsf{FINITE}$ and $y \subseteq \mathbb{N}$ and $x \in \mathbb{N}$.*

Proof. Let W be the set of members of $\mathbb{B}$ satisfying the conditions in the lemma; explicitly,

$$W = \{\ \langle\{x\}, y\rangle \in \mathbb{B} : y \in \mathsf{FINITE}\ \wedge\ y \subseteq \mathbb{N}\ \wedge\ x \in \mathbb{N}\ \}.$$

Then W satisfies the closure conditions in Definition 19.1:

$$\begin{array}{rl}
\langle\{\mathbf{0}\}, \{\mathbf{0}\}\rangle \in W & \text{by Lemma 19.2} \\
\{\mathbf{0}\} \in \mathsf{FINITE} & \text{by Lemma 3.9 of [1]} \\
y \cup \{\mathsf{S}x\} \in \mathsf{FINITE} & \text{if } \mathsf{S}x \notin y\text{, by Lemma 3.7 of [1]}
\end{array}$$

The details, omitted here, take about 90 steps. Therefore $Z \subseteq W$. That completes the proof of the lemma.

Lemma 19.5. *Suppose $\langle\{x\}, y\rangle \in \mathbb{B}$. Then*

$$\begin{aligned}
&\mathbf{0} \in y \\
&x \in y \\
&\forall u\,(u \in y \to u \neq x \to \mathsf{S}x \in y)
\end{aligned}$$

Remark. The last condition, expressed in words, is "y is closed under successor except x."

Proof. Let W be defined as the set of all $\langle\{x\}, y\rangle \in \mathbb{B}$ such that conditions of the lemma are satisfied. Since the formulas in the lemma are stratified, W can be defined in INF. We will prove W satisfies the closure conditions in the definition of $\mathbb{B}$.

First, $\langle\{\mathbf{0}\}, \{\mathbf{0}\}\rangle \in W$; it belongs to Z by Lemma 19.2, and the other conditions are straightforward.

Second, assume $\langle\{x\}, y\rangle \in W$ and $\mathsf{S}x \notin y$. We must show $\langle\{\mathsf{S}x\}, y \cup \{\mathsf{S}x\}\rangle \in W$. By Lemma 19.3, it belongs to $\mathbb{B}$.

Since $\langle\{x\}, y\rangle \in W$, we have $\mathbf{0} \in y$. Hence $\mathbf{0} \in y \cup \{\mathsf{S}x\}$.

By Lemma 19.4, we have $y \in \mathsf{FINITE}$. Then $y \in \mathsf{DECIDABLE}$, by Lemma 3.3 of [1]. We have to show $y \cup \{\mathsf{S}x\}$ is closed under successor except $\mathsf{S}x$. Let $u \in y \cup \{\mathsf{S}x\}$

with $u \neq \mathsf{S}x$. Then $u \in y$. Since $y \in \mathsf{DECIDABLE}$, we have $u = x \ \vee \ u \neq x$. If $u = x$ then $\mathsf{S}u = \mathsf{S}x \in y \cup \{\mathsf{S}x\}$. If $u \neq x$ then $\mathsf{S}x \in y$ since $\langle \{x\}, y\rangle \in W$; therefore $\mathsf{S}x \in y \cup \{\mathsf{S}x\}$ as well.

That completes the proof that W satisfies the closure conditions. That completes the proof of the lemma.

Lemma 19.6 (No loops)**.** *Assume* $\mathbb{N}$ *is not finite. Suppose* $\langle \{x\}, y\rangle \in \mathbb{B}$*. Then* $\mathsf{S}x \notin y$*.*

Proof. Suppose $\mathsf{S}x \in y$. Then

$$
\begin{array}{rl}
\mathbf{0} \in y & \text{by Lemma 19.5} \\
u \in y \to u \neq x \to \mathsf{S}u \in y & \text{by Lemma 19.5} \\
\mathsf{S}x \in y & \text{by hypothesis} \\
y \in \mathsf{FINITE} & \text{by Lemma 19.4} \\
y \in \mathsf{DECIDABLE} & \text{by Lemma 3.3 of [1]} \\
x \in y & \text{by Lemma 19.5} \\
u \in y \to u = x \ \vee \ u \neq x & \text{by the preceding lines} \\
u \in y \to \mathsf{S}u \in y & \text{by the preceding lines} \\
\mathbb{N} \subseteq y & \text{by the definition of } \mathbb{N} \\
y \subseteq \mathbb{N} & \text{by Lemma 19.4} \\
y = \mathbb{N} & \text{by the preceding two lines} \\
\mathbb{N} \in \mathsf{FINITE} & \text{since } y \in \mathsf{FINITE}
\end{array}
$$

But that contradicts the hypothesis. That completes the proof of the lemma.

Lemma 19.7. *Assume* $\mathbb{N}$ *is not finite. Then*

$$\forall x \in \mathbb{N}\, \exists y\, (\langle \{x\}, y\rangle \in \mathbb{B}).$$

Proof. The formula in the lemma is stratified, giving x and y index 0, since Z is a definable relation (occurring here as a parameter). Therefore we may prove it by induction on x.

Base case, $x = \mathbf{0}$, holds by Lemma 19.2.

Induction step. Suppose $\langle \{x\}, y\rangle \in \mathbb{B}$. By Lemma 19.6, $\mathsf{S}x \notin y$. Then by Lemma 19.3, $\{\mathsf{S}x\}, y \cup \{\mathsf{S}x\} \in \mathbb{B}$. That completes the induction step. That completes the proof of the lemma.

Lemma 19.8. *Suppose* $\langle \{x\}, p\rangle \in \mathbb{B}$*. Then* $x = \mathbf{0}$*, or* $x = \mathsf{S}u$ *for some* $u \in \mathbb{N}$*.*

Proof. Define

$$Z := \{\ \langle \{x\}, p\rangle \in \mathbb{B} : x = \mathbf{0} \ \vee \ \exists u \in \mathbb{N}\, (\mathsf{S}u = x)\}.$$

Then Z satisfies the conditions in the definition of $\mathbb{B}$, as one verifies in about 70 steps (here omitted). Therefore $\mathbb{B} \subseteq Z$. To finish the proof:

$$
\begin{array}{rl}
\langle \{x\}, p\rangle \in \mathbb{B} & \text{assumption} \\
\langle \{x\}, p\rangle \in Z & \text{since } \mathbb{B} \subseteq Z \\
x = \mathbf{0} \ \vee \ \exists u \in \mathbb{N}\, (\mathsf{S}u = x) & \text{by the definition of } Z
\end{array}
$$

The two resulting cases are just the conditions that Z has been proved to satisfy. That completes the proof of the lemma.

Lemma 19.9. *Suppose $\langle \{\mathbf{0}\}, p\rangle \in \mathbb{B}$. Then $p = \{\mathbf{0}\}$.*

Proof. Suppose $p \neq \{\mathbf{0}\}$. Then define

$$Z := \mathbb{B} - \{\langle \{\mathbf{0}\}, p\rangle\}.$$

One can verify that Z satisfies the closure conditions in the definition of $\mathbb{B}$. (It takes about 60 steps, omitted here, using several of the lemmas above, including Lemmas 19.3 and 19.8.) Therefore $\mathbb{B} \subseteq Z$. But that is a contradiction. Therefore $\neg\neg\, p = \{\mathbf{0}\}$. Now

$$\begin{array}{rl}
p \in \mathsf{FINITE} & \text{by Lemma 19.4} \\
p \in \mathsf{DECIDABLE} & \text{by Lemma 3.3 of [1]} \\
\mathbf{0} \in p & \text{by Lemma 19.5} \\
\neg\neg\, \forall u \in p\, (u = \mathbf{0}) & \text{since } \neg\neg\, p = \{\mathbf{0}\} \\
\forall u \in p\, (\neg\neg\, (u = \mathbf{0})) & \text{by intuitionistic logic} \\
\forall u \in p\, (u = \mathbf{0}) & \text{since } p \in \mathsf{DECIDABLE} \\
p = \{\mathbf{0}\} & \text{by the preceding line and } \mathbf{0} \in p
\end{array}$$

That completes the proof of the lemma.

Lemma 19.10. *Suppose $x \in \mathbb{N}$ and $\langle \{\mathsf{S}x\}, y\rangle \in \mathbb{B}$. Then there exist u and p such that*

$$\begin{array}{l}
\mathsf{S}x = \mathsf{S}u \\
\langle \{u\}, p\rangle \in \mathbb{B} \\
\mathsf{S}u \notin p \\
y = p \cup \{\mathsf{S}u\}
\end{array}$$

Remark. The point of the lemma (and the preceding one) is that everything in $\mathbb{B}$ is in $\mathbb{B}$ because it has been constructed according to the two construction rules in the definition.

Proof. Define

$$\begin{array}{rl}
Z := \{\ z \in \mathbb{B} : & z = \langle \{\mathbf{0}\}, \{\mathbf{0}\}\rangle\ \vee \\
& (\exists x, y\, (x \in \mathbb{N}\ \wedge\ z = \langle \{\mathsf{S}x\}, y\rangle)\ \wedge \\
& (\forall x, y\, (x \in \mathbb{N} \to z = \langle \{\mathsf{S}x\}, y\rangle) \to \\
& \exists u, p\, (\langle \{u\}, p\rangle \in \mathbb{B}\ \wedge\ x \in \mathbb{N}\ \wedge\ u \in \mathbb{N}\ \wedge \\
& \mathsf{S}u = \mathsf{S}x\ \wedge\ \mathsf{S}u \notin p\ \wedge\ y = p \cup \{\mathsf{S}u\})\ \}
\end{array}$$

The formula is stratified, giving x and u index 0, and y and p index 1. Then the ordered pairs are pairs of type 1 objects, so they get type 3. So z gets index 3, and $\mathbb{B}$ is a parameter. Therefore the definition is legal in INF.

Then one can verify that Z satisfies the closure conditions in the definition of $\mathbb{B}$. (It takes about 110 steps, omitted here.) There are several variations of the definition of Z that look equally convincing but are in fact not correct. Once the definition is correct, the 110 steps mentioned are fairly straightforward.

Having derived that Z satisfies the closure conditions, we have $\mathbb{B} \subseteq Z$, by definition of $\mathbb{B}$. Now suppose $x \in \mathbb{N}$ and $\langle \{\mathsf{S}x\}, y\rangle \in \mathbb{B}$. Then since $\mathbb{B} \subseteq Z$ we have $\langle \{\mathsf{S}x\}, y\rangle \in Z$. Substituting $\langle \{\mathsf{S}x\}, y\rangle$ for z in the definition of Z, the disjunction on the right of the definition gives rise to two cases.

Case 1, $\langle \{\mathsf{S}x\}, y\rangle = \langle \{\mathbf{0}\}, \{\mathbf{0}\}\rangle$. Then

$$\begin{array}{rl} \{\mathsf{S}x\} = \{\mathbf{0}\} & \text{by Lemma 2.1 of [1]} \\ \mathsf{S}x = \mathbf{0} & \text{by Lemma 2.4 of [1]} \\ x \in \mathbb{N} & \text{by hypothesis} \\ \mathsf{S}x \neq \mathbf{0} & \text{by Theorem 3.8} \end{array}$$

That disposes of Case 1. (Note the necessity of including $x \in \mathbb{N}$ as a hypothesis of the lemma; we cannot rule out the strange possibility that $\mathsf{S}x$ might be $\mathbf{0}$ for some x that is not a Church number.)

Case 2, the other disjunction of the definition of Z holds with $z := \langle \{\mathsf{S}x\}, y\rangle$. Then it is a straightforward ten steps (which we omit here) to deduce the conclusion of the lemma. That completes the proof of the lemma.

Definition 19.11. *Two subsets x and y of $\mathbb{N}$ are* **comparable***:*

$$comp\,(x, y) := x \subseteq \mathbb{N} \ \wedge \ y \subseteq \mathbb{N} \ \wedge \ \neg\neg\,(x \subseteq y \ \vee \ y \subseteq x).$$

Remark. Comparability is symmetric and reflexive, but not transitive. Perhaps this would have worked without the double negation, but it certainly does work with the double negation.

