INTUITIONISTIC NF SET THEORY

MICHAEL BEESON

Abstract. We develop NF set theory using intuitionistic logic; we call this theory INF. We develop the theories of finite sets and their power sets, finite cardinals and their ordering, cardinal exponentiation, addition, and multiplication. We follow Rosser and Specker with appropriate constructive modifications, especially replacing "arbitrary subset" by "separable subset" in the definitions of exponentiation and order. It is not known whether INF proves that the set of finite cardinals is infinite, so the whole development must allow for the possibility that there is a maximum integer; arithmetical computations might "overflow" as in a computer or odometer, and theorems about them must be carefully stated to allow for this possibility. The work presented here is intended as a substrate for further investigations of INF.

Contents

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 [9]. Intuitionistic NF, or INF, is the theory with the same language and axioms as NF, but with intuitionistic logic instead of classical.

Date: August 23, 2023.

The "axiom" of infinity is a theorem of NF, proved by Rosser [7, 9] and Specker [10]. These proofs use classical logic in an apparently essential way. It is still an open question whether INF proves the existence of an infinite set. The Stanford Encyclopedia of Philosophy's article on NF says [3]

> The only known proof (Specker's) of the axiom of infinity in NF has too little constructive content to allow a demonstration that INF admits an implementation of Heyting arithmetic.

This paper is devoted to supplying infrastructure, on the basis of which one can investigate that question, and possibly some of the many other questions about INF whose answers are presently unknown. Just to list a few of those:[1]

- Is the set $\mathbb{F}$ of finite cardinals finite? Is it infinite?
- Can one point to any specific instance of the law of the excluded middle that is not provable in INF (even assuming NF is consistent)?
- Is INF consistent if NF is consistent? Is there any double-negation interpretation from NF to INF?
- Is Church's thesis consistent with INF? Markov's principle?
- Is INF closed under Church's rule?

Only one thing is known about INF (see [4]): If $\mathbb{V}$ is finite, then logic is classical, so Specker's proof can be carried out. Therefore $\mathbb{V}$ is not finite. That, however, does not lead to the conclusion that the set of finite cardinals is not finite. For all we know, there might be a largest finite cardinal m, which would contain a finite set U that is "unenlargeable", in the sense that we cannot find any x that is not a member of U. Classically, that would imply $U = \mathbb{V}$, which is a contradiction if $\mathbb{V}$ is known to be not finite.

Thanks to Thomas Forster for asking me (once a year for twenty years) about the strength of INF. Thanks to Randall Holmes, Albert Visser, and Thomas Forster for many emails on this subject. Thanks to the creators of the proof assistant Lean [2], which has enabled me to state with high confidence that there are no errors in this paper.[2] Thanks to the users of Lean who helped me acquire sufficient expertise in using Lean by answering my questions, especially Mario Carneiro.

There are many lemmas in this paper, and the intention is that each of those lemmas is provable in INF. Occasionally we state explicitly "INF proves", but even when we do not, it is the case. An important reference for NF is Rosser's book [8, 9].[3] We follow some of Rosser's notation, e.g., Λ for the empty set, and $Nc(x)$ for the cardinal of x, $SC(x)$ for the class of subclasses of x (the power set), $USC(x)$ for the class of unit subclasses (singletons) of x, $\mathbb{V}$ for the universe.

But the logical apparatus of Rosser's system includes a Hilbert-style epsilon-operator, which is not compatible with an intuitionistic version, and also, we do not wish to assume the axiom of infinity, as that is what we are trying to prove. Since all of Rosser's results are obtained using classical logic, we must begin afresh, proving exactly what we need in a first-order intuitionistic system.

---

[1] The terms used in these questions can be looked up in the index of [1].

[2] Each proof in this paper has been formalized and checked for validity using the proof assistant Lean. However, the proofs presented in this paper are human-readable and as complete as a detailed human-readable proof needs to be.

[3] The two editions are identical except for the Appendices added to the second edition, one of which contains Rosser's proof of infinity.

2. Axioms of NF, ordered pairs, and functions

NF has exactly two axioms: extensionality and stratified comprehension. The axiom of extensionality says that two sets with the same elements are equal. The axiom of stratified comprehension says that $\{x : \phi(x)\}$ exists, if ϕ is a stratified formula. A formula is **stratified**, or **stratifiable**, if each of its variables (both bound and free) can be assigned a non-negative integer ("index" or "type") such that (i) in every subformula $x \in y$, y gets an index one greater than x gets, and (ii) every occurrence of each variable gets the same index.

Thus, the "universe" $\mathbb{V}$ can be defined as

$$\mathbb{V} = \{x : x = x\}$$

but the Russell set $\{x : x \notin x\}$ cannot be defined.

We write $\langle x, y\rangle$ for the (Wiener-Kuratowski) ordered pair $\{\{x\}, \{x, y\}\}$. The ordered pair and the corresponding projection functions are defined by stratified formulas. To wit, the formula that expresses $z = \langle x, y\rangle$ is

$$u \in z \leftrightarrow \forall w \in u\,(w = x) \vee \forall w \in u\,(w = x \vee w = y),$$

which is stratifiable. Note that the ordered pair gets an index 2 more than the indices of the paired elements.[4] Then we have the basic property

Lemma 2.1. $\langle x, y\rangle = \langle a, b\rangle \leftrightarrow x = a \;\wedge\; y = b.$

Proof. Straightforward application of the definition and extensionality. We omit the approximately 70-step proof.

As usual, a function is a univalent set of ordered pairs. We note that being a function in NF is a strong condition. For example, $\{x\}$ exists for every x, but the map $x \mapsto \{x\}$ is not a function in NF, since to stratify an expression involving ordered pairs, the elements x and y of $\langle x, y\rangle$ must be given the same index, while in the example, $\{x\}$ must get one higher index than x.

Because the ordered pair raises types by two levels, we define ordered triples by

Definition 2.2 (Ordered triples)**.**

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

Then a function of two variables is definable in INF if its graph forms a set of ordered triples $\langle x, y, f(x, y)\rangle$.

We can conservatively add function symbols for binary union, union, intersection, and generally we can add a function symbol c_ϕ for any stratified formula ϕ, so that $x \in c_\phi(y) \leftrightarrow \phi(x, y)$. For a detailed discussion of the logical underpinnings of this step, see [5]. Function symbols for $\{x\}$, $\{x, y\}$, and $\langle x, y\rangle$ are also special cases of the c_ϕ; we can add these function symbols even though the "functions" they denote are not functions in the sense that their graphs are definable in INF. Thus for example we have

Lemma 2.3. *For all x, u: $u \in \{x\} \leftrightarrow u = x$*

Proof. This is the defining axiom for the function symbol $\{x\}$, which is really just $\{u : u = x\}$; that is, the function symbol is c_ϕ where $\phi(u, x)$ is $u = x$.

Lemma 2.4. *For all x, y, $\{x\} = \{y\} \leftrightarrow x = y$.*

[4] The axiom of infinity is needed to construct an ordered pair that does not raise the type level. See [9], p. 280.

Proof. Right to left is just equality substitution. Ad left to right: Suppose $\{x\} = \{y\}$. Then

$$
\begin{aligned}
u \in \{x\} \leftrightarrow u \in \{y\} & \quad \text{by extensionality} \\
u = x \leftrightarrow u = y & \quad \text{by Lemma 2.3} \\
x = y & \quad \text{by equality axioms}
\end{aligned}
$$

Technical details about stratification. In practice we need to use stratified comprehension in the presence of function symbols and parameters; the notion of stratification has to be extended to cover these situations. We define the notion of a formula ϕ being "stratified with respect to x". The variables of $\phi(x)$ are of three kinds: x (the "eigenvariable"), variables other than x that occur only on the right of $\in$ ("parameters"), and all other variables. An assignment of natural numbers (indices) to the variables that are not parameters is said to stratify ϕ with respect to x if for each atomic formula $x \in y$, y is assigned an index one larger than the index assigned to x. Note that the assignment is to variables, rather than occurrences of variable, so every occurrence of x gets the same index. Note also that parameters need not be assigned an index.

Now when terms are allowed, built up from constants and function symbols that are introduced by definitions, an assignment of indices must be extended from variables to terms. When we introduce a function symbol, we must tell how to do this. For example, the ordered pair $\langle x, y\rangle$ must have x and y assigned the same index, and then the pair gets an index 2 greater. The singleton $\{x\}$ must get an index one more than x, and so on. Stratified comprehension in the extended language says that $\{x : \Phi(x)\}$ exists, when Φ is stratified with respect to x. The set so defined will depend on any free variables of Φ besides x, some of which may be parameters and some not.

It is "well-known" that stratified comprehension, so defined, is conservative over NF, but it does not seem to proved in the standard references on NF; and besides, we need that result for INF as well. The algorithm in [5] meets the need: it will unwind the function symbols in favor of their definitions, preserving stratification. The confused reader is advised to work this out on paper for the example of the binary function symbol $\langle x, y\rangle$.

In our work, we repeatedly assert that certain formulas are stratifiable, and then we apply comprehension, either directly or indirectly by using mathematical induction or induction on finite sets. The question then arises of ensuring that only correctly stratified instances of comprehension are used. One approach is to use a finite axiomatization of INF. (It is easy to write one down following well-known examples for classical NF.) But that just pushes the problem back to verifying the correctness of that axiomatization; moreover it is technically difficult to reduce given particular instances of comprehension to a finite axiomatization. Instead, we just made a list of each instance of comprehension that we needed. There are 154 instances of comprehension in that list (which includes more than just the instances used in this paper). The Lean proof assistant is not checking that those instances are stratified. If one is not satisfied with a manual check of those 154 formulas, then one has to write a computer program to check that they are stratified. We did write one and those 154 formulas passed; since this paper is being presented as human-readable, we rely here on the human reader to check each stratification as it is presented; we shall not go into the technicalities of computer-checking stratification.

Functions and functional notation.

Definition 2.5. *$f : X \to Y$ ("f maps X to Y") means for every $x \in X$ there exists a unique $y \in Y$ such that $\langle x, y\rangle \in f$. "$f$ is a function" means*

$$\langle x, y\rangle \in f \ \wedge \ \langle x, z\rangle \in f \to y = z.$$

The domain and range of f are defined as usual, so f is a function if and only if it maps its domain to its range.

When f is a function, one writes $f(x)$ for that unique y. It is time to justify that practice in the context of INF.[5] Here is how to do that. We introduce a function symbol Ap (with the idea that we will abbreviate $Ap(f, x)$ to $f(x)$ informally).

Definition 2.6.

$$Ap(f, x) = \{u : \exists y\, (\langle x, y\rangle \in f \ \wedge \ u \in y\}.$$

It is legal to introduce Ap because it is a special case of a stratified comprehension term. One can actually introduce the symbol Ap formally, or one can regard Ap as an informal abbreviation for the comprehension term in the definition. Informally we are going to abbreviate $Ap(f, x)$ by $f(x)$ anyway, so Ap will be invisible in the informal development anyway. This procedure is justified by the following lemma:

Lemma 2.7. *If f is a function and $\langle x, y\rangle \in f$, then $y = Ap(f, x)$.*

Proof. Suppose f is a function and $\langle x, y\rangle \in f$. We must prove $y = Ap(f, x)$. By extensionality it suffices to show that for all t,

$$t \in y \leftrightarrow t \in Ap(f, x) \tag{1}$$

Left to right: Suppose $t \in y$. Then by the definition of Ap, we have $t \in Ap(f, x)$.

Right to left: Suppose $t \in Ap(f, x)$. Then by the definition of Ap, for some z we have $\langle x, z\rangle \in f$ and $t \in z$. Since f is a function, $y = z$. Then $t \in y$. That completes the right-to-left direction. That completes the proof of the lemma.

One-to-one, onto, and similarities. The function $f : X \to Y$ is **one-to-one** if

$$y \in Y \ \wedge \ \langle x, y\rangle \in f \to x \in X$$

and for $x, z \in X$ we have

$$f(x) = f(z) \to x = z.$$

If $f : X \to Y$ is one-to-one then we define

$$f^{-1} = \{\langle y, x\rangle : \langle x, y\rangle \in f\}.$$

The definition of f^{-1} can be given by a stratified formula, so it is legal in INF.

Remark. We could also consider the notion of "weakly one-to-one":

$$x, y \in X \wedge x \neq y \to f(x) \neq f(y).$$

The two notions are not equivalent unless equality on X and Y is **stable**, meaning $\neg\neg\, x = y \to x = y$. Since equality on finite sets is decidable, the two notions do coincide on finite sets, but we need the stronger notion in general, in particular, to

[5] Rosser's version of classical NF has Hilbert-style choice operator, which gives us "some y such that $\langle x, y\rangle \in f$." But INF does not and cannot have such an operator, so a different formal treatment is needed.

make the notion of "similarity" in the next definition be an equivalence relation. The point is that the stronger notion is needed for the following lemma.

Lemma 2.8. *The inverse of a one-to-one function from X onto Y is a one-to-one function from Y onto X. That is, if $f : X \to Y$ is one-to-one, then $f^{-1} : Y \to X$ and f^{-1} is one-to-one and onto.*

Proof. Let $f : X \to Y$ be one-to-one and onto. Since f is one-to-one, for each $y \in Y$ there is a unique x such that $\langle x, y\rangle \in f$. Then by definition of function, $f^{-1} : y \to x$. Since $f : X \to Y$, for each $x \in X$ there is a unique $y \in Y$ such that $\langle x, y\rangle \in f$.

I say $f^{-1} : Y \to X$. Let $y \in Y$. Since f is one-to-one, there exists a unique $x \in X$ such that $\langle x, y\rangle \in f$. That is, $\langle y, x\rangle \in f^{-1}$. Therefore $f^{-1} : Y \to X$, as claimed.

I say f^{-1} is one-to-one from Y to X. Let $x \in X$; since $f : X \to Y$ there is $y \in Y$ such that $\langle x, y\rangle \in f$. Then $\langle y, x\rangle \in f^{-1}$. Suppose also $\langle z, x\rangle \in f^{-1}$ with $z \in Y$. Then $\langle x, z\rangle \in f$. Since $f : X \to Y$, we have $x = z$. Therefore f^{-1} is one-to-one, as claimed.

I say f^{-1} maps Y onto X. Let $x \in X$. Let $y = f(x)$. Then $\langle x, y\rangle \in f$. Then $\langle y, x\rangle \in f^{-1}$. Therefore f^{-1} is onto, as claimed. That completes the proof of the lemma.

Definition 2.9. *The relation "x is similar to y" is defined by*

$$x \sim y \leftrightarrow \exists f\,(f : x \to y \;\wedge\; f \text{ is one-to-one and onto}).$$

In that case, f is a **similarity** *from x to y.*

The defining formula is stratified giving x and y the same type, so the relation is definable in INF.

Lemma 2.10. *The relation $x \sim y$ is an equivalence relation.*

Proof. Ad reflexivity: $x \sim x$ because the identity map from x to x is one-to-one and onto.

Ad symmetry: Let $x \sim y$. Then there exists a one-to-one function $f : x \to y$. By Lemma 2.8, there exists a function $f^{-1} : y \to x$ that is one-to-one and onto. Hence $y \sim x$. That completes the proof of symmetry.

Ad transitivity: Let $x \sim y$ and $y \sim z$. Then there exist f and g such that $f : x \to y$ is one-to-one and onto, and $g : y \to z$ is one-to-one and onto. Then $f \circ g : x \to z$ is one-to-one and onto. Therefore $x \sim z$. That completes the proof of transitivity. That completes the proof of the lemma.

Lemma 2.11. *For all x,*

$$x \sim \Lambda \leftrightarrow x = \Lambda.$$

Proof. Left to right: suppose $x \sim \Lambda$. Let $f : x \to \Lambda$ be a similarity. Suppose $u \in x$. Then for some v, $\langle u, v\rangle \in f$ and $v \in \Lambda$. But $v \notin \Lambda$. Hence $u \notin x$. Since u was arbitrary, $x = \Lambda$, as desired.

Right to left: Suppose $x = \Lambda$. We have to show $\Lambda \sim \Lambda$. But $\Lambda : \Lambda \to \Lambda$ is a similarity. That completes the proof of the lemma.

3. Finite sets

Definition 3.1. *The set* FINITE *of finite sets is defined as the intersection of all* X *such that* X *contains the empty set* Λ *and*

$$u \in X \wedge z \notin u \to u \cup \{z\} \in X.$$

The formula in the definition can be stratified by giving u index 1, z index 0, and X index 2, so the definition can be given in INF.

Definition 3.2. *The set* X **has decidable equality** *if*

$$\forall x, y \in X (x = y \vee x \neq y).$$

The class DECIDABLE *is the class of all sets having decidable equality.*

The formula defining decidable equality is stratified, so the class DECIDABLE can be proved to exist.

Lemma 3.3. *Every finite set has decidable equality. That is,* FINITE $\subseteq$ DECIDABLE*.*

Proof. Let Z be the set of finite sets with decidable equality. I say that Z satisfies the closure conditions in the definition of FINITE, Definition 3.1. The empty set has decidable equality, so the first condition holds. Now suppose $Y = X \cup \{a\}$, where $X \in Z$ and $a \notin X$. We must show $Y \in Z$. Let $x, y \in Y$. Then $x \in X \vee x = a$ and $y \in X \vee y = a$. There are thus four cases to consider: If both x and y are in X, then by the induction hypothesis, we have the desired $x = y \vee x \neq y$. If one of x, y is in X and the other is a, then $x \neq y$, since $a \notin X$; hence $x = y \vee x \neq y$. Finally if both are equal to a, then $x = y$ and hence $x = y \vee x \neq y$. Therefore, as claimed, Z satisfies the closure conditions. Hence every finite set belongs to Z. That completes the proof of the lemma.

Lemma 3.4. *A finite set is empty or it is inhabited (has a member).*

Proof. Define

$$Z = \{X \in \mathsf{FINITE} \ : X = \Lambda \ \vee \ \exists u \, (u \in X)\}.$$

We will show Z satisfies the closure conditions in the definition of FINITE. Evidently $\Lambda \in Z$. Now suppose $X \in Z$ and $Y = X \cup \{a\}$ with $a \notin X$. We must show $Y \in Z$. Since $X \in Z$, X is finite. Therefore Y is finite. Since $a \in Y$ we have $Y \in Z$. That completes the proof of the lemma.

Corollary 3.5 (Finite Markov's principle)**.** *For every finite set* X

$$\neg\neg \, \exists u \, (u \in X) \to \exists u \, (u \in X).$$

Proof. Let X be a finite set. Suppose $\neg\neg \, \exists u \, (u \in X)$. That is, X is nonempty. By Lemma 3.4, X has a member. That completes the proof of the lemma.

Lemma 3.6. $\Lambda \in$ FINITE.

Proof. Λ belongs to every set W containing Λ and containing $u \cup \{e\}$ whenever $u \in W$ and $e \notin W$. Since FINITE is the intersection of such sets W, $\Lambda \in$ FINITE. That completes the proof of the lemma.

Lemma 3.7. *If* $x \in$ FINITE *and* $c \notin x$*, then* $x \cup \{c\} \in$ FINITE*.*

Proof. Let $x \in$ FINITE. Then x belongs to every set W containing Λ and containing $u \cup \{e\}$ whenever $u \in W$ and $e \notin W$. Let W be any such set. Then $x \cup \{c\} \in W$. Since W was arbitrary, $x \cup \{c\} \in$ FINITE. That completes the proof of the lemma.

Lemma 3.8. *If* $z \in \mathsf{FINITE}$*, then* $z = \Lambda$ *or there exist* $x \in \mathsf{FINITE}$ *and* $c \notin x$ *such that* $z = x \cup \{c\}$*.*

Proof. The formula is stratified, giving c index 0, and x and z index 1. FINITE is a parameter. We prove the formula by induction on finite sets. Both the base case (when $z = \Lambda$) and the induction step are immediate. That completes the proof of the lemma.

Lemma 3.9. *Every unit class* $\{x\}$ *is finite.*

Proof. We have

$$\begin{array}{rl} \Lambda \in \mathsf{FINITE} & \text{by Lemma 3.6} \\ x \notin \Lambda & \text{by the definition of } \Lambda \\ \Lambda \cup \{x\} \in \mathsf{FINITE} & \text{by Lemma 3.7} \\ \{x\} = \Lambda \cup \{x\} & \text{by the definitions of } \cup \text{ and } \Lambda \\ \{x\} \in \mathsf{FINITE} & \text{by the preceding two lines} \end{array}$$

That completes the proof of the lemma.

Lemma 3.10. $USC(x)$ *is finite if and only if* x *is finite.*

Proof. Left-to-right: we have to prove

$$\forall y \in \mathsf{FINITE}\, \forall x\, (y = USC(x) \to x \in \mathsf{FINITE}) \tag{2}$$

The formula is weakly stratified with respect to y, as we are allowed to give the two occurrences of FINITE different types. So we may prove the formula by induction on finite sets y.

Base case. When $y = \Lambda = USC(x)$ we have $x = \Lambda$, so $x \in \mathsf{FINITE}$.