Lemma 19.12. *Suppose $\langle \{x\}, y\rangle \in \mathbb{B}$ and y is comparable to every element in the rangle of $\mathbb{B}$ and*

$$\forall z\, \langle \{x\}, z\rangle \in \mathbb{B} \to y = z.$$

Then $y \cup \{\mathsf{S}x\}$ is comparable to every element in the range of $\mathbb{B}$.

Remark. Functionality at $\{x\}$ and comparability at y imply comparability at $y \cup \{\mathsf{S}x\}$.

Proof. Suppose $\langle \{x\}, y\rangle \in \mathbb{B}$ and $\langle \{u\}, p\rangle \in \mathbb{B}$. Then $comp\,(y, p)$, by the first hypothesis. We must show $comp\,(y \cup \{\mathsf{S}x\}, p)$. It suffices to prove it from

$$x = u \ \vee x \neq u \to y \subseteq p \ \vee \ p \subseteq y \to comp\,(y \cup \{\mathsf{S}x\}, p),$$

since double-negating that statement yields the desired

$$comp\,(y, p) \to comp\,(y \cup \{\mathsf{S}x\}, p).$$

Therefore we may assume

$$\begin{array}{lrl} (44) & x = u \ \vee x \neq u & \text{assumption} \\ & y \subseteq p \ \vee \ p \subseteq y & \text{assumption} \end{array}$$

We argue by cases accordingly to prove $comp\,(y \cup \{\mathsf{S}x\}, p)$.

Case 1, $p \subseteq y$. Then $p \subseteq y \cup \{\mathsf{S}x\}$, done.

Case 2. $y \subseteq p$. Then

$$\begin{array}{lrl} & x \in y & \text{by Lemma 19.5} \\ & x \in p & \text{since } y \subseteq p \\ & x \neq u \to \mathsf{S}x \in p & \text{by Lemma 19.5} \\ (45) & x \neq u \to y \cup \{\mathsf{S}x\} \subseteq p & \text{since } y \subseteq p \\ & x = u \ \vee x \neq u & \text{by (44)} \end{array}$$

We argue by cases accordingly.

Case 1, $x = u$. Then $\langle \{x\}, y\rangle \in \mathbb{B}$ and $\langle \{x\}, p\rangle \in \mathbb{B}$. So by hypothesis $y = p$. Then $p \subseteq y \cup \{\mathsf{S}x\}$, so $comp\,(y, p)$.

Case 2, $x \neq u$. Then

$$\begin{array}{rl} y \cup \{\mathsf{S}x\} \subseteq p & \text{by (45)} \\ comp\,(y \cup \{\mathsf{S}x\}, p & \text{by the definition of } comp \text{ and logic} \end{array}$$

That completes the proof of the lemma.

Lemma 19.13. *Assume* $\mathbb{N} \not\in \mathsf{FINITE}$*. Suppose* $x \in \mathbb{N}$ *and*

$$\langle \{x\}, y\rangle \in \mathbb{B}$$

$$\forall t, u\,(\langle \{t\}, u\rangle \in \mathbb{B} \to comp\,(y, u) \tag{46}$$

$$\forall z\,\langle \{x\}, z\rangle \in \mathbb{B} \to y = z \tag{47}$$

$$\forall t, u\,(\langle \{t\}, u\rangle \in \mathbb{B} \to t = x \ \vee \ t \neq x) \tag{48}$$

$$\langle \{\mathsf{S}x\}, u\rangle \in \mathbb{B}$$

$$\langle \{\mathsf{S}x\}, v\rangle \in \mathbb{B}. \tag{49}$$

Then $u = v$*.*

Remark. It may help to attach names to the formulas.
(46) is "comparability".
(47) is "functionality".
(48) is "domain decidability".
Then the lemma says: Functionality at $\{x\}$ and domain decidability at x and comparability at y imply functionality at $\{\mathsf{S}x\}$.

Proof.

$$\begin{array}{rl} u = p \cup \{\mathsf{S}t\} \ \wedge \ \mathsf{S}t = \mathsf{S}x \ \wedge \ \langle \{t\}, p\rangle \in \mathbb{B} & \text{by Lemma 19.10} \\ v = q \cup \{\mathsf{S}r\} \ \wedge \ \mathsf{S}r = \mathsf{S}x \ \wedge \ \langle \{r\}, q\rangle \in \mathbb{B} & \text{by Lemma 19.10} \\ \langle \{\mathsf{S}x\}, y \cup \{\mathsf{S}x\}\rangle \in \mathbb{B} & \text{by Lemma 19.3} \\ \langle \{x\}, y\rangle \in \mathbb{B} & \text{by hypothesis} \\ \mathsf{S}x \not\in y & \text{by Lemma 19.6, since } \mathbb{N} \not\in \mathsf{FINITE} \\ comp\,(y, p) & \text{by hypothesis, since } \langle \{t\}, p\rangle \in \mathbb{B} \end{array}$$

By Lemma 19.5, y is closed under successor except x, and p is closed under successor except t, and q is closed under successor except r. Explicitly,

$$\forall z \in y\,(z \neq x \to \mathsf{S}z \in y) \tag{50}$$

$$\forall z \in p\,(z \neq t \to \mathsf{S}z \in p) \tag{51}$$

$$\forall z \in q\,(z \neq r \to \mathsf{S}z \in q) \tag{52}$$

Now I say that

$$t = x \tag{53}$$

By (48), we have $t \in x \ \vee \ t \neq x$. In case $t = x$, we have (53) immediately; so we may assume

$$t \neq x \tag{54}$$

We must derive a contradiction. I say that $t \notin y$:

$$\begin{array}{rl} t \in y & \text{assumption, for contradiction} \\ \mathsf{S}t \in y & \text{by (50) and (54)} \\ \mathsf{S}x \in y & \text{since } \mathsf{S}x = \mathsf{S}t \\ \mathsf{S}x \notin y & \text{as shown above} \end{array}$$

Therefore $t \notin y$, as claimed. Similarly $x \notin p$. We have

$$\begin{array}{rl} t \in p & \text{by Lemma 19.5} \\ \neg\,(p \subseteq y) & \text{since } t \notin y \\ x \in y & \text{by Lemma 19.5} \\ \neg\,(y \subseteq p) & \text{since } x \notin p \\ \neg\,(p \subseteq y \ \vee\ y \subseteq p) & \text{by logic} \\ \neg\,(y \subseteq p \ \vee\ p \subseteq y) & \text{by logic} \\ \neg\, \mathit{comp}\,(y,p) & \text{by the definition of } \mathit{comp} \end{array}$$

But we have derived $\mathit{comp}\,(y,p)$ above. That contradiction completes the proof of (53), namely $t = x$.

Proceeding, we have

$$\begin{array}{rl} \langle \{x\}, y\rangle \in \mathbb{B} & \text{by hypothesis} \\ \langle \{t\}, p\rangle \in \mathbb{B} & \text{derived above} \\ \langle \{x\}, p\rangle \in \mathbb{B} & \text{since } t = x \\ y = p & \text{by the functionality hypothesis} \end{array}$$

Interchanging r for t and q for p, and using (52) instead of (51), we similarly derive $r = x$ and $y = q$. Then $t = r$, since both are equal to x, and $p = q$, since both are equal to y. Then $u = v$, since

$$u = p \cup \{\mathsf{S}t\} = q \cup \{\mathsf{S}r\} = v.$$

That completes the proof of the lemma.

Lemma 19.14. *Assume* $\mathbb{N} \notin \mathsf{FINITE}$. *Suppose* $x \in \mathbb{N}$ *and* $\langle \{x\}, y\rangle \in \mathbb{B}$ *and*

$$\begin{array}{l} \forall t, u\,(\langle \{t\}, u\rangle \in \mathbb{B} \to \mathit{comp}\,(y,u)) \\ \forall z\,\langle \{x\}, z\rangle \in \mathbb{B} \to y = z \\ \forall t, u\,(\langle \{t\}, u\rangle \in \mathbb{B} \to t = x \ \vee\ t \neq x) \\ \langle \{\mathsf{S}x\}, u\rangle \in \mathbb{B} \end{array}$$

Then

$$\forall t, q\,(\langle \{t\}, q\rangle \in \mathbb{B} \to \mathsf{S}x = t \vee \mathsf{S}x \neq t).$$

Remark. This lemma adds to Lemma 19.13 by extending "domain decidability" from x to $\mathsf{S}x$.

Proof.

$$
\begin{array}{rl}
\langle\{t\}, q\rangle \in \mathbb{B} & \text{assumption} \\
\langle\{x\}, y\rangle \in \mathbb{B} & \text{hypothesis} \\
\mathsf{S}x \notin y & \text{by Lemma 19.6} \\
\langle\{\mathsf{S}x\}, y \cup \{\mathsf{S}x\}\rangle \in \mathbb{B} & \text{by Lemma 19.3} \\
t \in \mathbb{N} & \text{by Lemma 19.4} \\
x \in \mathbb{N} & \text{by Lemma 19.4} \\
\langle\{\mathsf{S}x\}, z\rangle \in \mathbb{B} \to z = y \cup \{\mathsf{S}x\} & \text{by Lemma 19.13}
\end{array}
$$

By Lemma 3.10, $t = \mathbf{0} \ \vee \ t \neq \mathbf{0}$. We argue by cases accordingly.

Case 1, $t = \mathbf{0}$. Then $\mathsf{S}x \neq t$, by Theorem 3.8. That completes Case 1.

Case 2, $t \neq \mathbf{0}$. Then

$$
\begin{array}{rl}
t = \mathsf{S}m & \text{for some } m \in \mathbb{N}\text{, by Lemma 3.9} \\
\langle\{\mathsf{S}m\}, q\rangle \in \mathbb{B} & \text{since } \langle\{t\}, q\rangle \in \mathbb{B} \\
m = x \ \vee \ m \neq x & \text{by (55)}
\end{array}
$$

Case 2a, $m = x$. Then $\mathsf{S}x = \mathsf{S}m$, so we are done.

Case 2b, $m \neq x$. I say that $\mathsf{S}x \neq \mathsf{S}m$. Suppose $\mathsf{S}x = \mathsf{S}m$. Then

$$
\begin{array}{rl}
\langle\{\mathsf{S}m\}, q\rangle \in \mathbb{B} & \\
\langle\{\mathsf{S}x\}, q\rangle \in \mathbb{B} & \text{since } \mathsf{S}x = \mathsf{S}m \\
\langle\{\mathsf{S}x\}, y \cup \{\mathsf{S}x\}\rangle \in \mathbb{B} & \\
q = y \cup \{\mathsf{S}x\} & \text{by Lemma 19.13} \\
\langle\{x\}, y\rangle \in \mathbb{B} & \text{by hypothesis} \\
\langle\{m\}, u\rangle \in \mathbb{B} & \text{for some } u \in \mathbb{N}\text{, by Lemma 19.7} \\
m \in u & \text{by Lemma 19.5} \\
\mathsf{S}m \notin u & \text{by Lemma 19.6} \\
\langle\{\mathsf{S}m\}, u \cup \{\mathsf{S}m\}\rangle \in \mathbb{B} & \text{by Lemma 19.3} \\
\langle\{\mathsf{S}x\}, u \cup \{\mathsf{S}x\}\rangle \in \mathbb{B} & \text{since } \mathsf{S}x = \mathsf{S}m \\
u \cup \{\mathsf{S}x\} = y \cup \{\mathsf{S}x\} & \text{by Lemma 19.13} \\
\mathsf{S}x \notin y & \text{by Lemma 19.6, since } \langle\{x\}, y\rangle \in \mathbb{B} \\
\mathsf{S}m \notin u & \text{by Lemma 19.6, since } \langle\{m\}, u\rangle \in \mathbb{B} \\
\mathsf{S}x \notin u & \text{since } \mathsf{S}x = \mathsf{S}m \\
u = y & \text{since } u \cup \{\mathsf{S}x\} = y \cup \{\mathsf{S}x\} \\
m \in y & \text{since } m \in u \text{ and } u = y \\
\forall q \in y\, (q \neq x \to \mathsf{S}q \in y) & \text{by Lemma 19.5, since } \langle\{x\}, y\rangle \in \mathbb{B} \\
\mathsf{S}m \in y & \text{since } m \neq x \text{ and } m \in y \\
\mathsf{S}x \in y & \text{since } \mathsf{S}x = \mathsf{S}m \\
\mathsf{S}x \notin y & \text{as proved above, by Lemma 19.6}
\end{array}
$$

That contradiction completes the proof that $\mathsf{S}x \neq \mathsf{S}m$. That completes Case 2b. That completes Case 2. That completes the proof of the lemma.