Induction step. Suppose $y \in \mathsf{FINITE}$ has the form $y = z \cup \{w\} = USC(x)$ and $w \notin z$, and $z \in \mathsf{FINITE}$. Then $w = \{c\}$ for some $c \in x$. The induction hypothesis is

$$\forall w\, (z = USC(w) \to w \in \mathsf{FINITE}) \tag{3}$$

Then

$$\begin{array}{rcll} z & = & y - \{w\} & \text{since } y = z \cup \{w\} \\ & = & USC(x) - \{\{c\}\} & \text{since } y = USC(x) \text{ and } w = \{c\} \\ & = & USC(x - \{c\}). & \end{array}$$

Since $y \in \mathsf{FINITE}$ and $\{c\} \in y$, we have

$$\begin{array}{rl} q \in y \to q = \{c\} \ \vee \ q \neq \{c\} & \text{by Lemma 3.3} \\ u \in x \to \{u\} = \{c\} \ \vee \ \{u\} \neq \{c\} & \text{since } y = USC(x) \\ u \in x \to u = c \ \vee \ u \neq c & \end{array}$$

It follows that

$$(x - \{c\}) \cup \{c\} \quad = \quad x \tag{4}$$

By the induction hypothesis (3), with $x - \{c\}$ substituted for w, we have

$$\begin{array}{rl} x - \{c\} \in \mathsf{FINITE} & \\ (x - \{c\}) \cup \{c\} \in \mathsf{FINITE} & \text{by definition of } \mathsf{FINITE} \\ x \in \mathsf{FINITE} & \text{by (4)} \end{array}$$

That completes the induction step. That completes the proof of the left-to-right implication.

Right-to-left: We have to prove

$$x \in \mathsf{FINITE} \to USC(x) \in \mathsf{FINITE} \tag{5}$$

Again the formula is weakly stratified since FINITE is a parameter. We proceed by induction on finite sets x.

Base case: $USC(\Lambda) = \Lambda \in \mathsf{FINITE}$.

Induction step: We have for any x and $c \notin x$,

$$USC(x \cup \{c\}) = USC(x) \cup \{\{c\}\}.$$

Let $c \notin x$ and $x \in \mathsf{FINITE}$. By the induction hypothesis (5), $USC(x)$ is finite, and since $c \notin x$, we have $\{c\} \notin USC(x)$. Then $USC(x) \cup \{\{c\}\}$ is finite. Then $USC(x \cup \{c\})$ is finite. That completes the induction step. That completes the proof of the lemma.

Lemma 3.11. *The union of two disjoint finite sets is finite.*

Proof. We prove by induction on finite sets X that

$$\forall Y \in \mathsf{FINITE}\,(X \cap Y = \Lambda \to X \cup Y \in \mathsf{FINITE}).$$

Base case: $\Lambda \cup Y = Y$ is finite.

Induction step: Suppose $X = Z \cup \{b\}$ with $b \notin Z$ and $Y \cap (Z \cup \{b\}) = \Lambda$ and Z finite. Then

$$\begin{aligned} X \cup Y &= (Z \cup Y) \cup \{b\} \\ X \cup Y &= Z \cup (Y \cup \{b\}) \end{aligned} \tag{6}$$

Since $Y \cap (Z \cup \{b\}) = \Lambda$, $b \notin Y$. Then by the definition of FINITE, $Y \cup \{b\}$ is finite. We have

$$Z \cap (Y \cup \{b\}) = Y \cap (Z \cup \{b\}) = \Lambda.$$

Then by the induction hypothesis, $Z \cup (Y \cup \{b\})$ is finite. Then by (6), $X \cup Y$ is finite. That completes the induction step. That completes the proof of the lemma.

Lemma 3.12. *If x has decidable equality, and $x \sim y$, then y has decidable equality.*

Proof. Suppose $x \sim y$. Then there exists $f : x \to y$ with f one-to-one and onto. By Lemma 2.8, $f^{-1} : y \to x$ is a one-to-one function. Then we have for $u, v \in y$,

$$u = v \leftrightarrow f^1(u) = f^{-1}(v). \tag{7}$$

Since x has decidable equality, we have

$$f^1(u) = f^{-1}(v) \;\vee\; f^1(u) \neq f^{-1}(v).$$

By (7),

$$u = v \;\vee\; u \neq v.$$

Therefore y has decidable equality.

Lemma 3.13. *Let $f : z \cup \{c\} \to y$ be one-to-one and onto. Suppose $c \notin z$, and let g be f restricted to z. Then $g : z \to y - \{f(c)\}$ is one-to-one and onto.*

Remark. Somewhat surprisingly, it is not necessary to assume that $z \cup \{c\}$ has decidable equality. That is not important as decidable equality is available when we use this lemma.

Proof. Let $q = f(c)$. Then $g : z \to y - \{q\}$. Suppose $g(u) = g(v)$. Then $f(u) = f(v)$. Since f is one-to-one, $u = v$. Hence g is one-to-one. Suppose $v \in y - \{q\}$. Since f is onto, $v = f(u)$ for some $u \in z \cup \{c\}$; but $u \neq c$ since if $u = c$ then $v = f(u) = q$, but $v \neq q$ since $v \in y - \{q\}$. Then $u \in z$. Hence g is onto. That completes the proof.

Lemma 3.14. *A set that is similar to a finite set is finite.*

Proof. We prove by induction on finite sets x that

$$\forall y\, (y \sim x \to y \in \mathsf{FINITE}).$$

The formula is stratified, so induction is legal.

Base case: When $x = \Lambda$. Suppose $y \sim \Lambda$. Then $y = \Lambda$, so $y \in \mathsf{FINITE}$. That completes the base case.

Induction step: Suppose the finite set x has the form $x = z \cup \{c\}$ with $c \notin z$, and $x \sim y$. By Lemma 3.3, x has decidable equality. Then by Lemma 3.12, y has decidable equality. Let $f : z \cup \{c\} \to y$ be f one-to-one and onto. Let $q = f(c)$. Then $\langle c, z\rangle \in f$. Let g be f restricted to z. By Lemma 3.13, $g : z \to y - \{q\}$ is one-to-one and onto. Then by the induction hypothesis, $y - \{q\}$ is finite. Then $(y - \{q\}) \cup \{q\} \in \mathsf{FINITE}$, by the definition of FINITE. But since y has decidable equality, we have

$$y = (y - \{q\}) \cup \{q)\}.$$

Therefore $y \in \mathsf{FINITE}$. That completes the induction step. That completes the proof of the lemma.

Definition 3.15. *The* **power set** *of a set X is defined as the set of subclasses of X:*

$$SC(X) = \{Y : Y \subset X\}.$$

We shall not make use of $SC(X)$, because there are "too many" subclasses of X. Consider, by contrast, the separable subclasses of X:

Definition 3.16. *We define the set of* **separable subclasses** *of X by*

$$SSC(X) := \{u : u \subseteq X \ \wedge \ X = u \cup (X - u)\}$$

That is, u is a separable subclass (or subset, which is synonymous) of X if and only if $\forall y \in X\, (y \in u \ \vee \ y \notin u)$. Classically, of course, every subset is separable, so we have $SSC(X) = SC(X)$, but that is not something we can assert constructively. The formula in the definition is stratified, so the definition can be given in INF. When working with finite sets, $SSC(X)$ is a good constructive substitute for $SC(X)$. We illustrate this by proving some facts about $SC(X)$, before returning to the question of the proper constructive substitute for $SC(X)$ when X is not necessarily finite.

Lemma 3.17. *Let x be a finite set. Then $SSC(x)$ is also a finite set.*

Remark. We cannot prove this with $SC(x)$ in place of $SSC(x)$.

Proof. The formula to be proved is

$$x \in \mathsf{FINITE} \to SSC(x) \in \mathsf{FINITE}.$$

The formula is weakly stratified because the two occurrences of the parameter FINITE may receive different indices. Therefore we can proceed by induction on finite sets x.

Base case: $SSC(\Lambda) = \{\Lambda\}$ is finite.

Induction step: Suppose x is finite and consider $x \cup \{c\}$ with $c \notin x$. Then $x \cup \{c\}$ is finite and hence, by Lemma 3.3, it has decidable equality.

By the induction hypothesis, $SSC(x) \in \mathsf{FINITE}$. I say that the map $u \mapsto u \cup \{c\}$ is definable in INF:

$$f := \{\langle u, y\rangle : u \in SSC(x) \ \wedge \ y = u \cup \{c\}.\}$$

The formula can be stratified by giving c index 0, u and y index 1, $SSC(x)$ index 2; then $\langle u, y\rangle$ has index 3 and we can give f index 4. Hence f is definable in INF as claimed. f is a function since y is uniquely determined as $u \cup \{c\}$ when u is given. Also f is one-to-one, since if $u \subseteq x$ and $v \subseteq x$ and $c \notin x$, and $u \cup \{c\} = v \cup \{c\}$, then $u = v$. Define

$$A := Range(f).$$

Then

$$A = \{u \cup \{c\} : u \in SSC(x)\}. \tag{8}$$

Then $SSC(x) \sim A$, because $f : SSC(x) \to A$ is one-to-one and onto. Since $SSC(x)$ is finite (by the induction hypothesis), by Lemma 3.3, $SSC(x)$ has decidable equality. Then A has decidable equality, by Lemma 3.12. Since A has decidable equality, and is similar to the finite set $SSC(x)$, A is finite, by Lemma 3.14.

I say that

$$SSC(x \cup \{c\}) \quad = \quad A \cup SSC(x). \tag{9}$$

By extensionality, it suffices to show that the two sides of (9) have the same members.

Left-to-right: Let $v \in SSC(x \cup \{c\})$. Then v is a separable subset of $x \cup \{c\}$. Then $c \in v \ \vee \ c \notin v$. If $c \notin v$ then $v \in SSC(x)$. If $c \in v$

$$
\begin{array}{rll}
 & x \cup \{c\} \in \mathsf{FINITE} & \text{since } x \in \mathsf{FINITE} \text{ and } c \notin x \\
x \cup \{c\} & \text{has decidable equality} & \text{by Lemma 3.3} \\
v & \text{has decidable equality} & \text{since } v \subseteq x \cup \{c\} \\
 & v = (v - \{c\}) \cup \{c\} & \text{since } x \in v \to x = c \ \vee \ x \neq c
\end{array}
$$

We have $v - \{c\} \in SSC(x)$, since $v \subset x \cup \{c\}$ and v has decidable equality. Then $f(v - \{c\}) \in Range(f) = A$. But $f(v - \{c\}) = (v - \{c\}) \cup \{c\} = v$. Therefore $v \in A$. Therefore $v \in A \cup SSC(x)$, as desired. That completes the proof of the left-to-right direction of (9).

Right-to-left. Let $v \in A \cup SSC(x)$. Then $v \in A \ \vee \ v \in SSC(x)$.

Case 1, $v \in A$. Then by (8), v has the form $v = u \cup \{c\}$ for some $u \in SSC(x)$. Then $u \cup \{c\} \in SSC(x \cup \{c\}$ as required.

Case 2, $v \in SSC(x)$. First we note that if $c \notin x$ then

$$SSC(x) \subseteq SSC(x \cup \{c\})$$

Therefore, since $v \in SSC(x)$, we have $v \in SSC(x \cup \{c\})$. That completes the proof of (9).

Note that A and $SSC(x)$ are disjoint, since every member of A contains c, and no member of $SSC(x)$ contains c, since $c \notin x$. Then by Lemma 3.11 and (9), $SSC(x \cup \{c\}) \in \mathsf{FINITE}$, as desired. That completes the proof of the lemma.

Lemma 3.18. *A finite subset of a finite set is a separable subset.*

Proof. Let $a \in \mathsf{FINITE}$. By induction on finite sets b we prove

$$b \in \mathsf{FINITE} \to b \subseteq a \to a = (a - b) \cup b. \tag{10}$$

The formula is stratified, so induction is legal.

Base case: Suppose $b = \Lambda$. Then $b \subseteq a$, so we have to prove $a = (a - \Lambda) \cup \Lambda$, which is immediate. That completes the base case.

Induction step: Suppose $b \in \mathsf{FINITE}$ and $c \notin b$ and $b \cup \{c\} \subseteq a$. We must show

$$a \quad = \quad (a - (b \cup \{c\}) \cup (b \cup \{c\})$$

By extensionality, it suffices to show that

$$x \in a \quad \leftrightarrow \quad x \in (a - (b \cup \{c\}) \cup (b \cup \{c\}) \tag{11}$$

Since a is finite, a has decidable equality, by Lemma 3.3.

Ad left-to-right of (11): Let $x \in a$. Then by decidable equality on a, we have

$$x = c \ \vee \ x \neq c \tag{12}$$

By the induction hypothesis (10), we have

$$x \in b \ \vee \ x \notin b \tag{13}$$

By (12) and (13) we have

$$x \in b \cup \{c\} \ \vee \ x \notin b \cup \{c\} \tag{14}$$

Therefore

$$x \in (a - (b \cup \{c\}) \cup (b \cup \{c\}).$$

That completes the left-to-right implication in (11).

Ad right-to-left: Suppose

$$x \in (a - (b \cup \{c\}) \cup (b \cup \{c\}).$$

We must show $x \in a$. If $x \in (a - (b \cup \{c\})$ then $x \in a$. If $x \in (b \cup \{c\})$ then $x \in a$, since by hypothesis $b \cup \{c\} \subseteq a$. That completes the right-to-left direction. That completes the induction step. That completes the proof of the lemma.

Lemma 3.19. *Every separable subset of a finite set is finite.*

Proof. By induction on finite sets X. When X is the empty set, every subset of X is the empty set, so every subset of X is empty, and hence finite. Now let $X = Y \cup \{a\}$ with $a \notin Y$ and Y finite, and let U be a separable subset of X; that is,

$$\forall z \in X \, (z \in U \ \vee \ z \notin U). \tag{15}$$

We have to show U is finite. Since U is separable, $a \in U \ \vee a \notin U$; we argue by cases accordingly.

Case 1: $a \notin U$. Then $U \subseteq Y$, so by the induction hypothesis, U is finite.

Case 2: $a \in U$. Let $V = U - \{a\}$. Then $V \subseteq Y$. I say that V is a separable subset of Y; that is,

$$\forall z \in Y\,(z \in V \ \vee \ z \notin V) \tag{16}$$

Let $z \in Y$. Since U is a separable subset of X, $z \in U \vee z \notin U$. By Lemma 3.3, X has decidable equality, so $z = a \vee z \neq a$. Therefore $z \in V \vee z \notin V$, as claimed in (16). Then, by the induction hypothesis, V is finite. Since $a \notin V$, also $V \cup \{a\}$ is finite. I say that $V \cup \{a\} = U$. If $x \in V \cup \{a\}$ then $x \in U$, since $V \subseteq U$ and $a \in U$. Conversely if $x \in U$ then $x = a \ \vee x \neq a$, since a and x both are members of X and X has decidable equality by Lemma 3.3. If $x = a$ then $x \in \{a\}$ and if $x \neq a$ then $x \in V$, so in either case $x \in V \cup \{a\}$. Therefore $V \cup \{a\} = U$ as claimed. Since V is finite and $a \notin V$, $V \cup \{a\}$ is finite. Since $U = V \cup \{a\}$, U is finite. That completes the induction step. That completes the proof of the lemma.

Lemma 3.20. *Let a and b be finite sets with $b \subseteq a$. Then $a - b$ is also a finite set.*

Proof. We first prove the special case when b is a singleton, $b = \{c\}$. That is,

$$a \in \mathsf{FINITE} \ \wedge \ c \in a \to a - \{c\} \in \mathsf{FINITE} \tag{17}$$

By Lemma 3.3, a has decidable equality. Hence $a - \{c\}$ is a separable subset of a. Then by Lemma 3.19, it is finite. That completes the proof of 17.

We now turn to the proof of the theorem proper. By induction on finite sets a we prove

$$\forall b \in \mathsf{FINITE}\,(b \subseteq a \to (a - b) \in \mathsf{FINITE}).$$

Base case: $\Lambda - b = \Lambda$ is finite.

Induction step. Let $a = p \cup \{c\}$, with $c \notin p$. Let b be a finite subset of a. We have $c \in b \ \vee c \notin b$ by Lemma 3.18. We argue by cases accordingly.

Case 1: $c \in b$. Then

$$\begin{aligned} a - b &= p \cup \{c\} - b \\ &= p - b \\ &= p - (b - \{c\}) \qquad \text{since } c \notin p \text{ and } c \in b \end{aligned}$$

Since b is finite, also $b - \{c\}$ is finite, by 17. Since $b - \{c\} \subseteq p$, by the induction hypothesis we have

$$p - (b - \{c\}) \in \mathsf{FINITE}.$$

Therefore $p - b \in \mathsf{FINITE}$. Therefore $a - b \in \mathsf{FINITE}$. That completes Case 1.

Case 2: $c \notin b$. Then $b \subseteq p$, so by the induction hypothesis $p - b$ is finite.

$$\begin{aligned} a - b &= (p \cup \{c\}) - b \\ &= (p - b) \cup \{c\} \qquad \text{since } c \notin b \end{aligned}$$

Therefore $a - b$ is finite. That completes Case 2. That completes the induction step. That completes the proof of the lemma.

Lemma 3.21 (Bounded quantification)**.** *Let X be any set with decidable equality. Let R be a separable relation on X. Let B be a finite subset of X. Let Y be defined by*

$$z \in Y \leftrightarrow z \in X \ \wedge \ \exists u \in B\, \langle u, z\rangle \in R$$

Then Y is a separable subset of X. With complete precision:

$$\begin{array}{l} \forall u, v \in X\,(u = v \ \vee\ u \neq v)\ \wedge \\ B \in \mathsf{FINITE}\ \wedge\ B \subseteq X\ \wedge\ \forall u, z \in X\,(\langle u, z\rangle \in R\ \vee\ \neg\,\langle u, z\rangle \in R) \\ \ \to \forall z \in X\,(\exists u \in B\,\langle u, z\rangle \in R\ \vee\ \neg\,\exists u \in B\,\langle u, z\rangle \in R) \end{array}$$

Remark. We may express the lemma informally as “The decidable sets are closed under bounded quantification.”

Proof. The formula to be proved is stratified, with FINITE as a parameter, giving u and z index 0, B index 1, and R index 3. Therefore it is legal to prove it by induction on finite sets B.

Base case: $B = \Lambda$. Then $Y = \Lambda$. Then $\forall z\,\neg\,\exists u \in B\,\langle u, z\rangle \in R$, and therefore

$$\forall z \in X\,(\exists u \in B\,\langle u, z\rangle \in R\ \vee\ \neg\,\exists u \in B\,\langle u, z\rangle \in R).$$

That completes the base case.

Induction step. Suppose $B = A \cup \{c\}$ with A finite and $c \notin A$. Then

$$\forall z \in X\,(\exists u \in B\,\langle u, z\rangle \in R \quad\leftrightarrow\quad (\exists u \in A\,\langle u, z\rangle \in R)\ \vee\ \langle c, z\rangle \in R) \tag{18}$$

We have to prove

$$(\exists u \in B\,\langle u, z\rangle \in R)\ \vee\ \neg\,(\exists u \in B\,\langle u, z\rangle \in R) \tag{19}$$

By (18), that is equivalent to

$$\begin{array}{ll} & (\exists u \in A\,\langle u, z\rangle \in R\ \vee\ \langle c, z\rangle \in R)\ \vee\ \neg\,(\exists u \in A\,\langle u, z\rangle \in R\ \vee\ \langle c, z\rangle \in R) \\ \leftrightarrow & (\exists u \in A\,\langle u, z\rangle \in R\ \vee\ \langle c, z\rangle \in R)\ \vee\ (\neg\,(\exists u \in A\,\langle u, z\rangle \in R)\ \wedge\ \langle c, z\rangle \notin R)) \\ \leftrightarrow & (\exists u \in A\,\langle u, z\rangle \in R\ \vee \neg\,\exists u \in A\,\langle u, z\rangle \in R\ \vee \langle c, z\rangle \in R) \\ & \ \wedge\ (\exists u \in A\,\langle u, z\rangle \in R\ \vee \neg\,\exists u \in A\,\langle u, z\rangle \in R\ \vee \neg\,\langle c, z\rangle \in R) \end{array}$$

Since $\langle c, z\rangle \in R\ \vee\ \neg\,\langle c, z\rangle \in R$, the last formula is equivalent to

$$\exists u \in A\,\langle u, z\rangle \in R\ \vee \neg\,\exists u \in A\,\langle u, z\rangle \in R.$$

But by the induction hypothesis, that holds. That completes the induction step. That completes the proof of the lemma.

Lemma 3.22 (swap similarity)**.** *Let X have decidable equality and let $U \subseteq X$ and $b, c \in X$ with $b \in U$ and $c \notin U$. Let $Y = U - \{b\} \cup \{c\}$. Then $U \sim Y$.*

Proof. Since $b \in U$ and $c \notin U$, we have $b \neq c$. Define $f : U \to Y$ by

$$f(x) = \begin{cases} c & \text{if } x = b \\ \\ x & \text{otherwise} \end{cases}$$

Since X has decidable equality, f is well-defined on X, and from the definitions of f and Y we see that $f : U \to Y$ and f is onto. Ad one-to-one: suppose $f(u) = f(v)$. Since X has decidable equality, u and v are either equal or not. If $u = v$, we are done. If $u \neq v$ then exactly one of u, v is equal to b, say $u = b$ and $v \neq b$. Then x$f(u) = c$ and $f(v) = v$. Since $f(u) = f(v)$ we have $v = c$. But $v \in U$ and $c \notin U$, contradiction. That completes the proof of the lemma.

Definition 3.23 (Dedekind)**.** *The class X is* **infinite** *if $X \sim Y$ for some $Y \subseteq X$ with $Y \neq X$.*

Theorem 3.24. *Let X be infinite, in the sense that it is similar to some $Y \subset X$ with $Y \neq X$. Then X is not finite.*

Remark. We expressed the theorem as "infinite implies not finite", but of course it is logically equivalent to "finite implies not infinite", since both forms amount to "not both finite and infinite."