Now we are in a position to prove $\mathbb{B} \in \mathsf{FUNC}$; that is, the value y such that $\langle\{\mathsf{S}x\}, y\rangle \in \mathbb{B}$ is uniquely determined by $\mathsf{S}x$. We prove this property simultaneously with the property that equality is decidable between x and any element of the domain of $\mathbb{B}$, and y is comparable to any element of the range of $\mathbb{B}$. The last three lemmas together have the information needed to carry out the induction step.[6]

Lemma 19.15. *Assume* $\mathbb{N} \not\in \mathsf{FINITE}$. *Then* $\mathbb{B}$ *is a functional relation, in the sense that if* $\langle\{x\}, y\rangle \in \mathbb{B}$ *and* $\langle\{x\}, z\rangle \in \mathbb{B}$, *then* $y = z$.

Proof. As described above, we actually prove a more complicated proposition. Namely, the conjunction of these three:

$$\begin{array}{rl} \text{functionality} & \forall y, z\, \langle\{x\}, y\rangle \in \mathbb{B} \to \langle\{x\}, z\rangle \in \mathbb{B} \to y = z \\ \text{domain decidability} & \forall y, p, t\, \langle\{x\}, y\rangle \in \mathbb{B} \to \langle\{t\}, p\rangle \in \mathbb{B} \to x = t \ \vee \ x \neq t \\ \text{comparability} & \forall y, p, t\, \langle\{x\}, y\rangle \in \mathbb{B} \to \langle\{t\}, p\rangle \in \mathbb{B} \to \mathit{comp}\,(y, p) \end{array}$$

These formulas are all stratified, giving x and t index 0 and y, z, and p index 1. Therefore we may proceed by induction.

Base case, $x = \mathbf{0}$. By Lemma 19.9, we have $\langle\{\mathbf{0}\}, y\rangle \in \mathbb{B}$ if and only if $y = \{\mathbf{0}\}$. That takes care of functionality when $x = \mathbf{0}$. By Lemma 3.10, we have $t \in \mathbb{N} \to \mathbf{0} = t \ \vee \ \mathbf{0} \neq t$. That takes care of domain decidability when $x = \mathbf{0}$. To prove comparability, it suffices by Lemma 19.9 to prove that $\{\mathbf{0}\}$ is comparable to any y such that $\langle\{x\}, y\rangle \in \mathbb{B}$ for some x, y. But any such y contains $\mathbf{0}$, by Lemma 19.5. Therefore $\{\mathbf{0}\} \subseteq y$. Therefore $\mathit{comp}\,(\{\mathbf{0}\}, y)$. That completes the base case.

Induction step. We will use the three lemmas 19.12, 19.13, and 19.14 to carry out the induction step. We will spell out the logic explictly here. To that end, let A, B, and C be the three sets, respectively, of x satisfying functionality, domain decidability, and comparability, as explicitly written about above. Let $Z := A \cap B \cap C$. Then the induction hypotheses is $x \in X$. We have

$$\begin{array}{rl} x \in Z \to \mathsf{S}x \in A & \text{by Lemma 19.13} \\ x \in Z \to \mathsf{S}x \in B & \text{by Lemma 19.14} \\ x \in Z \to \mathsf{S}x \in A \to \mathsf{S}x \in C & \text{by Lemma 19.12} \end{array}$$

Combining these three implications, we have $x \in Z \to \mathsf{S}x \in Z$. Note that the induction step for A is used again in proving the induction step for C. Let us look at that part of the argument, i.e., at the third implication listed above.

$$\begin{array}{rl} \langle\{\mathsf{S}x\}, y\rangle \in \mathbb{B} & \text{assumption} \\ \langle\{t\}, p\rangle \in \mathbb{B} & \text{assumption} \\ \langle\{x\}, u\rangle \in \mathbb{B} & \text{for some } u\text{, by Lemma 19.7} \\ \langle\{\mathsf{S}x\}, u \cup \{\mathsf{S}x\}\rangle & \text{by Lemma 19.3} \end{array}$$

and we have to prove $\mathit{comp}\,(y, p)$. We have

$$\mathsf{S}x \not\in u \qquad \text{by Lemma 19.6}$$

[6] If any readers think this proof is too complicated, I can assure them there are several simpler "proofs" that are not correct. This one may be complicated, but it *is* correct. It is, however, annoying that the picture is so much simpler than the proof. At least a part of the problem is that we do not have decidability of equality on $\mathbb{N}$ at this point.

Then the crucial step is

$$y = u \cup \{\mathsf{S}x\}$$

which comes from the induction step for functionality, i.e. $\mathsf{S}x \in A$. Then we have

$$\begin{array}{rl}
\forall z\,(\langle\{x\}, z\rangle \in \mathbb{B} \to u = z) & \text{since } x \in A \\
\forall r, p\,(\langle\{r\}, p\rangle \in \mathbb{B} \to comp\,(u, p) & \text{since } x \in C \\
comp\,(u \cup \{\mathsf{S}x\}, p) & \text{by Lemma 19.12} \\
comp\,(y, p) & \text{since } y = u \cup \{\mathsf{S}x\}
\end{array}$$

That is the desired goal of the third implication.

The first two implications are straightforward applications of the lemmas; they take about 100 "bookkeeping" steps, which we omit here. That completes the proof of the lemma.

Remark. The original plan was to prove that $\mathbb{B}$ is the graph of a function, and then introduce the function itself by a comprehension term, so that

$$\begin{aligned}
\mathcal{J}(\{\mathbf{0}\}) &= \{\mathbf{0}\} \\
\mathcal{J}(\{\mathsf{S}x\}) &= \mathcal{J}(x) \cup \{\mathsf{S}x\}
\end{aligned}$$

That is now easily done; but we do not do it, because from this point we can reach the main theorem directly from $\mathbb{B}$.

Theorem 19.16. *Suppose* $\mathbb{N}$ *is not finite. Then Church successor is weakly one-to-one on* $\mathbb{N}$*, in the sense that*

$$x \neq y \to \mathsf{S}x \neq \mathsf{S}y,$$

and $\mathbb{N}$ *is (therefore) infinite.*

Proof. Suppose $x \in \mathbb{N}$ and $t \in \mathbb{N}$ and $\mathsf{S}x = \mathsf{S}t$. and $x \neq t$. We must derive a contradiction. We have

$$\begin{array}{rl}
\langle\{x\}, y\rangle \in \mathbb{B} & \text{for some } y\text{, by Lemma 19.7} \\
\mathsf{S}x \notin y & \text{by Lemma 19.6} \\
\langle\{\mathsf{S}x\}, y \cup \{\mathsf{S}x\}\rangle \in \mathbb{B} & \text{by Lemma 19.3} \\
\langle\{t\}, p\rangle \in \mathbb{B} & \text{for some } p\text{, by Lemma 19.7} \\
\mathsf{S}t \notin p & \text{by Lemma 19.6} \\
\langle\{\mathsf{S}t\}, p \cup \{\mathsf{S}t\}\rangle \in \mathbb{B} & \text{by Lemma 19.3} \\
\langle\{\mathsf{S}x\}, p \cup \{\mathsf{S}x\}\rangle \in \mathbb{B} & \text{since } \mathsf{S}t = \mathsf{S}x \\
\mathsf{S}x \in \mathbb{N} & \text{by Lemma 2.19} \\
\mathsf{S}t \in \mathbb{N} & \text{by Lemma 2.19} \\
p \cup \{\mathsf{S}x\} = y \cup \{\mathsf{S}x\} & \text{by Lemma 19.15} \\
\mathsf{S}x \notin p & \text{since } \mathsf{S}t \notin p \text{ and } \mathsf{S}x = \mathsf{S}t \\
\mathsf{S}x \notin y & \text{proved above} \\
p = y & \text{by the preceding three lines}
\end{array}$$

Now by Lemma 19.5, y is closed under successor except x, and p is closed under successor except t. Explicitly,

$$\begin{array}{rl}
\forall u \in y\,(u \neq x \to \mathsf{S}u \in y) & \text{by Lemma 19.5} \\
\forall u \in p\,(u \neq t \to \mathsf{S}u \in p) & \text{by Lemma 19.5} \\
y \in \mathsf{FINITE} & \text{by Lemma 19.4} \\
y \in \mathsf{DECIDABLE} & \text{by Lemma 3.3 of [1]} \\
x \in y & \text{by Lemma 19.5} \\
x \in p & \text{since } y = p \\
t \in y & \text{since } t \in p \text{ and } y = p \\
\mathbf{0} \in y & \text{by Lemma 19.5} \\
t = x \ \vee \ t \neq x & \text{since } y \in \mathsf{DECIDABLE}
\end{array}$$

Now I say that y is closed under successor. To prove that, suppose $u \in y$. We have to prove $\mathsf{S}u \in y$. Since $y \in \mathsf{DECIDABLE}$, we have

$$u = x \ \vee u \neq x.$$

We argue by cases accordingly.

Case 1, $u = x$. Then

$$\begin{array}{rl}
x \neq t & \text{by hypothesis} \\
p = y & \text{proved above} \\
\mathsf{S}x \in y & \text{since } p \text{ is closed under successor except } t \text{ and } y = p
\end{array}$$

That completes Case 1.

Case 2, $u \neq x$. Since y is closed under successor except x, we have $\mathsf{S}u \in y$. That completes Case 2. That completes the proof that y is closed under successor.

Now we have proved that y contains $\mathbf{0}$ and is closed under successor. By definition of $\mathbb{N}$, we have $\mathbb{N} \subseteq y$. By Lemma 19.4, we have $y \subseteq \mathbb{N}$. Hence $y = \mathbb{N}$. But $y \in \mathsf{FINITE}$ and $\mathbb{N} \notin \mathsf{FINITE}$. That contradiction completes the proof of the theorem.

Corollary 19.17. *If $\mathbb{N}$ is not finite, then $\mathbb{N}$ has decidable equality.*

Proof. We prove by induction on x that

$$\forall y \in \mathbb{N}\,(x = y \ \vee \ x \neq y). \tag{55}$$

The base case is Lemma 3.10. For the induction step, the induction hypothesis is (55). We have to prove $\mathsf{S}x = y \ \vee \ \mathsf{S}x \neq y$. Let $y \in \mathbb{N}$ be given. By Lemma 3.10, $y = 0 \ \vee \ y \neq 0$. If $y = 0$ then we are done by Lemma 3.10 (or by Theorem 3.8), so we may assume $y \neq 0$. Then by Lemma 3.9, $y = \mathsf{S}z$ for some $z \in \mathbb{N}$. Then we have to prove $\mathsf{S}x = \mathsf{S}z \ \vee \ \mathsf{S}x \neq \mathsf{S}z$. By (55), we have $x = z \ \vee x \neq z$. We argue by cases.

Case 1, $x = z$. Then $\mathsf{S}x = \mathsf{S}z$. That completes Case 1.

Case 2, $x \neq z$. Then by Theorem 19.16, $\mathsf{S}x \neq \mathsf{S}z$. That completes Case 2. That completes the proof of the lemma.

Theorem 19.18. *If $\mathbb{N}$ is not finite, then Church successor is one-to-one.*

Proof. Suppose $\mathbb{N}$ is not finite. Suppose $x \in \mathbb{N}$ and $y \in \mathbb{N}$, and $\mathsf{S}x = \mathsf{S}y$. We must show $x = y$. By Theorem 19.16, we have $\neg\neg(x = y)$. By Corollary 19.17, $\mathbb{N}$ has decidable equality. Therefore $x = y$. That completes the proof.

Theorem 19.19. *If $\mathbb{N}$ is not finite, then $\mathbb{N}$ is infinite.*

Proof. Suppose $\mathbb{N} \notin \mathsf{FINITE}$. Define $Z := \mathbb{N} - \{\mathbf{0}\}$. By Theorem 3.8, Z is a proper subset of $\mathbb{N}$. By Lemma 3.9, Church successor maps $\mathbb{N}$ onto Z. By Theorem 19.18, Church successor is one-to-one; therefore it is a similarity from $\mathbb{N}$ to Z. One can verify straightforwardly that Church successor is a similarlity between $\mathbb{N}$ and Z (120 steps omitted here). By the definition of infinite, $\mathbb{N}$ is infinite. That completes the proof of the theorem.

Theorem 19.20. *The Church counting axiom implies $\mathbb{N}$ is infinite and Church successor is one-to-one.*

Proof. By Theorem 18.6, the Church counting axiom implies $\mathbb{N}$ is not finite. Then by Theorem 19.19, $\mathbb{N}$ is infinite. By Theorem 19.18, Church successor is one-to-one. That completes the proof of the theorem.

Theorem 19.21. *Heyting's arithmetic HA can be interpreted in INF plus the Church counting axiom.*

Remark. Since this is a meta-theorem, not a theorem of INF, we have not checked it in Lean as we did all the other proofs in this paper.

Proof. We have already shown in [1] that one may conservatively add comprehension terms to INF. We have defined Church successor, Church addition, and Church multiplication by such comprehension terms. The interpretation of a formula A of HA is defined by replacing the function terms of A by comprehension terms involving the symbols for Church successor, addition, and multiplication, and the constant 0 of HA by the comprehension term defining $\mathbf{0}$. The quantifiers of A are replaced by bounded quantifiers restricted to $\mathbb{N}$, which is defined by a comprehension term. The interpretations of the axioms for addition and multiplication hold, by Lemmas 7.4, 7.5, 15.7, 15.8, 4.5, and 4.4. The interpretation of any formula of HA is a stratified formula, giving all the variables index 0, so the interpretation of the induction axiom schema follows from the definition of $\mathbb{N}$. The main point of interest is that we need Theorem 19.18 to verify that successor is one-to-one. That completes the proof of the theorem.

20. If $\mathbb{F}$ is infinite, so is $\mathbb{N}$

The plan of this section is to prove that (assuming $\mathbb{F}$ is infinite), every Church number is the order of a cyclic permutation on some finite set. Then if $\mathbb{N}$ is finite, we have $\mathsf{S}\mathbf{n} = \mathsf{S}k$ with $\mathbf{n} = \mathbf{k} + \mathbf{m}$ and $\mathbf{m} \neq \mathbf{0}$, so $\mathbf{m}$ has a predecessor r. Then there is a finite set X and cyclic permutation f of X whose order is r. Then $\mathbf{m}fx = \mathsf{S}rfx = f(rfx) = fx$. But by the Annihilation Theorem, $\mathbf{m}fx = x$, contradiction, since a cyclic permutation is not the identity. While this proof is conceptually simple, there are many details to supply.

Lemma 20.1. *Suppose Frege successor maps $\mathbb{F}$ to $\mathbb{F}$. Then for every finite set X, not-not there exists c with $c \notin X$.*

Remark. That is, every finite set is not-not enlargeable, as $X \cup \{c\}$ is a finite set properly containing X. We were not able to eliminate the double negation (which would have simplified the subsequent arguments).

Proof. Let $p = Nc(X)$. Then

$$\begin{array}{rl} p \in \mathbb{F} & \text{by Lemma 4.21 of [1]} \\ p^+ \in \mathbb{F} & \text{since } \mathbb{F} \text{ is closed under successor, by hypothesis} \\ u \in p^+ & \text{for some } u\text{, by Lemma 4.7 of [1]} \\ u \in \mathsf{FINITE} & \text{by Lemma 4.9 of [1]} \end{array}$$

By the definition of Frege successor, there exist v and c such that $u = v \cup \{c\}$, $v \in p$, and $c \notin v$. Then

$$\begin{array}{rl} X \in p & \text{by Lemma 4.11 of [1]} \\ X \sim v & \text{by Lemma 4.9 of [1]} \end{array}$$

I say $u \not\subseteq X$. To prove that, assume $u \subseteq X$. Then

$$\begin{array}{rl} c \in u & \text{since } u = v \cup \{c\} \\ c \in X & \text{since } u \subseteq X \\ v \neq X & \text{since } c \notin v \text{ and } c \in X \\ v \subseteq X & \text{since } v \subseteq u \text{ and } u \subseteq X \\ X \text{ is infinite} & \text{by Definition 3.23 of [1]} \\ X \in \mathsf{FINITE} & \text{by hypothesis} \end{array}$$

But then X is both finite and infinite, contradicting Theorem 3.24 of [1]. That completes the proof that $u \not\subseteq X$.

By Lemma 4.21 of [1], since $u \in p^+$ and $p^+ \in \mathbb{F}$, we have $u \in \mathsf{FINITE}$. Recall that we can move double negation both ways across a finite universal quantifier:

$$\forall z \in u \neg\neg (z \in X) \to \neg\neg \forall z \in u(z \in X) \qquad \text{by Lemma 3.28 of [1]}$$

and double negation moves in the other direction by pure logic. Using these facts we have

$$\begin{array}{rl} \neg \forall z \in u \, (z \in X) & \text{by the definition of } \subseteq \\ \neg \forall z \in u \neg\neg (z \in X) & \text{by Lemma 3.28 of [1], since } u \text{ and } X \text{ are finite} \\ \neg\neg \exists z \in u \neg (z \in X) & \text{by logic} \end{array}$$

That completes the proof of the lemma.

For convenience we repeat Definition 3.1.

Definition 20.2. *f is a* **permutation** *of a finite set X if and only if $f : X \to X$, and $Rel(f)$ and $f \in \mathsf{FUNC}$, and $dom(f) \subseteq X$, and f is both one-to-one and onto from X to X.*

Definition 20.3. *f is a* **cyclic permutation** *of a finite set X with* **generator** *a if f is a permutation of X and $a \in X$ and*

$$\forall z \in X \, \exists r \in \mathbb{N} \, (z = rfa).$$

Definition 20.4. *Let X be a finite set and let $f : X \to X$ be a cyclic permutation of X with generator a. Suppose $q \in \mathbb{N}$ and $qfa = a$ and q is the $\preceq$-least such Church number, i.e.,*

$$\forall r \in \mathbb{N}\,(r \preceq q \to (\forall x\,(rfx = x)) \to r = q).$$

Suppose also that

$$\forall x \in X\, \exists r \in \mathbb{N}\,(r \preceq q \ \wedge\ rfa = x).$$

Then q is the **order** *of f.*

Remark. The second condition is usually omitted, and could also be omitted in this context, but then we would have to prove that when we divide x by y, the remainder is $\prec y$. That can be done, but it is easier to just use this stronger definition of "order."

Lemma 20.5. *Let X be a finite set and let $f : X \to X$ be a cyclic permutation of X with generator a. Let $q \in \mathbb{N}$ and suppose $qfa = a$. Then $\forall x \in X\,(qfx = x)$.*

Proof. Let $x \in X$. Since f is a cyclic permutation with generator a, we have $x = jfa$ for some $j \in \mathbb{N}$. Suppose $qfa = a$. Then

$$\begin{aligned}
qfx &= qf(jfa) && \text{since } x = jfa\\
&= (q \oplus j)fa && \text{by Lemma 7.6}\\
&= (j \oplus q)fa && \text{since } \oplus \text{ is commutative}\\
&= jf(qfa) && \text{by Lemma 7.6}\\
&= jfa && \text{since } qfa = a\\
&= x && \text{since } x = jfa
\end{aligned}$$

Lemma 20.6. *Suppose X is a finite set, $f : X \to X$ is a cyclic permutation of X with generator a, and $c \notin X$. Suppose $\mathbb{N}$ is finite with $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ and $k \in \mathsf{STEM}$. Let q be the order of f. Suppose $q \neq \mathbf{n}$ and $q \neq \mathbf{0}$. Then there is a cyclic permutation g of $X \cup \{c\}$ with generator a and order $\mathsf{S}q$.*

Proof. Let a be a generator of f. Let $b = f^{-1}(a)$, so $a = f(b)$. Define

$$g = f - \{\langle b, a\rangle\} \cup \{\langle b, c\rangle\} \cup \{\langle c, a\rangle\}.$$

Using functional notation may clarify the idea of the definition of g, although we are not legally entitled to do so until we prove that g is a function.

$$g(x) = \begin{cases} f(x) & \text{if } x \neq b \ \wedge\ x \neq c\\ c & \text{if } x = b\\ a & \text{if } x = c \end{cases}$$

Then g is a permutation of $X \cup \{c\}$. The formal proof of that fact requires about 850 steps, since there are several cases in the definition of "permutation", and three cases in the definition of g, making nine cases for each case in the definition of "permutation". We omit those 850 steps.

Since $q \neq \mathbf{0}$, by Lemma 14.19 there exists $t \in \mathbb{N}$ with

$$\mathsf{S}t = q \ \wedge\ t \neq \mathbf{n}. \tag{56}$$

I say that

$$r \prec t \to rga = rfa \ \wedge\ rfa \neq b \tag{57}$$

$$tfa = tga = b \tag{58}$$

In spite of the intuitive conviction that a simple picture of the situation provides, the proofs of these assertions are not short; and unlike the proof that g is a permutation, they are not particularly straightforward or obvious. To keep the length and logical complexity of proofs manageable, we prove these formulas in three separate lemmas. Logically those lemmas should come before this one, but for readability we postpone them. We will first finish this proof under the additional assumptions (57) and (58).

We then have

$$\begin{array}{rll} & tfa \in X & \text{by Lemma 12.6} \\ & f(tfa) = f(b) & \text{by (58)} \\ & \mathsf{S}tfa = f(b) & \text{by Theorem 3.6} \\ & qfa = f(b) & \text{since } \mathsf{S}t = q \\ (59) & qfa = a & \text{since } f(b) = a \end{array}$$

Similarly,

$$\begin{array}{rll} & tga \in X \cup \{c\} & \text{by Lemma 12.6} \\ & g(tga) = g(b) & \text{by (58)} \\ & \mathsf{S}tga = g(b) & \text{by Theorem 3.6} \\ & qga = g(b) & \text{since } \mathsf{S}t = q \\ (60) & qga = c & \text{since } g(b) = c \\ & g(qga) = g(c) & \text{by the preceding line} \\ & \mathsf{S}qga = g(c) & \text{by Theorem 3.6} \\ (61) & \mathsf{S}qga = a & \text{since } g(c) = a \end{array}$$

We must prove that g is a cyclic permutation of $X \cup \{c\}$ with generator a and order $\mathsf{S}q$. Let $z \in X \cup \{c\}$. We must show that $z = rga$ for some $r \in \mathbb{N}$ with $r \preceq \mathsf{S}q$. We have

$$\begin{array}{rl} X \in \mathsf{FINITE} & \text{by hypothesis} \\ X \cup \{c\} \in \mathsf{FINITE} & \text{by Lemma 3.7} \\ X \cup \{c\} \in \mathsf{DECIDABLE} & \text{by Lemma 3.3} \\ z = a \ \vee \ z \neq a & \text{by definition of } \mathsf{DECIDABLE} \\ z = c \ \vee \ z \neq c & \text{by definition of } \mathsf{DECIDABLE} \end{array}$$

If $z = a$ we take $r = \mathbf{0}$; then $rga = a = z$. If $z = c$ we take $r = q$; then by (60) we have $rga = qga = c = z$. Therefore we may assume

(62) $$z \neq a \ \wedge \ z \neq c$$

Since $z \in X \cup \{c\}$ and $z \neq c$, we have $z \in X$. Since f is a cyclic permutation of X of order q, there exists $r \preceq q$ such that $z = rfa$. By Theorem 14.16, we have $r \prec t \ \vee \ r = t \ \vee \ t \prec r$. I say first that

(63) $$r \neq t$$

Case 1, $r \prec t$. Then

$$\begin{array}{rl} rga = rfa \ \wedge \ rfa \neq b & \text{by (57)} \\ z = rga & \text{since } z = rfa \text{ and } rga = rfa \\ q \prec \mathsf{S}q & \text{by Lemma 14.11} \\ r \preceq \mathsf{S}q & \text{by Lemma 14.6, since } r \preceq q \end{array}$$

That completes Case 1.