Proof. It suffices to show that every finite set is not infinite. The formula to be proved is

$$X \in \mathsf{FINITE} \to \forall Y\,(Y \subseteq X \to X \sim Y \to X = Y)\}.$$

That formula is stratified, giving X and Y index 1, since the similarity relation can be defined in INF. Therefore induction is legal.

Base case, $X = \Lambda$. The only subset of Λ is Λ, so any subset of X is equal to X. That completes the base case.

Induction step. Suppose $X = A \cup \{b\}$, with $A \in \mathsf{FINITE}$ and $b \notin A$. Then

$Y \subseteq X$	by hypothesis
$X \in \mathsf{FINITE}$	by Lemma 3.7
$X \in \mathsf{DECIDABLE}$	by Lemma 3.3
$X \sim Y \;\wedge\; Y \subseteq X$	assumption
$f : X \to Y$	with f one-to-one and onto, by definition of $X \sim Y$
$Y \in \mathsf{FINITE}$	by Lemma 3.14
$Y \in \mathsf{DECIDABLE}$	by Lemma 3.3

Let $c = f(b)$ and $U = Y - \{c\}$. Let g be f restricted to A. Then $g : A \to U$ is one-to-one and onto (140 steps omitted). Thus $A \sim U$.

Since X has decidable equality, $b = c \vee b \neq c$. By Lemma 3.18, Y is a separable subset of X. Therefore $b \in Y \;\vee b \notin Y$. We can therefore argue by three cases: $b = c$, or $b \neq c$ and $b \in Y$, or $b \neq c$ and $b \notin Y$.

Case 1, $b = c$. Then $U \subseteq A$. By the induction hypothesis, we have $A = U$. Then $X = A \cup \{b\} = U \cup \{b\} = U \cup \{c\} = Y$. That completes Case 1.

Case 2, $b \neq c$ and $b \in Y$. Then

$f(p) = b$	for some $p \in A \cup \{b\}$, since f is onto Y
$p \neq b$	since $f(b) = c \neq b$, and f is one-to-one

Define

$$g = (f - \{\langle b, c\rangle\} - \{\langle p, b\rangle\}) \cup \{\langle p, c\rangle\}.$$

Then one can check that $g : A \to Y - \{b\}$ is one-to-one and onto. (It requires more than six hundred inference steps, here omitted.) We note that $A \cup \{b\}$ is finite, and therefore has decidable equality, which allows us to argue by cases whether $x = b$ or not, and whether $x = p$ or not.) Then

$A \sim Y - \{b\}$	since g is a similarity
$Y - \{b\} \subseteq A$	since $X = A \cup \{b\}$ and $Y \subseteq$X

Thus A is similar to its subset $Y - \{b\}$. Then by the induction hypothesis,

$$A = Y - \{b\} \tag{20}$$

Therefore $Y = A \cup \{b\} = X$. That completes Case 2.

Case 3: $b \neq c$ and $b \notin Y$. Since $Y \subseteq X = A \cup \{b\}$, and $b \notin Y$, we have $Y \subseteq A$. Then $f : A \to Y - \{c\} \subseteq A$. Then by the induction hypothesis,

$$Y - \{c\} = A. \tag{21}$$

Then $c \notin A$. But $X = A \cup \{b\}$, and $c = f(b) \in Y \subseteq A$, so $c \in A$. That contradiction completes Case 3, and that completes the proof of the induction step. That in turn completes the proof of the theorem.

Lemma 3.25. *A finite union of finite disjoint sets is finite. That is,*

$$\begin{aligned} & x \in \mathsf{FINITE} \ \wedge \ \forall u\,(u \in x \to u \in \mathsf{FINITE}) \\ & \wedge \ \forall u, v \in x\,(u \neq v \to u \cap v = \Lambda) \\ & \to \bigcup x \in \mathsf{FINITE}. \end{aligned}$$

Proof. By induction on the finite set x. Base case, $x = \Lambda$. Then $\bigcup x = \Lambda$, which is finite.

Induction step, $x = y \cup \{c\}$ with $c \notin y$. The induction hypothesis is that if all members of y are finite, and any two distinct members of y are disjoint, then $\bigcup y$ is finite. We have to prove that if all members of x are finite and any two distinct members of x are disjoint, then $\bigcup x \in \mathsf{FINITE}$. Assume all members of x are finite and any two distinct members of x are disjoint. Since the members of y are members of x, all the members of y are finite, and any two distinct members of y are disjoing. Then by the induction hypothesis, $\bigcup y$ is finite. A short argument from the definitions of union and binary union proves

$$\bigcup (y \cup \{c\}) = \left(\bigcup y\right) \cup c.$$

Since $x = y \cup \{c\}$, we have

$$\bigcup x \quad = \quad \left(\bigcup y\right) \cup c \tag{22}$$

Now c is finite, since every member of x is finite and $c \in x$. We have $\bigcup y \cap c = \Lambda$, since if p belongs to both $\bigcup y$ and c, then for some $w \in y$ we have $p \in w \cap c$, contradicting the hypothesis that any two distinct members of $x = y \cup \{c\}$ are disjoint. Then $\bigcup y \cup c$ is finite, by Lemma 3.11. Then $\bigcup x$ is finite, by (22). That completes the induction step, and that completes the proof of the lemma.

Lemma 3.26. *Suppose $c \notin x$. Then*

$$SSC(x) \subseteq SSC(x \cup \{c\}).$$

Proof. About 30 straightforward steps, which we choose to omit here.

Lemma 3.27. *Let A be any set. Then the intersection and union of two separable subsets of A are also separable subsets of A.*

Proof. Let X and Y be two separable subsets of A. Let $u \in A$. By definition of separability, we have

$$(u \in X \vee u \notin X) \ \wedge \ (u \in Y \vee u \notin Y).$$

I say that $X \cap Y$ is a separable subset of A. To prove that, we must prove

$$u \in X \cap Y \ \vee \ u \notin X \cap Y. \tag{23}$$

This can be proved by cases; there are four cases according to whether u is in X or not, and whether u is in Y or not. In each case, (23) is immediate. Hence $X \cap Y$ is a separable subset of A, as claimed. Similarly, $X \cup Y$ is a separable subset of A. That completes the proof of the lemma.

Lemma 3.28 (Finite DNS)**.** *For every finite set B we have*

$$\forall P\,(\forall x \in B\,(\neg\neg\, x \in P)) \to \neg\neg\, \forall x \in B\,(x \in P).$$

Remark. DNS stands for "double negation shift." Generally it is not correct to move a double negation leftward through $\forall x$; but this lemma shows that it is OK to do so when the quantifier is bounded by a finite set.

Proof. The formula of the lemma is stratified, giving x index 0, B index 1, and P index 1. Therefore we may proceed by induction on finite sets B. (Notice that the statement being proved by induction is universally quantified over P–that is important because in the induction step we need to substitute a different set for P; the proof does not work with P a parameter.)

Base case, $B = \Lambda$. The conclusion $\forall x \in \Lambda\, x \in P$ holds since $x \in \Lambda$ is false.

Induction step. Suppose $c \notin B$ and $B \in \mathsf{FINITE}$ and

$$\forall x \in B \cup \{c\}\,(\neg\neg\, x \in P).$$

By Lemma 3.4, B is empty or inhabited. We argue by cases.

Case 1, B is empty. Then $B \cup \{c\} = \{c\}$, so we must prove

$$\forall x\,(x \in \{c\} \to \neg\neg\, x \in P) \to \neg\neg\forall x\,(x \in \{c\} \to x \in P)$$

That is equivalent to

$$\forall x\,(x = c \to \neg\neg\, x \in P) \to \neg\neg\, \forall x\,(x = c \to x \in P)$$

That is, $\neg\neg\, c \in P \to \neg\neg\, c \in P$, which is logically valid. That completes case 1.

Case 2, B is inhabited. Fix u with $u \in B$. Then

$$\forall x \in B\,(\neg\neg\, x \in P)$$
$$\neg\neg\, c \in P$$

Since x does not occur in $c \in P$ we have

$$\forall x \in B\,(\neg\neg\, x \in P \;\wedge\; \neg\neg\, c \in P)$$
$$\forall x \in B\, \neg\neg\,(x \in P \;\wedge\; c \in P)$$

Define $Q = \{x : x \in P \;\wedge\; c \in P\}$, which is legal since the defining formula is stratified. Then

$$\forall x \in B\,(\neg\neg\, x \in Q) \tag{24}$$

Since P is quantified in the formula being proved by induction, we are allowed to substitute Q for P in the induction hypothesis; then with (24) we have

$$\neg\neg\, \forall x \in B\,(x \in Q) \qquad \text{by the induction hypothesis}$$
$$\neg\neg\, \forall x \in B\,(x \in P \;\wedge\; c \in P) \qquad \text{by the definition of } Q \tag{25}$$

Now we would like to infer

$$\neg\neg\,((\forall x \in B\,(x \in P)) \;\wedge\; c \in P), \tag{26}$$

which seems plausible as x does not occur in '$c \in P$'. In fact we have the equivalence of (25) and 26), since B is inhabited. (That was why we had to break the proof into cases according as B is empty or inhabited.) Then indeed (26) follows. By the definitions of union and unit class we have

$$(\forall x \in B\,(x \in P)) \;\wedge\; c \in P \leftrightarrow \forall x \in (B \cup \{c\})\,(x \in P).$$

Applying that equivalence to (26), we have the desired conclusion,

$$\neg\neg\,\forall x \in (B \cup \{c\})\,(x \in P).$$

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

Lemma 3.29. *Every subset of a finite set is not-not separable and not-not finite.*

Remark. We already know that separable subsets of a finite set are finite, and finite subsets of finite set are separable, but one cannot hope to prove every subset of a finite set is finite, because of sets like $\{x \in \{\Lambda\} : P$. That set is finite if and only if $P \;\vee\; \neg P$, by Lemma 3.4.

Proof. Let X be a finite set, and $A \subseteq X$. By Lemma 3.19, if A is a separable subset of X then A is finite. Double-negating that implication, if A is not-not separable, then it is not-not finite. Hence, it suffices to prove that not-not A is a separable subset of X. More formally, we must prove

$$\neg\neg\, X = A \cup (X - A) \tag{27}$$

We have

$\forall t \in X\,\neg\neg\,(t \in A \;\vee\; t \notin A)$	by logic
$\neg\neg\,\forall t \in X\, t \in A \;\vee\; t \notin A)$	by Lemma 3.28
$\neg\neg\, X = A \cup (X - A)$	by the definitions of union and difference

That is (27), so that completes the proof of the lemma.

Lemma 3.30. *Let* $x \in \mathsf{FINITE}$ *and* $y \in \mathsf{FINITE}$*. Then* $\neg\neg\,(x \cup y \in \mathsf{FINITE})$.

Remark. Lemma 3.11 shows the double negation can be dropped if x and y are assumed to be disjoint. It cannot be dropped in general, as $\{a\} \cup \{b\} \in \mathsf{FINITE}$ implies $a = b \;\vee a \neq b$, so if we could drop the double negation in this lemma, then every set would have decidable equality.

Proof. The formula is stratified, so we can prove it by induction on finite sets y, for a fixed finite set x.

Base case, $y = \Lambda$. We have $x \cup \Lambda = x$, which is finite by hypothesis. That completes the base case.

Induction step. Suppose $y \in \mathsf{FINITE}$, $x \cup y \in \mathsf{FINITE}$, and $c \notin y$. Then I say

$$c \notin x \to x \cup (y \cup \{c\}) \in \mathsf{FINITE} \tag{28}$$

To prove that:

$x \cup (y \cup \{c\}) = (x \cup y) \cup \{c\}$	by definition of union
$c \notin x \cup y$	since $c \notin x$
$x \cup (y \cup \{c\}) \in \mathsf{FINITE}$	

That completes the proof of (28).

We also have

$$c \in x \to x \cup (y \cup \{c\}) \in \mathsf{FINITE} \tag{29}$$

since $(x \cup y) \cup \{c\} = x \cup y \in \mathsf{FINITE}$.

We have by intuitionistic logic

$$\neg\neg\,(c \in x \ \vee\ c \notin x).$$

and by the induction hypothesis we have $\neg\neg\, x \cup y \in \mathsf{FINITE}$. Then by (28) and (29), we have

$$\neg\neg\,(x \cup y) \cup \{c\} \in \mathsf{FINITE}.$$

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

4. Frege cardinals

The formula in the following definition is stratifiable, so the definition can be given in INF. Specifically, we can give a index 0, x and z index 1, and κ index 2. Then κ^+ gets index 2, so the successor function $\kappa \mapsto \kappa^+$ is a function in INF.

Definition 4.1. *The successor of any set κ, denoted κ^+, is defined as*

$$\kappa^+ = \{x : \exists z, a\,(z \in \kappa \wedge a \notin z \wedge x = z \cup \{a\})\}.$$

Definition 4.2.

$$\mathsf{zero} \quad = \quad \{\Lambda\}$$

Definition 4.3. *The set $\mathbb{F}$ of finite Frege cardinals is the least set containing* $\mathsf{zero} = \{\Lambda\}$ *and containing κ^+ whenever it contains κ and κ^+ is inhabited. More precisely,*

$$\kappa \in \mathbb{F} \leftrightarrow \forall w\,(\mathsf{zero} \in w \ \wedge\ \forall \mu\,(\mu \in w \ \wedge\ (\exists z\,(z \in \mu^+)) \to \mu^+ \in w) \to \kappa \in w).$$

Remarks. The formula defining $\mathbb{F}$ is stratified, so the definition can be given in INF. According to that definition, if there were a largest finite cardinal κ, then κ^+ would be the empty set, not Frege zero, which is $\{\Lambda\}$. So in that case, the successor of the largest finite cardinal κ would not belong to $\mathbb{F}$, which does not contain Λ. Instead, in that case the result would be that successor does not map $\mathbb{F} \to \mathbb{F}$. Of course $\Lambda^+ = \Lambda$, so once that happened, more applications of successor would do nothing more. Note also that in general a finite cardinal is not a finite set; rather, the members of a finite cardinal are finite sets.

Lemma 4.4. *Let $\kappa \in \mathbb{F}$ and $x \in \kappa$. Then x is a finite set.*

Proof. Define

$$Z = \{x \in \mathbb{F} : \forall y \in x\,(y \in \mathsf{FINITE})\}.$$

The formula in the definition is stratifiable, so the definition is legal. We will show that Z is closed under the conditions defining $\mathbb{F}$. First, Frege zero $= \{\Lambda\}$ is in Z, since Λ is finite. To verify the second condition, assume $\kappa \in Z$ and κ^+ is inhabited; we must show $\kappa^+ \in Z$. Let $u \in \kappa^+$. Then there exists $x \in \kappa$ and there exists a such that $u = x \cup \{a\}$. Since $\kappa \in Z$, x is finite. Then by definition of FINITE, u is finite. That completes the proof that Z satisfies the second condition. Hence $\mathbb{F} \subseteq Z$. That completes the proof of the lemma.

Lemma 4.5 (Stratified induction)**.** *Let ϕ be a stratified formula (or weakly stratified with respect to x), so $\{x : \phi(x)\}$ exists. Then*

$$(\phi(\mathsf{zero}) \ \wedge\ \forall x\,(\phi(x) \ \wedge \exists u\,(u \in \ x^+) \to \phi(x^+)) \to \forall x\,\phi(x).$$

Proof. $Z := \{x : \phi(x)\}$ is definable and satisfies the closure conditions that define $\mathbb{F}$. Therefore $\mathbb{F} \subseteq Z$. That completes the proof of the lemma.

Remark. Note that when carrying out a proof by induction, during the induction step we get to assume that x^+ is inhabited.

We follow Rosser ([8], p. 372) in defining cardinal numbers: a cardinal number, or just "cardinal", is an equivalence class of the similarity relation $x \sim y$ of one-to-one correspondence:

Definition 4.6. *The class NC of cardinal numbers is defined by*

$$NC = \{\kappa : \forall u \in \kappa \forall v (v \in \kappa \leftrightarrow u \sim v)\}.$$

Remark. It would not do to use $\exists u$ instead of $\forall u$, since then Λ would not be a cardinal, but we need to allow for that possibility. We note that Rosser's definition is equivalent to ours.

The following two lemmas show that the members of $\mathbb{F}$ are indeed cardinals in that sense.

Corollary 4.7. *Every finite cardinal is inhabited.*

Proof. Lemma 4.5 justifies us in proving $\exists u (u \in \kappa)$ by induction on κ.

Base case: $\mathsf{zero} = \{\Lambda\}$ is inhabited.

Induction step: Suppose κ^+ is inhabited. Then κ^+ is inhabited. (We do not even need to use the induction hypothesis.) That completes the proof of the lemma.

Lemma 4.8. *If $\kappa \in \mathbb{F}$ and $x \in \kappa$ and $x \sim y$, then $y \in \kappa$.*

Remarks. This lemma shows that finite cardinals are cardinals, in the sense of equivalence classes under similarity.

Proof. Define

$$Z = \{\kappa \in \mathbb{F} : \forall x \in \kappa \forall y (x \sim y \to y \in \kappa)\}.$$

That formula can be stratified, since we have already shown that $x \sim y$ is definable in INF. Therefore the definition of Z is legal.

We will show Z contains Frege zero and is closed under Frege successor. Z contains Frege zero since the only member of Frege zero is the empty set, and the only set in one-to-one correspondence with the empty set is Λ itself.

Ad the closure under Frege successor: Suppose $\kappa \in Z$, and $x \in \kappa^+$, and $f : x \to y$ is one-to-one and onto. Then $x = u \cup \{a\}$ for some $u \in \kappa$ and $a \notin u$. Let g be f restricted to u, and let v be the range of g. Then $g : u \to v$ is one-to-one and onto. Since $\kappa \in Z$ and $u \in \kappa$, we have $v \in \kappa$. Let $b = f(a)$. Then $b \notin v$, since f is one-to-one. Then $v \cup \{b\} \in \kappa^+$.

I say that $v \cup \{b\} = y$. Let $p \in y$. Then $p = f(q)$ for some $q \in x$, since f maps x onto y. By Lemma 4.4, since $x \in \kappa^+$, x is finite. Since x is finite, it has decidable equality by Lemma 3.3. Therefore $q = a \vee q \neq a$. If $q = a$ then $p = f(a) = b \in \{b\}$. If $q \neq a$ then since $q \in x = u \cup \{a\}$ and $q \in x$, we have $q \in u$. Then by definition of v, $p = f(q) \in v$. Therefore $p \in v \cup \{b\}$. Since p was an arbitrary member of y, we have proved $y \subseteq v \cup \{b\}$. But $v \cup \{b\} \subseteq y$ is immediate, since $v \subseteq y$ and $b \in y$. Therefore $v \cup \{b\} = y$, as claimed.

Since $v \in \kappa$, it follows that $y \in \kappa^+$ as desired. Thus Z is closed under Frege successor. By the definition of $\mathbb{F}$, we have $\mathbb{F} \subseteq Z$. That completes the proof of the lemma.

Lemma 4.9. *Let $\kappa \in \mathbb{F}$ and $x, y \in \kappa$. Then $x \sim y$.*

Proof. By induction on κ. Similarity is defined by a stratified formula, so induction is legal. The base case is immediate as Frege zero has only one member. For the induction step, let x and y belong to κ^+. Then there exist u, v, a, b such that $u, v \in \kappa$ and $a \notin u$ and $b \notin v$ and $x = u \cup \{a\}$ and $y = v \cup \{b\}$. By the induction hypothesis, there is a one-to-one correspondence $g : u \to v$. We define $f : x \to y$ by

$$f(x) = \begin{cases} g(x) & \text{if } x \in u \\ \\ b & \text{if } x = a \end{cases}$$

By Lemma 4.4, x is finite. Since x is finite, it has decidable equality by Lemma 3.3. Since $a \notin u$, f is a function. Hence the domain of f is x. By Lemma 4.4, y is finite. Therefore by Lemma 3.3, y has decidable equality, so the range of f is y. I say that f is one-to-one. Suppose $f(x) = f(z)$. We must show $x = z$. Since y has decidable equality, we may argue by the following cases:

Case 1: $f(x) = f(z) = b$. Then since $b \notin v$, x and z are not in u, so $x = a$ and $z = a$. Then $x = z$ as desired.

Case 2: $f(x) = g(x)$ and $f(z) = g(z)$. Then $g(x) = g(z)$. Since g is one-to-one, we have $x = z$ as desired.

Therefore f is one-to-one, as claimed. Therefore $x \sim y$. That completes the induction step. That completes the proof of the lemma.

Definition 4.10. *Following Rosser, we define the cardinal of x to be*

$$Nc(x) = \{u : u \sim x\}.$$

Then the inhabited cardinals, that is, the inhabited members of NC, are exactly the sets of the form $Nc(x)$ for some x.

Lemma 4.11. *For all x, $x \in Nc(x)$*

lemma By Lemma 2.10, we have $x \sim x$. Then $x \in Nc(x)$ by Definition 4.10. That completes the proof of the lemma.

Lemma 4.12. *$Nc(x) = Nc(y)$ if and only if $x \sim y$.*

Proof. By Lemma 2.10, which says that the relation $\sim$ is an equivalence relation.