Case 2, $r = t$. Then

$$\begin{array}{rl} z = tfa & \text{since } z = rfa \text{ and } r = t \\ = tga & \text{by (58)} \\ = rga & \text{since } r = t \end{array}$$

It remains to show $r \preceq \mathsf{S}q$. We have

$$\begin{array}{rl} q \neq \mathbf{n} & \text{by hypothesis} \\ \mathsf{S}r \neq \mathbf{n} & \text{since } q = \mathsf{S}t \text{ and } r = t \\ r \neq \mathbf{n} & \text{by (56), since } r = t \\ \mathsf{S}r \preceq \mathsf{SS}r & \text{by Lemma 14.11, since } \mathsf{S}r \neq \mathbf{n} \\ r \preceq \mathsf{S}r & \text{by Lemma 14.11, since } r \neq \mathbf{n} \\ r \preceq \mathsf{SS}r & \text{by Lemma 14.6} \\ r \preceq \mathsf{S}q & \text{since } q = \mathsf{S}t \text{ and } r = t \end{array}$$

That completes Case 2.

Case 3, $t \prec r$. Then

$$\begin{array}{rl} t \neq r \ \wedge \ t \preceq r & \text{by definition of } \prec \\ r \preceq q = \mathsf{S}t & \text{proved above} \\ r \preceq t \ \vee \ r = \mathsf{S}t & \text{by Lemma 14.10, since } t \neq \mathbf{n} \\ \neg\,(r \preceq t) & \text{by Theorem 14.20, since } t \preceq r \text{ and } t \neq r \\ r = \mathsf{S}t & \text{by the preceding two lines} \\ tfa = tga & \text{by (58)} \\ r = q & \text{since } q = \mathsf{S}t \\ z = qfa & \text{since } z = rfa \text{ and } r = q \\ \exists r \preceq q\,(z = rfa) & \text{namely, } r = q \end{array}$$

That completes Case 3.

I say that $\mathsf{S}q$ is the order of g. By (61), $\mathsf{S}qga = a$. Suppose $rga = a$. We must prove $\mathsf{S}q \preceq r$. By Theorem 14.20, it suffices to derive a contradiction from $r \prec \mathsf{S}q$. We now assume $r \prec \mathsf{S}q$

Then by Lemma 14.10, $r \preceq q$. We have

$$\begin{array}{rl} qga = c & \text{by (60)} \\ rga = a & \text{by the definition of order} \\ a \neq c & \text{since } a \in X \text{ but } c \notin X \\ r \neq q & \text{since if } r = q \text{ then } a = c \end{array}$$

$$
\begin{array}{rl}
r \preceq \mathsf{S}t & \text{since } q = \mathsf{S}t \\
r \preceq t \ \vee r = \mathsf{S}t & \text{by Lemma 14.10} \\
r \neq \mathsf{S}t & \text{since } q = \mathsf{S}t \text{ and } r \neq q \\
r \preceq t & \text{by the preceding two lines} \\
rga = a & \text{since } r \text{ is the order of } g \\
tga = b & \text{by (58)} \\
r \neq t & \text{by the preceding lines, since } a \neq b \\
r \prec t & \text{by the definition of } \prec \\
rga = rfa & \text{by (57)} \\
rfa = a & \text{since } rga = a \\
q \preceq r & \text{since } q \text{ is the order of } f \\
q = r & \text{by Theorem 14.20, since } r \preceq q
\end{array}
$$

That contradicts $r \neq q$, which was proved above. We have now proved that if $rga = a$, then $\mathsf{S}q \preceq r$. That is, however, only have the definition of "$\mathsf{S}q$ is the order of g."

We still have to prove that every $x \in X \cup \{c\}$ has the form rga for some $r \preceq \mathsf{S}q$, which is the second part of the definition. Let $x \in X \cup \{c\}$. Since $X \cup \{c\}$ is finite, it has decidable equality, so we have

$$x = c \ \vee \ x = b \ \vee x = a \ \vee \ (x \neq c \ \wedge \ x \neq b \ \wedge \ x \neq a).$$

We argue by cases.

Case 1, $x = c$. Then take $r = q$. We have $qga = c$ by (60), and $q \preceq \mathsf{S}q$ since $q \neq \mathbf{n}$.

Case 2, $x = b$. Then take $r = t$. We have $tga = b$ by (58), and $t \preceq \mathsf{S}t \preceq \mathsf{S}(\mathsf{S}t) = \mathsf{S}q$, since $t \neq \mathbf{n}$ and $q \neq \mathbf{n}$.

Case 3, $x = a$. Then take $r = \mathsf{S}q$. We have $\mathsf{S}qga = a$ by (61).

Case 4, $x \neq c \ \wedge \ x \neq b \ \wedge \ x \neq a$. Then $x \in X$. By the induction hypothesis, q is the order of f, so there exists $\rho \preceq q$ such that $rfa = x$. We have

$$
\begin{array}{rl}
\rho \preceq \mathsf{S}t & \text{since } q = \mathsf{S}t \\
\rho \preceq t \ \vee \ r = \mathsf{S}t & \text{by Lemma 14.10} \\
\rho = t \ \vee \ \rho \neq t & \text{since } \mathbb{N} \in \mathsf{DECIDABLE} \\
\rho \prec t \ \vee \ \rho = t \ \vee \ \rho = \mathsf{S}t & \text{by the definition of } \prec
\end{array}
$$

If $\rho \prec t$ then by (57), $\rho ga = \rho fa = x$, so we can take $r = \rho$. If $\rho = t$ then by (58), then $tga = b$, so $x = b$, contradicting the hypothesis of Case 4. If $\rho = \mathsf{S}t = q$, then $x = \rho ga = qga = c$ by (60), contrary to the hypothesis $x \neq c$ of Case 4. That completes Case 4. That completes the proof that $\mathsf{S}q$ is the order of g. That completes the proof of the lemma, under the assumptions (57) and (58).

Lemma 20.7. *Suppose X is a finite set, $f : X \to X$ is a cyclic permutation of X with generator a, and $c \notin X$. Suppose $\mathbb{N}$ is finite with $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ and $k \in \mathsf{STEM}$. Let q be the order of f. Suppose $q \neq \mathbf{n}$ and $q = \mathsf{S}t$ with $t \neq \mathbf{n}$, and*

$$g = f - \{\langle b, a\rangle\} \cup \{\langle b, c\rangle\} \cup \{\langle c, a\rangle\}.$$

Then

$$r \prec t \to rga = rfa \ \wedge \ rfa \neq b.$$

Proof. The conclusion of the lemma is a stratified formula, giving a and b index 0, f index 3, and t and r index 6. We prove it by induction on r.

Base case, $r = \mathbf{0}$. Then $rga = rfa = a$. If $a = b$ then $f(a) = a$, so f is the identity, contradiction. That completes the base case.

Induction step. We use "finite induction", so we may assume $r \neq \mathbf{n}$.

$\mathsf{S}r \prec t$	assumption
$r \prec \mathsf{S}r$	by Lemma 14.12, since $r \neq \mathbf{n}$
$r \prec t$	by Lemma 14.24
$rga = rfa$	by the induction hypothesis
$g(rga) = g(rfa)$	by the preceding line
$f : X \to X$	by definition of "permutation"
$rf : X \to X$	by Lemma 12.6
$rfa \in X$	since $a \in X$ and $rf : X \to X$
$rfa \neq b$	by the induction hypothesis
$g(rfa) = f(rfa)$	by the definition of g, since $rfa \neq b$
$= \mathsf{S}rfa$	by Theorem 3.6
$\mathsf{S}rga = g(rga)$	by Theorem 3.6
$= \mathsf{S}rfa$	by the preceding lines

It remains to show that $\mathsf{S}rfa \neq b$. We have

$\mathsf{S}rfa = b$	by assumption, for proof by contradiction
$f(\mathsf{S}rfa)) = f(b)$	by the previous line
$f(\mathsf{S}rfa) = a$	since $f(b) = a$
$(\mathsf{SS}r)fa = a$	by Theorem 3.6
$q \preceq \mathsf{SS}r$	since q is the order of f
$\mathsf{S}t \preceq \mathsf{SS}r$	since $\mathsf{S}t = q$
$\neg \mathbf{n} \prec t$	by Lemma 14.22
$\mathsf{S}r \prec t$	as assumed above for the induction step
$\mathsf{S}r \neq \mathbf{n}$	by the preceding two lines
$t \neq \mathbf{n}$	by (56)
$t \preceq \mathsf{S}r$	by Lemma 14.25, since $\mathsf{S}t \preceq \mathsf{SS}r$ and $t \neq \mathbf{n}$
$\mathsf{S}r \preceq t$	by definition of $\prec$, since $\mathsf{S}r \prec t$
$\mathsf{S}r = t$	by Theorem 14.20
$\mathsf{S}r \neq t$	by definition of $\prec$, since $\mathsf{S}r \prec t$

That contradiction completes the proof that $\mathsf{S}rga \neq b$. That completes the induction step. That completes the proof of the lemma.

Lemma 20.8. *Suppose X is a finite set, $f : X \to X$ is a cyclic permutation of X with generator a, and $c \notin X$. Suppose $\mathbb{N}$ is finite with $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ and $k \in \mathsf{STEM}$. Let*

q be the order of f. Suppose $q \neq \mathbf{n}$ and $q = \mathsf{S}t$ with $t \neq \mathbf{n}$, and

$$g = f - \{\langle b, a\rangle\} \cup \{\langle b, c\rangle\} \cup \{\langle c, a\rangle\}.$$

Then $tga = tfa = b$.

Proof.

$z := tfa$	definition of z
$tfa \in X$	by Lemma 12.6
$z \in X$	by the preceding two lines
$fz = f(tfa)$	since $z = tfa$
$fz = \mathsf{S}tfa$	by Theorem 3.6
$fz = qfa$	since $q = \mathsf{S}t$
$fz = a$	since $qfa = a$
$z = b$	since f is one-to-one and $fb = a$
$t \prec \mathsf{S}t$	by Lemma 14.12, since $t \neq \mathbf{n}$
$t \prec q$	since $\mathsf{S}t = q$
$tfa \neq a$	since q is the order of f
$z \neq a$	since $z = tfa$
$t \neq \mathbf{0}$	since if $t = \mathbf{0}$ then $z = tfa = a$
$t = \mathsf{S}p$	for some $p \in \mathbb{N}$ with $p \neq \mathbf{n}$, by Lemma 14.19
$p \prec t$	by Corollary 14.12
$u := pfa$	defining u
$u = pga$	by (57)
$gu = \mathsf{S}pga$	by Theorem 3.6
$= tga$	since $t = \mathsf{S}p$
$fu = f(pfa)$	since $u = pfa$
$= \mathsf{S}pfa$	by Theorem 3.6
$= tfa$	since $\mathsf{S}p = t$
$= z = b$	as shown above
$fu \neq fb$	since $fu = b$ and $fb = a$ and $a \neq b$
$pf : X \to X$	by Lemma 12.6
$u \in X$	since $u = pfa$ and $a \in X$ and $pf : X \to X$
$u \neq b$	since f is one-to-one and $fu \neq fb$
$gu = fu$	by definition of g, since $u \neq b$
$gu = b$	since $fu = b$
$z = b = tga$	since $gu = tga$
$z = rga$	since $r = t$

That completes the proof of the lemma.

Now we have supplied the supporting lemmas required to prove (57) and (58). That completes the proof of Lemma 20.6.

Lemma 20.9. *Let $X = \{a, b\}$, where $a \neq b$. Let $f = \{\langle a, b\rangle, \langle b, a\rangle\}$. Then f is a cyclic permutation with generator a of X with order $\mathsf{S}(\mathsf{S}\mathbf{0})$.*

Remark. There is no cyclic permutation of order $\mathsf{one} = \mathsf{S}\mathbf{0}$, as it would have to fix the generator a, so X would have to be a singleton, and the identity permutation on a singleton has order $\mathbf{0}$.

Proof. We omit the 610 simple steps of this proof. (The definitions involved create many cases.)

Lemma 20.10. *Suppose $\mathbb{N}$ is finite and Frege successor maps $\mathbb{F}$ to $\mathbb{F}$ (so $\mathbb{F}$ is infinite). Let $q \in \mathbb{N}$ with $q \neq \mathbf{0}$ and $q \neq \mathsf{S}\mathbf{0}$. Then not-not there exists a finite set X and a cyclic permutation f of X with generator a and order q.*

Remark. "Every Church number is not-not the order of some permutation." The double negation comes from Lemma 20.1.

Proof. By Lemma 18.3, there exist $\mathbf{k}$ and $\mathbf{n}$ in $\mathbb{N}$ with $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ and $\mathbf{k} \in \mathsf{STEM}$ and $\mathbf{n} \neq \mathbf{k}$. By induction on q we prove that $q \neq \mathbf{0}$ implies not-not q is the order of some cyclic permutation on a finite set. We use "finite induction", which means we get to assume $q \neq \mathbf{n}$ in the induction step.

Base case, there is nothing to prove because of the hypothesis $q \neq \mathbf{0}$.

Induction step. The assumptions for the induction step are

$$\begin{aligned} q &\in \mathbb{N} \\ \mathsf{S}q &\neq \mathbf{0} \\ \mathsf{S}q &\neq \mathsf{S}\mathbf{0} \\ q &\neq \mathbf{n} && \text{for "finite induction"} \end{aligned}$$

Then also

$$q \neq \mathbf{0} \qquad \text{since } \mathsf{S}q \neq \mathsf{S}\mathbf{0}$$

We have to produce a set X and a permutation f of X whose order is $\mathsf{S}q$. If $\mathsf{S}q = \mathsf{S}(\mathsf{S}\mathbf{0})$, or for short $\mathsf{S}q = 2$, then by Lemma 20.9, there is a permutation of order 2, so we are finished. In other words, we may assume

$$q \neq \mathsf{S}\mathbf{0} \qquad \text{by Lemma 20.9}$$

Now that we have $q \neq \mathbf{0}$ and $q \neq \mathsf{S}\mathbf{0}$, we may apply the induction hypothesis. By the induction hypothesis, not-not there is a finite set X and a cyclic permutation of X with generator a such that $xfa = a$, and f has order q. Suppose X is such a set; by Lemma 20.1, not-not there exists $c \notin X$. By Lemma 20.6, not-not there is an X, and a cyclic permutation of $X \cup \{c\}$, such that $\mathsf{S}xfa = a$, and f has order $\mathsf{S}q$. That completes the induction step. That completes the proof of the lemma.

Theorem 20.11. *Suppose Frege successor maps $\mathbb{F}$ to $\mathbb{F}$ (so $\mathbb{F}$ is infinite). Then $\mathbb{N}$ is infinite and Church successor is one-to-one.*

Proof. Suppose Frege successor maps $\mathbb{F}$ to $\mathbb{F}$. We have to prove Church successor is one-to-one. By Theorem 19.18, it suffices to prove that $\mathbb{N}$ is not finite. Suppose $\mathbb{N}$ is finite; we must derive a contradiction. Since we have assumed $\mathbb{N}$ is finite, by Lemma 18.3 there exist $\mathbf{k}$ and $\mathbf{n}$ in $\mathbb{N}$ with $\mathsf{S}\mathbf{k} = \mathsf{S}\mathbf{n}$ and $\mathbf{k} \in \mathsf{STEM}$ and $\mathbf{n} \neq \mathbf{k}$. By Lemma 16.3, there exists $\mathbf{m}$ such that $\mathbf{n} = \mathbf{k} + \mathbf{m}$. Since $\mathbf{n} \neq \mathbf{k}$, we have $\mathbf{m} \neq \mathbf{0}$. By Lemma 3.9, there exists $r \in \mathbb{N}$ with $\mathsf{S}r = \mathbf{m}$. We have $r \neq \mathbf{0}$ and $r \neq \mathsf{S}\mathbf{0}$, by

Lemma 12.2. By Lemma 20.10, not-not there is a finite set X and a permutation $f : X \to X$ with generator a such that $rfa = a$ and $fa \neq a$. Suppose X and f are such a finite set and permutation. Then

$$\begin{aligned} \mathbf{m}fa &= \mathsf{S}rfa && \text{since } \mathbf{m} = \mathsf{S}r \\ &= f(rfa) && \text{by Theorem 3.6} \\ &= f(a) && \text{since } rfx = x \end{aligned}$$

On the other hand, by the Annihilation Theorem, $\mathbf{m}fa = a$. Hence $f(a) = a$, contradiction.

We reached that contradiction under the assumption that X is a finite set with a permutation f of order r; but we have actually proved only the double negation of that. But still, if a proposition leads to a contradiction, so does its double negation. That completes the proof of the theorem.

Corollary 20.12. *Classical NF proves* $\mathbb{N}$ *is infinite and Church successor is one-to-one.*

Proof. Specker [10] proved, in classical NF, that $\mathbb{F}$ is infinite. By Theorem 20.11, Specker's result implies that $\mathbb{N}$ is infinite and Church successor is one-to-one. That completes the proof of the corollary.

Remarks. We also proved that every inhabited finite set has a cyclic permutation; this proof uses the lemmas above in its induction step, but it also requires proving that the order of a permutation cannot be $\mathbf{n}$, which needs the Annihilation theorem and a bit more. That focuses attention on the question whether an unenlargeable finite set U can have a cyclical permutation f, since if that were impossible, then $\mathbb{F}$ could not be finite, so both $\mathbb{F}$ and $\mathbb{N}$ would be infinite. However, we could not derive a contradiction from the assumption that there is a cyclic permutation f on an unenlargeable set U.

21. Equivalence of Church and Rosser counting axioms

Thanks are due to Thomas Forster, who overcame my initial skepticism about proving the equivalence of these two axioms.

We make use of $\mathbb{T}x$, defined so that for $x \in \mathbb{F}$, and $a \in x$, we have $\mathbb{T}(x) = Nc(USC(a))$.

Lemma 21.1. *Suppose that* $\mathbb{T}^2 x = x$ *for all* $x \in \mathbb{F}$*. Then* $\mathbb{T}x = x$ *holds for all* $x \in \mathbb{F}$*.*

Proof. By Lemma 11.6 of [1], $\mathbb{T}x \in \mathbb{F}$. By Theorem 5.18 of [1], we have

$$x < \mathbb{T}x \ \vee \ x = \mathbb{T}x \ \vee \ \mathbb{T}x < x.$$

We argue by cases.

Case 1, $x < \mathbb{T}x$. Then

$$\begin{aligned} \mathbb{T}x &< \mathbb{T}^2 x && \text{by Lemma 11.20 of [1]} \\ \mathbb{T}x &< x && \text{since } \mathbb{T}^2 x = x \\ x &< x && \text{by Lemma 5.25 of [1]} \\ x &\not< x && \text{by Lemma 5.28 of [1]} \end{aligned}$$

That contradiction completes Case 1.

Case 2, $x = \mathbb{T}x$. Then $\mathbb{T}x = x$ and we are done.

Case 3, $\mathbb{T}x < x$. Then

$$\begin{array}{rl} \mathbb{T}^2 x < \mathbb{T}x & \text{by Lemma 11.20 of [1]} \\ x < \mathbb{T}x & \text{since } \mathbb{T}^2 x = x \\ x < x & \text{by Lemma 5.25 of [1]} \\ x \not< x & \text{by Lemma 5.28 of [1]} \end{array}$$

That contradiction completes Case 3. That completes the proof of the lemma.

Lemma 21.2. *Suppose that $\mathbb{T}^6 x = x$ for all $x \in \mathbb{F}$. Then $\mathbb{T}x = x$ holds for all $x \in \mathbb{F}$.*

Proof. (Similar to the proof of Lemma 21.1.) By Lemma 11.6 of [1], $\mathbb{T}x \in \mathbb{F}$. By Theorem 5.18 of [1], we have

$$x < \mathbb{T}x \ \vee \ x = \mathbb{T}x \ \vee \ \mathbb{T}x < x.$$

We argue by cases.

Case 1, $x < \mathbb{T}x$. Then

$$\begin{array}{rl} x < \mathbb{T}x < \mathbb{T}^2 x < T^3 x \ldots < \mathbb{T}^6 x & \text{by Lemma 11.20 of [1]} \\ x < \mathbb{T}^6 x & \text{by Lemma 5.25 of [1]} \\ x < x & \text{since } \mathbb{T}^6 x = x \\ x \not< x & \text{by Lemma 5.28 of [1]} \end{array}$$

That contradiction completes Case 1.

Case 2, $x = \mathbb{T}x$. Then $\mathbb{T}x = x$ and we are done.

Case 3, $\mathbb{T}x < x$. Then

$$\begin{array}{rl} \mathbb{T}^6 x < \mathbb{T}^5 x \ldots < \mathbb{T}^2 x < \mathbb{T}x & \text{by Lemma 11.20 of [1]} \\ \mathbb{T}^6 x < x & \text{by Lemma 5.25 of [1]} \\ x < x & \text{since } \mathbb{T}^6 x = x \\ x \not< x & \text{by Lemma 5.28 of [1]} \end{array}$$

That contradiction completes Case 3. That completes the proof of the lemma.

Define $J(x) := \{z \in \mathbb{F} : z < x\}$. Rosser stated his counting axiom in the form $J(x) \in x$ for $x \in \mathbb{F}$.

Lemma 21.3. *Rosser's counting axiom is equivalent to $\mathbb{T}(x) = x$ for all $x \in \mathbb{F}$.*

Proof. Left to right: Assume Rosser's counting axiom. Let $x \in \mathbb{F}$. Then

$$\begin{array}{rl} Nc(J(x)) = \mathbb{T}^2 x & \text{by Lemma 14.4 of [1]} \\ J(x) \in x & \text{by Rosser's counting axiom} \\ Nc(J(x)) = x & \text{by Lemma 11.4 of [1]} \\ \mathbb{T}^2 x = x & \text{by the preceding lines} \end{array}$$

Since x was arbitrary, we have proved $\forall x \in \mathbb{F}\, (\mathbb{T}^2 x = x)$. Then by Lemma 21.1, we have $\forall x \in \mathbb{F}\, (\mathbb{T}x = x)$. That completes the left-to-right direction.

Right to left: Assume for all $x \in \mathbb{F}$, $\mathbb{T}(x) = x$. Then $Nc(J(x)) = \mathbb{T}^2 x = \mathbb{T}x = x$, so $\mathbb{J}(x) \in x$ by Lemma 4.21 of [1]. That completes the proof of the lemma.