Lemma 4.13. *$c \notin x \to Nc(x \cup \{c\}) = Nc(x)^+$.*

Proof. By extensionality, it suffices to show that the two sides have the same members. That is, we must show, under the assumption $c \notin x$,

$$u \sim x \cup \{c\} \quad \leftrightarrow \quad \exists b, v\, (b \notin v \ \wedge \ v \sim x \ \wedge \ u = v \cup \{b\}). \tag{30}$$

Ad right-to-left: Suppose $b \notin v$ and $v \sim x$ and $u = v \cup \{b\}$. Let $f : v \to x$ be a similarity, and extend it to g defined by $g = f \cup \{\langle b, c\rangle\}$. Then g is a similarity from $v \cup \{b\}$ to $x \cup \{c\}$. That completes the right-to-left direction. f Ad left-to-right: Suppose $f : u \to x \cup \{c\}$ is a similarity. Since f is onto, there exists $b \in x$ with $f(b) = c$. Let $v = u - \{b\}$. Use this b and v on the right. Then $g = f - \{\langle b, c\rangle\}$ is a similarity from v to x. It remains to show $u = v \cup \{b\} = (u - \{b\}) \cup \{b\}$. That is,

$$z \in u \to z \in u \to z \neq b \ \vee \ z = b.$$

Let $z \in u$. Since f is a similarity from u to $x \cup \{c\}$, there is a unique $y \in x \cup \{c\}$ such that $\langle z, y\rangle \in f$. Then $z = b \leftrightarrow y = c$. Since $c \notin x$, and $y \in x \cup \{c\}$, $y = c \ \vee \ y \neq c$. Therefore $z = b \ \vee z \neq b$, as desired. Note that it is not necessary that z have decidable equality. That completes the left-to-right direction. That completes the proof of the lemma.

Lemma 4.14. $Nc(\Lambda) = \mathsf{zero}$.

Proof. By Definition 4.2, $\mathsf{zero} = \{\Lambda\}$. By definition, $Nc(\Lambda)$ contains exactly the sets similar to Λ. By Lemma 2.11, Λ is the only set similar to Λ. Therefore $Nc(\Lambda) = \{\Lambda\}$. Then $Nc(\Lambda) = \mathsf{zero}$ since both are equal to $\{\Lambda\}$. That completes the proof of the lemma.

Lemma 4.15. *For every set κ, if κ^+ is inhabited, then κ^+ contains an inhabited set, and every member of κ^+ is inhabited.*

Remark. Note that κ is not assumed to be a finite cardinal, or even a cardinal. Successor cannot take the value $\mathsf{zero} = \{\Lambda\}$ on any set. We will need that generality at a certain point.

Proof. By definition the members of κ^+ are exactly the sets of the form $x \cup \{a\}$ with $x \in \kappa$ and $a \notin x$. (That is true whether or not there are any such members.) But if κ^+ is inhabited, then there is at least one such member, and each such member $x \cup \{a\}$ is inhabited, since it contains a. That completes the proof of the lemma.

Lemma 4.16. *Frege successor does not take the value Frege zero on any set at all:* $\forall x \, (x^+ \neq \mathsf{zero})$.

Remark. This does not depend on the finiteness or not-finiteness of $\mathbb{F}$. If $\mathbb{F}$ is finite then eventually κ^+ is Λ, rather than zero, which is $\{\Lambda\}$, so even in that case Frege zero does not occur as a successor.

Proof. If $\kappa^+ = \{\Lambda\}$ then κ^+ is inhabited, but contains no inhabited set, contradicting Lemma 4.15. That completes the proof of the lemma. b

Lemma 4.17. *Every finite cardinal not equal to Frege zero is a successor.*

Proof. The set $Z = \{\kappa \in \mathbb{F} : \kappa = \mathsf{zero} \ \vee \ \exists \mu \, (\kappa = \mu^+)\}$ is definable in INF, since its defining formula is stratified. Z contains Frege zero and is closed under successor. Therefore, by definition of $\mathbb{F}$, $\mathbb{F} \subseteq Z$. That completes the proof of the lemma.

Lemma 4.18. $\mathsf{zero} \in \mathbb{F}$.

Proof. Let W be one of the sets whose intersection defines $\mathbb{F}$, i.e., W contains zero and is closed under inhabited successor. Then W contains zero. Since W was arbitrary, $\mathsf{zero} \in \mathbb{F}$. That completes the proof.

Lemma 4.19. $\mathbb{F}$ *is closed under inhabited successor.*

Proof. Suppose $\kappa \in \mathbb{F}$ and κ^+ is inhabited. Let W be one of the sets whose intersection defines $\mathbb{F}$, i.e., W contains zero and is closed under inhabited successor. By induction on κ, we can prove $\kappa \in W$. Since W is closed under inhabited successor, and $\kappa \in W$, and κ^+ is inhabited, we have $\kappa^+ \in W$. Since $\mathbb{F}$ is the intersection of all such sets W, and κ^+ belongs to every such W, we have $\kappa^+ \in \mathbb{F}$ as desired. That completes the proof of the lemma.

Lemma 4.20. $\mathsf{one} \in \mathbb{F}$.

Proof.

$$\begin{array}{rl}
\mathsf{zero} \in \mathbb{F} & \text{by Lemma 4.18} \\
\mathsf{one} = \mathsf{zero}^+ & \text{by the definition of } \mathsf{one} \\
\Lambda \in \mathsf{zero} & \text{by the definition of } \mathsf{zero} \\
\mathsf{zero} \notin \mathsf{zero} & \text{since } \mathsf{zero} = \{\Lambda\} \text{ and } \mathsf{zero} \neq \Lambda \\
\Lambda \cup \{\mathsf{zero}\} \in \mathsf{zero}^+ & \text{by definition of successor} \\
\exists u\,(u \in \mathsf{one}) & \text{since } \mathsf{one} = \mathsf{zero}^+ \\
\mathsf{one} \in \mathbb{F} & \text{by Lemma 4.19}
\end{array}$$

That completes the proof of the lemma.

Lemma 4.21. *The cardinal of a finite set is a finite cardinal. That is,*

$$\forall x \in \mathsf{FINITE}\,(Nc(x) \in \mathbb{F}).$$

Proof. The formula to be proved is stratified, so we can prove it by induction on finite sets.

Base case: By Lemma 4.14, $Nc(\Lambda) = \mathsf{zero}$. By Lemma 4.19, $\mathsf{zero} \in \mathbb{F}$.

Induction step: Let $x \in \mathsf{FINITE}$ and $c \notin x$. Consider $Nc(x \cup \{c\})$, which by Lemma 4.13 is $Nc(x)^+$. By the induction hypothesis, $Nc(x) \in \mathbb{F}$. By definition of $\mathbb{F}$, $Nc(x)^+ \in \mathbb{F}$. That completes the induction step. That completes the proof of the lemma.

Lemma 4.22. *Every member of* $\mathbb{F}$ *is inhabited.*

Proof. By induction we prove

$$\forall m\,(m \in \mathbb{F} \to \exists u\,(u \in m).$$

The formula is stratified, giving u index 0 and m index 1. For the base case, $\mathsf{zero} = \{\Lambda\}$ by definition, so zero is inhabited. For the induction step, we always suppose m^+ is inhabited, so there is nothing more to prove. That completes the proof of the lemma. To put the proof directly: the set of inhabited members of $\mathbb{F}$ contains zero and is closed under inhabited successor, so it contains $\mathbb{F}$.

Lemma 4.23. *A set similar to a finite set is finite.*

Proof. Let a be finite and $a \sim b$. Let $\kappa = Nc(a)$. Then

$$\begin{array}{rl}
\kappa \in \mathbb{F} & \text{by Lemma 4.21} \\
a \sim a & \text{by Lemma 2.10} \\
a \in \kappa & \text{by definition of } Nc(a) \\
b \in \kappa & \text{by Lemma 4.8} \\
b \in \mathsf{FINITE} & \text{by Lemma 4.4}
\end{array}$$

That completes the proof of the lemma.

5. Order on the cardinals

In this section, κ, μ, and λ will always be cardinals. We start with Rosser's classical definition (which is not the one we use).

Definition 5.1 (Rosser)**.**

$$\begin{aligned} \kappa \le \mu &:= \exists a, b\,(a \in \kappa \ \wedge\ b \in \mu) \\ \kappa < \mu &:= \kappa \le \mu \ \wedge\ \kappa \neq \mu. \end{aligned}$$

For constructive use, we need to add the requirement $b = a \cup (b - a)$, which says that b is a separable subset of a. Classically, every subset is separable, so the definition is classically equivalent to Rosser's.

Definition 5.2. *For cardinals κ and μ:*

$$\begin{aligned} \kappa \le \mu &:= \exists a, b\,(a \in \kappa \ \wedge\ b \in \mu \ \wedge\ a \subseteq b \ \wedge\ b = a \cup (b - a)) \\ \kappa < \mu &:= \kappa \le \mu \ \wedge\ \kappa \neq \mu. \end{aligned}$$

Definition 5.3. *The* **image of** a **under** f*, written* $f``a$*, is defined by*

$$f``a := Range(f \cap (a \times \mathbb{V})).$$

If f is a function then $f``a$ is the set of values $f(x)$ for $x \in a$.

Lemma 5.4. *The image of a separable subset under a similarity is a separable subset. More precisely, let $f : b \to c$ be a similarity and suppose $b = a \cup (b - a)$. Let $e = f``a$ be the image of a under f. Then $c = e \cup (c - e)$.*

Proof. We have

$$e \cup (c - e) \quad \subseteq \quad c \tag{31}$$

since $e \subseteq c$ and $c - e \subseteq c$. We have

$$c \quad \subseteq \quad e \cup (c - e) \tag{32}$$

since if $q \in c$ then $q = f(p)$ for some $p \in b$, and $p \in a \vee p \in b - a$, since $b = a \cup (b - a)$, and if $p \in a$ then $q \in e$, while if $p \in b - a$ then $q \in c - e$. Combining (31) and (32), we have $c = e \cup (c - e)$ as desired. That completes the proof of the lemma.

Lemma 5.5. *Let $f : a \to b$ be a similarity, and let $x \subseteq a$. Let g be f restricted to x. Then $g : x \to f``x$ is a similarity.*

Proof. Straightforward; requires about 75 inferences that we choose to omit here.

Lemma 5.6. *The ordering relation $\le$ is transitive on $\mathbb{F}$.*

Proof. Suppose $\kappa \le \lambda$ and $\lambda \le \mu$. We must show $\kappa \le \mu$. Since $\kappa < \lambda$ and $\lambda < \mu$, there exist $a \in \kappa$, $b, c \in \lambda$, and $d \in \mu$ such that $a \subseteq b$ and $c \subseteq d$, and $b = a \cup (b - a)$, and $d = c \cup (d - c)$. By Lemma 4.9, $b \sim c$, since both belong to λ. Let $f : b \to c$ be one-to-one and onto. Let $e = f``a$. Then $e \subseteq c$ and $a \sim e$. So $e \in \kappa$, by Lemma 4.8. Then $e \subseteq d$. By Lemma 5.4 we have

$$c \quad = \quad e \cup (c - e) \tag{33}$$

Now I say that $d = e \cup (d - e)$.

$$\begin{aligned} e \cup (d - e) &= e \cup ((c \cup (d - c)) - e) && \text{since } d = c \cup (d - c) \\ &= e \cup (c - e) \cup ((d - c) - e) && \text{since } (p \cup q) - r = (p - r) \cup (q - r) \\ &= c \cup ((d - c) - e) && \text{by (33)} \\ &= c \cup (d - c) && \text{since } e \subseteq c \\ &= d && \text{since } d = c \cup (d - c) \end{aligned}$$

as desired. Then $\kappa \le \mu$ as desired. That completes the proof of the lemma.