Definition 21.4. *Let* $\mathbf{i}$ *be the intersection of all sets* w *such that*

$$\begin{aligned}
&u \in w \to \exists p, q\,(u = \langle p, q\rangle \ \wedge\ p \in \mathbb{N} \ \wedge\ q \in \mathbb{F} \\
&\langle \mathbf{0}, \mathsf{zero}\rangle \in w \\
&\langle p, q\rangle \in w \to q^+ \in \mathbb{F} \to \langle \mathsf{S}p, q^+\rangle \in w.
\end{aligned}$$

Remark. If $\mathbb{N}$ is finite, then $\mathbf{i}$ may not be a function, because if $\mathsf{S}\mathbf{n} = \mathsf{S}\mathbf{k}$ then $\mathbf{i}\,(\mathsf{S}\mathbf{n})$ would have to be both $\mathbf{i}\,(\mathbf{n})^+$ and $\mathbf{i}\,(\mathbf{k})^+$. And, if $\mathbb{F}$ is not finite, then the domain of $\mathbf{i}$ might be a proper subset of $\mathbb{F}$. But, if both $\mathbb{N}$ and $\mathbb{F}$ are infinite, then $\mathbf{i}$ should turn out to be a similarity between them.

Lemma 21.5. $\langle \mathbf{0}, \mathsf{zero}\rangle \in \mathbf{i}$.

Proof. Let w be a set satisfying the conditions in the definition of $\mathbf{i}$. Then $\langle \mathbf{0}, \mathsf{zero}\rangle \in w$. Since w is arbitrary, $\langle \mathbf{0}, \mathsf{zero}\rangle \in \mathbf{i}$. That completes the proof of the lemma.

Lemma 21.6. *Suppose* $\langle p, q\rangle \in \mathbf{i}$ *and* $q^+ \in \mathbb{F}$. *Then* $\langle \mathsf{S}p, q^+\rangle \in \mathbf{i}$.

Proof. Suppose $\langle p, q\rangle \in \mathbf{i}$ and $q^+ \in \mathbb{F}$. We must show $\langle \mathsf{S}p, q^+\rangle \in \mathbf{i}$. Let w be any set satisfying the conditions in the definition. Then $\langle p, q\rangle \in w$. Since $q^+ \in \mathbb{F}$ we have $\langle \mathsf{S}p, q^+\rangle \in w$. Since w was any set satisfying the conditions, we have $\langle \mathsf{S}p, q^+\rangle \in \mathbf{i}$ as desired. That completes the proof of the lemma.

Lemma 21.7. *Let* $\mathbf{i}$ *be as in Definition 21.4. Suppose* $\langle p, q\rangle \in \mathbf{i}$. *Then either* $p = \mathbf{0} \ \wedge\ q = \mathsf{zero}$, *or for some* $t \in \mathbb{N}$ *and* $r \in \mathbb{F}$, *we have*

$$\langle t, r\rangle \in \mathbf{i} \ \wedge\ p = \mathsf{S}t \ \wedge\ q = r^+.$$

Proof. Define

$$w := \{\, \langle p, q\rangle \in \mathbf{i} : (p = \mathbf{0} \ \wedge\ q = \mathsf{zero}) \ \vee\ \exists t, r\,(\langle t, r\rangle \in \mathbf{i} \ \wedge\ p = \mathsf{S}t \ \wedge\ q = r^+)\,\}.$$

The formula is stratified, giving p, q, r all index 0; $\mathbf{i}$ is a parameter. Therefore the definition is legal.

Then w satisfies the conditions in Definition 21.4. Therefore $\mathbf{i} \subseteq w$. That completes the proof of the lemma.

Lemma 21.8. *Let* $\mathbf{i}$ *be as in Definition 21.4. Suppose* $\langle p, y^+\rangle \in \mathbf{i}$. *Then for some* $t \in \mathbb{N}$, *we have*

$$\langle t, y\rangle \in \mathbf{i} \ \wedge\ p = \mathsf{S}t.$$

Proof. Take q in Lemma 21.7 to be y^+. By Lemma 4.16 of [1], we do not have $y^+ = \mathsf{zero}$. Hence there exists t, r with $\langle t, r\rangle \in \mathbf{i}$ and $p = \mathsf{S}t$ and $y^+ = r^+$. By Lemma 5.12 of [1], we have $y = r$. Then $\langle t, y\rangle \in i$. That completes the proof of the lemma.

Lemma 21.9. *Suppose Church successor is one-to-one on* $\mathbb{N}$. *Then for all* $x \in \mathbb{N}$ *and* $z \in \mathbb{F}$,

$$\langle x, y\rangle \in \mathbf{i} \to \langle x\mathsf{S}\mathbf{0}, z\rangle \in \mathbf{i} \to \mathbb{T}^6 z = y.$$

Proof. The formula is stratified, giving x and y index 6 and z index 0, with $\mathbf{i}$ as a parameter. Therefore we may prove it by $\mathbb{N}$-induction on x.

Base case, $x = \mathbf{0}$. Assume $\langle \mathbf{0}, y\rangle \in \mathbf{i}$ and $\langle \mathbf{0}\mathsf{S}\mathbf{0}, z\rangle \in \mathbf{i}$. Then $y = z = \mathsf{zero}$, since $\mathbf{0}\mathsf{S}\mathbf{0} = \mathbf{0}$. By Lemma 11.9 of [1], $\mathbb{T}^6\mathbf{0} = \mathbf{0}$. That completes the base case.

Induction step. Suppose $\langle \mathsf{S}x, y\rangle \in \mathbf{i}$ and $\langle \mathsf{S}x\mathsf{S}\mathbf{0}, z\rangle \in \mathbf{i}$. Then

$$\langle \mathsf{S}(x\mathsf{S}\mathbf{0}), z\rangle \in \mathbf{i} \qquad \text{by Theorem 3.6}$$

By Lemma 21.8, $z = r^+$ for some $r \in \mathbb{F}$ and some p with $\langle p, r\rangle \in \mathbf{i}$ where $\mathsf{S}p = \mathsf{S}(x\mathsf{S}\mathbf{0})$. Since Church successor is one-to-one (by hypothesis), we have $p = x\mathsf{S}\mathbf{0}$. Therefore $\langle x\mathsf{S}\mathbf{0}, r\rangle \in \mathbf{i}$. Similarly, since $\langle \mathsf{S}x, y\rangle \in \mathbf{i}$, $y = t^+$ for some $t \in \mathbb{F}$ with $\langle x, t\rangle \in \mathbf{i}$. Since $\langle x, t\rangle \in \mathbf{i}$ and $\langle x\mathsf{S}\mathbf{0}, r\rangle \in \mathbf{i}$, we have

$$\begin{array}{rl} \mathbb{T}^6 r = t & \text{by the induction hypothesis} \\ (\mathbb{T}^6 r)^+ = t^+ & \text{by the previous line} \\ (\mathbb{T}^6 r)^+ = y & \text{since } y = t^+ \end{array}$$

I say that

$$(\mathbb{T}^6 r)^+ = \mathbb{T}^6(r^+) \tag{64}$$

We wish to justify (64) by six applications of Lemma 11.8 of [1]; let us consider the first step, $(\mathbb{T}r)^+ = \mathbb{T}(r^+)$. To use Lemma 11.8 of [1], we need to show that r^+ is inhabited. We have

$$\begin{array}{rl} z \in \mathbb{F} & \text{since } \langle \mathsf{S}x\mathsf{S}\mathbf{0}, z\rangle \in \mathbf{i} \\ \exists u\,(u \in z) & \text{by Lemma 4.7 of [1]} \\ \exists u\,(u \in r^+) & \text{since } z = r^+ \\ (\mathbb{T}r)^+ = \mathbb{T}(r^+) & \text{by Lemma 11.8 of [1]} \end{array}$$

Now to take the next steps, we need Lemma 11.16 of [1], which says that $\mathbb{T}$ of anything in $\mathbb{F}$ has its successor in $\mathbb{F}$. We have

$$\begin{array}{rl} \mathbb{T}r \in \mathbb{F} & \text{by Lemma 11.6} \\ (\mathbb{T}r)^+ \in \mathbb{F} & \text{by Lemma 11.16} \\ \exists u\,(u \in (\mathbb{T}r)^+) & \text{by Lemma 4.7 of [1]} \\ \mathbb{T}^2 r \in \mathbb{F} & \text{by Lemma 11.6} \\ (\mathbb{T}^2 r)^+ \in \mathbb{F} & \text{by Lemma 11.16} \\ \exists u\,(u \in (\mathbb{T}^2 r)^+) & \text{by Lemma 4.7 of [1]} \end{array}$$

Continuing in this way we eventually prove $\mathbb{T}^m r$ is in $\mathbb{F}$ and is inhabited, for m up to and including 6. Now we have all the side conditions necessary to apply Lemma 11.8 of [1] six times. That completes the proof of (64). Continuing, we have

$$\begin{array}{rl} (\mathbb{T}^6 r)^+ = y & \text{as shown above} \\ \mathbb{T}^6(r^+) = y & \text{by (64)} \\ \mathbb{T}^6 z = y & \text{since } z = r^+ \end{array}$$

That completes the induction step. That completes the proof of the lemma.

Lemma 21.10. *The relation* $\mathbf{i}$ *is onto* $\mathbb{F}$. *Explicitly,*

$$\forall y \in \mathbb{F}\, \exists x \in \mathbb{N}\,(\langle x, y\rangle \in \mathbf{i}) \tag{65}$$

Proof. The formula is stratified, giving x and y index 0, so it can be proved by $\mathbb{F}$-induction on y.

Base case, $y = \mathsf{zero}$; then $x = \mathbf{0}$ will do.

Induction step. Suppose $\langle x, y\rangle \in \mathbf{i}$ and y^+ is inhabited. Then $y^+ \in \mathbb{F}$ by Lemma 4.19 of [1], so $\langle \mathsf{S}x, y^+\rangle \in \mathbf{i}$. That completes the proof of the lemma.

Theorem 21.11. *The Church counting axiom implies the Rosser counting axiom.*

Proof. Assume the Church counting axiom. By Theorem 18.6, $\mathbb{N}$ is not finite. Then by Theorem 19.20, Church successor is one-to-one on $\mathbb{N}$. Let $z \in \mathbb{F}$. By Lemma 21.10, there exists $x \in \mathbb{N}$ such that $\langle x, z\rangle \in \mathbf{i}$. We have

$$\begin{array}{rll} x\mathsf{S}\mathbf{0} = x & & \text{by the Church counting axiom} \\ \langle x\mathsf{S}\mathbf{0}, z\rangle \in \mathbf{i} & & \text{since } \langle x, z\rangle \in \mathbf{i} \\ \mathbb{T}^6 z = z & & \text{by Lemma 21.9, with } y = z \\ \forall z \in \mathbb{F}\,(\mathbb{T}^6 z = z) & & \text{since } z \text{ was arbitrary} \\ \forall z \in \mathbb{F}\,(\mathbb{T}x = x) & & \text{by Lemma 21.2} \end{array}$$

By Lemma 21.3, we have the Rosser counting axiom. That completes the proof of the theorem.

Lemma 21.12. $\langle x, y\rangle \in \mathbf{i} \to \langle z, y\rangle \in \mathbf{i} \to x = z$.

Proof. The formula is stratified, giving x, y, and z all index 0. We prove it by $\mathbb{F}$-induction on y.

Base case, $y = \mathsf{zero}$. By Lemma 21.7 and Lemma 4.16 of [1], we have $x = \mathbf{0}$ and $z = \mathbf{0}$. Therefore $x = z$. That completes the base case.

Induction step. Suppose $\langle x, y^+\rangle \in \mathbf{i}$ and $\langle z, y^+\rangle \in \mathbf{i}$. We must show $x = z$. By Lemma 21.7 and Lemma 4.16 of [1], there exist $p, q \in \mathbb{N}$ and $r, t \in \mathbb{F}$ such that $x = \mathsf{S}p$, $z = \mathsf{S}q$, and $r^+ = y^+ = t^+$, and $\langle p, r\rangle \in \mathbf{i}$ and $\langle q, t\rangle \in \mathbf{i}$. By Lemma 5.12 of [1], $r = y = t$. Then

$$\begin{array}{rll} \langle q, y\rangle \in \mathbf{i} & & \text{since } t = y \text{ and } \langle q, t\rangle \in \mathbf{i} \\ \langle p, y\rangle \in \mathbf{i} & & \text{since } \langle p, r\rangle \in \mathbf{i} \text{ and } y = r \\ p = q & & \text{by the induction hypothesis} \\ x = z & & \text{since } x = \mathsf{S}p,\ z = \mathsf{S}q, \text{ and } p = q \end{array}$$

That completes the induction step. That completes the proof of the lemma.

Lemma 21.13. *The Rosser counting axiom implies that x^+ is inhabited for every $x \in \mathbb{F}$.*

Proof. Assume the Rosser counting axiom. Define $J(x) := \{z \in \mathbb{F} : z < x\}$. Then $x \notin J(x)$, by Lemma 5.28 of [1]. We will prove that x^+ is inhabited for every $x \in \mathbb{F}$. The formula is stratified, so we may prove it by induction on x.

Base case, zero^+ is inhabited, since $\mathsf{zero} \in \mathsf{zero}^+$.

Induction step. Suppose x^+ is inhabited; we must show x^{++} is inhabited. By the Rosser counting axiom, $J(x^+) \in x^+$. By Lemma 4.19 of [1], $x^+ \in \mathbb{F}$. By Lemma 5.28 of [1], $x^+ \notin J(x^+)$. Then $J(x^+) \cup \{x^+\} \in x^{++}$. That completes the induction step. That completes the proof of the lemma.

Lemma 21.14. *The Rosser counting axiom implies $\mathbf{i}$ is total. Explicitly:*

$$\forall x \in \mathbb{N}\, \exists y \in \mathbb{F}\,(\langle x, y\rangle \in \mathbf{i})$$

Remark. $\mathbf{i}$ may still not be a function.

Proof. Assume the Rosser counting axiom. The formula is stratified, giving x and y index 0, with $\mathbf{i}$ as parameter. We prove it by $\mathbb{N}$-induction on x.

Base case, $x = \mathbf{0}$. Take $y = \mathsf{zero}$.

Induction step. By the induction hypothesis, there exists y such that $\langle x, y\rangle \in \mathbf{i}$ and $y \in \mathbb{F}$. Then

$$\begin{array}{rl} x \in \mathbb{N} \ \wedge \ y \in \mathbb{F} & \text{since } \langle x, y\rangle \in \mathbf{i} \\ \exists u\,(u \in y^+) & \text{by Lemma 21.13} \\ y^+ \in \mathbb{F} & \text{by Lemma 4.19 of [1]} \\ \langle \mathsf{S}x, y^+\rangle \in \mathbf{i} & \text{by Lemma 21.6} \end{array}$$

That completes the induction step. That completes the proof of the lemma.

Lemma 21.15. *Assume the Rosser counting axiom. Let* $\mathbf{j}$ *be the converse relation of* $\mathbf{i}$*, that is,* $\langle u, v\rangle \in j \leftrightarrow \langle v, u\rangle \in \mathbf{i}$*. Then* $j : \mathbb{F} \to \mathbb{N}$ *is a function.*

Proof. We have to prove

$$\forall y, z\,(\langle y, x\rangle \in \mathbf{i} \ \rightarrow \langle z, x\rangle \in \mathbf{i} \ \rightarrow y = z)$$

That formula is stratified, giving x, y, and z all index 0, with $\mathbf{i}$ as a parameter. We prove it by $\mathbb{F}$-induction on x.

Base case, $x = \mathsf{zero}$. Suppose $\langle y, \mathsf{zero}\rangle \in \mathbf{i}$ and $\langle z, \mathsf{zero}\rangle \in \mathbf{i}$. Then $y = z = \mathbf{0}$. That completes the base case.

Induction step. Suppose x^+ is inhabited and $\langle y, x^+\rangle \in \mathbf{i}$ and $\langle z, x^+\rangle \in i$. Then

$$\begin{array}{rl} y = \mathsf{S}r \ \wedge \ \langle r, x\rangle \in i & \text{for some } r\text{, by Lemma 21.8} \\ z = \mathsf{S}t \ \wedge \ \langle t, x\rangle \in i & \text{for some } r\text{, by Lemma 21.8} \\ r = t & \text{by the induction hypothesis} \\ y = z & \text{since } y = \mathsf{S}r \text{ and } z = \mathsf{S}t \end{array}$$

That completes the induction step. That completes the proof of the lemma.

Lemma 21.16. *Assume the Rosser counting axiom. Then for all* $x \in \mathbb{F}$*,*

$$(\mathbf{j}\,x)\mathsf{S}\mathbf{0} = \mathbf{j}\,(\mathbb{T}^6 x).$$

Proof. The formula of the lemma is stratified, so we may prove it by $\mathbb{F}$-induction on x.

Base case, $x = \mathsf{zero}$. We have

$$\begin{array}{rl} \mathbf{j}\,(\mathsf{zero}) = \mathbf{0} & \text{by Lemma 21.5} \\ (\mathbf{j}\,\mathsf{zero})\mathsf{S}\mathbf{0} = \mathbf{0}\mathsf{S}\mathbf{0} & \text{by the preceding line} \\ = \mathbf{0} & \text{by Lemma 2.12} \end{array}$$

On the other hand

$$\begin{array}{rl} \mathbb{T}^6\mathsf{zero} = \mathsf{zero} & \text{by Lemma 11.9 of [1]} \\ \mathbf{j}\,(\mathbb{T}^6\mathsf{zero}) = \mathbf{j}\,(\mathsf{zero}) & \text{by the preceding line} \\ = \mathbf{0} & \text{by Lemma 21.5} \end{array}$$

Therefore $(\mathbf{j}\,\mathsf{zero})\mathsf{S}\mathbf{0} = \mathbf{j}\,(\mathbb{T}^6\mathsf{zero})$, since both sides are equal to $\mathbf{0}$. That completes the base case.

Induction step. We have

$$\begin{aligned}
(\mathbf{j}\,(x^+))\mathsf{S}\mathbf{0} &= (\mathsf{S}(\mathbf{j}\,x))\mathsf{S}\mathbf{0} && \text{by Lemma 21.8}\\
&= \mathsf{S}((\mathbf{j}\,x)\mathsf{S}\mathbf{0}) && \text{by Theorem 3.6}\\
&= \mathsf{S}(\mathbf{j}\,(\mathbb{T}^6 x)) && \text{by the induction hypothesis}\\
\mathbb{T}x &= x && \text{by Lemma 21.3 and the Rosser counting axiom}\\
\mathbb{T}^6 x &= x && \text{by six applications of the preceding line}\\
(\mathbf{j}\,(x^+))\mathsf{S}\mathbf{0} &= \mathsf{S}(\mathbf{j}\,x) && \text{by the preceding three lines}\\
&= \mathbf{j}\,(\mathbb{T}^6(x^+)) && \text{since } \mathbb{T}(x^+) = x^+ \text{ by Lemma 21.3}
\end{aligned}$$

That completes the induction step. That completes the proof of the lemma.

Theorem 21.17. *The Rosser counting axiom implies the Church counting axiom.*

Proof. Assume the Rosser counting axiom. Let $z \in \mathbb{N}$. Then

$$\begin{aligned}
z\mathsf{S}\mathbf{0} &\in \mathbb{N} && \text{by Lemma 16.9}\\
\langle z, x\rangle &\in \mathbf{i} && \text{for some } x\text{, by Lemma 21.14}\\
\mathbf{j}\,x &= z && \text{since } \langle x, z\rangle \in \mathbf{j} \leftrightarrow \langle z, x\rangle \in \mathbf{i}\\
(\mathbf{j}\,x)\mathsf{S}\mathbf{0} &= \mathbf{j}\,\mathbb{T}^6 x && \text{by Lemma 21.16}\\
\mathbb{T}^6 x &= x && \text{by Lemma 21.3 and the Rosser counting axiom}\\
(\mathbf{j}\,x)\mathsf{S}\mathbf{0} &= \mathbf{j}\,x && \text{by the preceding two lines}
\end{aligned}$$

Since $z = \mathbf{j}\,x$, we have $z\mathsf{S}\mathbf{0} = z$. Since z was arbitrary, we have proved the Church counting axiom. That completes the proof of the lemma.

22. Conclusion

We have thoroughly studied the Church numbers in NF set theory, thus relating the logical work of the two great twentieth-century logicians Quine and Church. This analysis led to the result that the set of Church numbers $\mathbb{N}$, if not infinite, must have a certain structure under successor, namely a stem STEM and a loop $\mathcal{L}$, connected at the unique double successor. That situation led to the Annihilation Theorem: There is a Church number $\mathbf{m}$ such that the $\mathbf{m}$-th iterate of any map from any finite set to itself is the identity.

This leads to a contradiction if we can show that there is a finite set with a permutation of order not divisible by $\mathbf{m}$. This we could do only under the additional assumption of the Church counting axiom, that $j\mathsf{S}\mathbf{0} = j$ for every Church number j.

Assuming the Church counting axiom, we can use the Annihilation Theorem to prove that the set $\mathbb{N}$ of Church numbers is not finite. That result is new even in NF with classical reasoning. That is, Specker's result shows that $\mathbb{F}$ is infinite, but that was not known to imply anything about $\mathbb{N}$, even with the aid of the Rosser counting axiom.

We also proved that if $\mathbb{N}$ is not finite, then $\mathbb{N}$ is infinite and Church successor is injective. While that result is classically trivial, it is far from obvious intuitionistically. That implicaation does not require the Church counting axiom. Together, the two results show that Heyting's arithmetic HA is interpretable in INF plus the Church counting axiom. It remains open whether HA is interpretable in INF alone.

However, if we are willing to use classical logic, then we do not need the Church counting axiom, as we will now explain. Specker proved, using classical logic, that $\mathbb{F}$ is infinite. We proved in Theorem 20.11 that if $\mathbb{F}$ is infinite, but $\mathbb{N}$ is finite, then every Church number is the order of some permutation, contradicting the Annihilation Theorem. Therefore, if $\mathbb{F}$ is infinite, $\mathbb{N}$ is not finite, and therefore $\mathbb{N}$ is infinite. Then, appealing to Specker's result, classical logic implies $\mathbb{N}$ is infinite. Summarizing, we showed that $\mathbb{N}$ is infinite if either the Rosser counting axiom, or the Church counting axiom, or classical logic holds. It remains open whether INF proves $\mathbb{N}$ is infinite (without any additional assumption).

We also proved that the Church counting axiom is equivalent to the Rosser counting axiom in INF. This proof uses our results that Church counting implies $\mathbb{N}$ is infinite. And again, although we proved the equivalent intuitionistically, it is a new result even classically.

References

[1] Michael Beeson. Intuitionistic NF set theory. 2021.

[2] Alonzo Church. *The Calculi of Lambda-conversion*, volume 6 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, New Jersey, 1941.

[3] Leonardo Mendonça de Moura, Soonho Kong, Jeremy Avigad, Floris van Doorn, and Jakob von Raumer. The Lean theorem prover (system description). In *Automated Deduction - CADE-25 - 25th International Conference on Automated Deduction, Berlin, Germany, August 1-7, 2015, Proceedings*, pages 378–388, 2015.

[4] Thomas E. Forster. *Set Theory with a Universal Set: Exploring an Untyped Universe*. Number 31 in Oxford Logic Guides. Oxford Science Publications, second edition, 1995.

[5] Stephen C. Kleene. A theory of positive integers in formal logic. *American Journal of Mathematics*, 57:153–175,219–244, 1935.

[6] Steven Orey. New foundations and the axiom of counting. *Duke Mathematical Journal*, 31(4):655–660, 1964.

[7] Willard Quine. New foundations for mathematical logic. *American Mathematical Monthly*, 44:77–80, 1937.

[8] J. B. Rosser. The axiom of infinity in Quine's New Foundations. *Journal of Symbolic Logic*, 17:238–242, 1952.

[9] J. Barkley Rosser. *Logic for Mathematicians*. McGraw-Hill, New York, Toronto, London, first edition, 1953.

[10] E. P. Specker. The axiom of choice in Quine's new foundations for mathematical logic. *Proceedings of the National Academy of Sciences of the USA*, 39:972–975, 1953.