Lemma 5.7. *(i) If two finite cardinals have a common member, then they are equal.*
(ii) Two distinct finite cardinals are disjoint.

Proof. Part (ii) is the contrapositive of (i), so it suffices to prove (i). Let κ and μ belong to $\mathbb{F}$. Suppose x belongs to both κ and μ. We must show $\kappa = \mu$. By extensionality, it suffices to show that κ and μ have the same members. Let $y \in \kappa$. Then by Lemma 4.9, $y \sim x$. By Lemma 4.8, $y \in \mu$. Therefore $\kappa \subseteq \mu$. Similarly $\mu \subseteq \kappa$. That completes the proof of the lemma.

Lemma 5.8. *For finite cardinals κ and μ,*

$$\kappa < \mu \leftrightarrow \exists x, y\,(x \in \kappa \ \wedge\ y \in \mu \ \wedge\ x \subset y \ \wedge\ y = x \cup (y - x)).$$

Proof. Left to right: Suppose $\kappa < \mu$. Then by definition of $<$, $\kappa \le \mu$ and $\kappa \ne \mu$. By definition of $\le$, there exist x and y with $x \in \kappa$, $y \in \mu$, and $x \subseteq y$ and $y = x \cup (y - x)$. By Lemma 5.7, which applies because $\kappa \ne \mu$, we have $x \ne y$. Therefore $x \subset y$ as desired. That completes the proof of the left-to-right implication.

Right to left: Suppose $x \in \kappa$ and $y \in \mu$ and $x \subset y$ and $y = x \cup (y - x)$. Then $\kappa \le \mu$ by definition. We must show $\kappa \ne \mu$. If $\kappa = \mu$ then $y \sim x$, by Lemma 4.9. Then y is similar to a proper subset of y, namely x. Since $y \in \mu$ and $\mu \in \mathbb{F}$, by Lemma 4.4, y is finite. Since y is similar to a proper subset of itself (namely x), Theorem 3.24 implies that y is not finite, which is a contradiction. That completes the proof of the lemma.

Lemma 5.9. *Let $\kappa, \mu \in \mathbb{F}$, with μ inhabited. Then*

$$\kappa \le \mu \leftrightarrow \forall b \in \mu\, \exists a \in \kappa\,(a \subseteq b \ \wedge\ b = a \cup (b - a)).$$

Proof. Left-to-right. Suppose $\kappa \le \mu$. Then by definition of $\le$, there exist $x \in \kappa$ and $y \in \mu$ with $x \subseteq y$ and

$$y \quad = \quad x \cup (y - x) \tag{34}$$

Let $b \in \mu$; we must show there exists $a \in \kappa$ with $a \subseteq b$ and $b = a \cup (b - a)$.

We have $b \sim y$ by Lemma 4.9. So $y \sim b$. Let $f : y \to b$ be one-to-one and onto. Let $a = f``(x)$. Then $a \subseteq b$ and $x \sim a$. By Lemma 4.8, $a \in \kappa$. By Lemma 5.4 and (34), we have $b = a \cup (b - a)$. That completes the proof of the left-to-right implication.

Right-to-left. Suppose $\forall b \in \mu\, \exists a \in \kappa\,(a \subseteq b \ \wedge\ b = a \cup (b - a))$. Since μ is a inhabited, there exists $b \in \mu$. Then $\exists a \in \kappa\,(a \subseteq b \ \wedge\ b = a \cup (b - a))$. That completes the proof of the lemma.

Lemma 5.10. *Suppose $\kappa \in \mathbb{F}$ and $x \in \kappa^+$ and $c \in x$. Then $x - \{c\} \in \kappa$.*

Remark. We will use this in the proof that successor is one to one, so we cannot use that fact to prove this lemma.

Proof. Since $x \in \kappa^+$, there exists $z \in \kappa$ and $a \notin z$ such that $x = z \cup \{a\}$. Since $c \in x$, we have $c \in z \ \vee\ c = a$. If $c = a$ then $z = x - \{c\} \in \kappa$ and we are done. Therefore we may assume $c \in z$ and $c \ne a$.

Since $a \ne c$ we have

$$(z \cup \{a\}) - \{c\} = (z - \{c\}) \cup \{a\} \tag{35}$$

Since $x \in \kappa^+$, x is finite, by Lemma 4.4. By Lemma 3.3, x has decidable equality. Then

$$\begin{array}{rcll} z & \sim & (z - \{c\} \cup \{a\} & \text{by Lemma 3.22} \\ & = & (z \cup \{a\}) - \{c\} & \text{by (35)} \end{array}$$

Then by Lemma 4.8 and the fact that $z \in \kappa$, we have

$$(z \cup \{a\}) - \{c\} \in \kappa \tag{36}$$

(37)

Since $z \cup \{a\} = x$, that implies $x - \{c\} \in \kappa$, which is the conclusion of the lemma. That completes the proof of the lemma.

Lemma 5.11. *For finite cardinals κ and μ, if μ^+ is inhabited, we have*

$$\kappa \le \mu \leftrightarrow \kappa^+ \le \mu^+.$$

Proof. Left to right. Suppose $\kappa \le \mu$. Since μ^+ is inhabited, there is some $y \in \mu$ and some $c \notin y$, so $y \cup \{c\} \in \mu^+$. By Lemma 5.9, there is a separable subset $x \subseteq y$ with $x \in \kappa$. Then $x \cup \{c\} \in \kappa^+$ and $x \cup \{c\} \subset y \cup \{c\}$. We have to show that

$$y \cup \{c\} \quad = \quad (x \cup \{c\}) \cup (y \cup \{c\} - (x \cup \{c\})). \tag{38}$$

Left-to-right of (38): Suppose $u \in y \cup \{c\}$. Then $u \in y$ or $u = c$. If $u = c$ then $u \in x \cup \{c\}$, so u belongs to the right side of (38). Now $y \cup \{c\}$ is finite (by Lemma 4.4), and hence has decidable equality by Lemma 3.3. Therefore $u = c \ \vee \ u \ne c$; so we can assume $u \ne c$. If $u \in y$ then, since $y = x \cup (y - x)$, $u \in x \ \vee \ u \notin x$. If $u \in x$ then $u \in x \cup \{c\}$ and hence u belongs to the right side of (38). If $u \notin x$ then $u \in y \cup \{c\} - (x \cup \{c\})$, and hence u belongs to the right side of (38). That completes the proof of the left-to-right direction of (38).

Right-to-left of (38). Since $x \subseteq y$ we have

$$x \cup \{c\} \subseteq y \cup \{c\}$$

and

$$y \cup \{c\} - (x \cup \{c\}) \subseteq y \cup \{c\}.$$

Hence the right side of (38) is a subset of the left side. That completes the proof of (38).

Therefore $\kappa^+ \le \mu^+$. That completes the proof of the left-to-right direction of the lemma.

Right-to-left. Suppose $\kappa^+ \le \mu^+$. Then there exist $x \in \kappa^+$ and $y \in \mu^+$ with $x \subseteq y$ and $y = x \cup (y - x)$. By Lemma 4.15, x is inhabited, so there exists $c \in x$. Since $x \subseteq y$, also $c \in y$. Then by Lemma 5.10, $x - \{c\} \in \kappa$ and $y - \{c\} \in \mu$. Since $y \in \mu^+$, y is finite, by Lemma 4.4. By Lemma 3.3, y has decidable equality. Then

$$u \in y \to u = c \ \vee \ u \ne c \tag{39}$$

. Since $y = x \cup (y - x)$, we have

$$u \in y \to u \in x \ \vee \ u \notin x \tag{40}$$

Then by (39) and (40), we have

$$u \in y \to u \in (x - \{c\}) \ \vee \ u \notin (x - \{c\}). \tag{41}$$

It follows from (41) that

$$y - \{c\} \quad = \quad ((y - \{c\}) - (x - \{c\})) \cup (x - \{c\})$$

Therefore $\kappa \le \mu$. That completes the proof of the lemma.

Lemma 5.12. *For λ and μ in $\mathbb{F}$, if $\lambda+$ and μ^+ are inhabited, then*

$$\lambda = \mu \leftrightarrow \lambda^+ = \mu^+.$$

Proof. Left to right is immediate. We take up the right to left implication. Suppose $\kappa^+ = \mu^+$. By Lemma 5.7, it suffices to show that $\kappa \cap \mu$ is inhabited. Since κ^+ is inhabited, there exists $y \in \kappa^+$. By definition of successor, y has the form $y = x \cup \{a\}$ for some $x \in \kappa$ and $a \notin x$. We will prove $x \in \mu$. Since $\mu^+ = \kappa^+$ we have $x \cup \{a\} \in \mu^+$. Then by Lemma 5.10, $x \cup \{a\} - \{a\} \in \mu$. Since $x \cup \{a\} \in \mu^+$, $x \cup \{a\}$ is finite, by Lemma 4.4. By Lemma 3.3, $x \cup \{a\}$ has decidable equality. Then $x \cup \{a\} - \{a\} = x$, so $x \in \mu$. Then $x \in \kappa \cap \mu$ as claimed. That completes the proof of the lemma.

Lemma 5.13. *For finite cardinals κ and μ, if κ^+ and μ^+ are inhabited we have*

$$\kappa < \mu \leftrightarrow \kappa^+ < \mu^+.$$

Proof. By Lemma 5.11 and Lemma 5.12. The formal details require about 40 inferences, which we choose to omit.

Lemma 5.14. *Let x be a separable subset of y, that is, $x \subseteq y$ and $y = x \cup (y - x)$. Then $y - x = \Lambda \leftrightarrow y = x$.*

Proof. Suppose $x \subseteq y$ and $y = x \cup (y - x)$. Left to right: suppose $y - x = \Lambda$; we must show $y = x$. If $u \in x$ then by $y = x \cup (y - x)$ we have $u \in y$. Conversely, if $u \in y$ then $u \in x \ \vee \ u \notin x$. If $u \in x$ we are done. If $u \notin x$ then $u \in y - x$, so $u \in y$. That completes the left-to-right direction. Right to left: Suppose $y = x$. Then $y - x = x - x = \Lambda$. That completes the proof of the lemma.

Lemma 5.15. *For finite cardinals κ and μ, if κ^+ and μ^+ are inhabited we*

$$\kappa < \mu \leftrightarrow \kappa^+ < \mu^+.$$

Proof. Left-to-right. Suppose $\kappa < \mu$. By definition that means $\kappa \le \mu$ and $\kappa \ne \mu$. By Lemma 5.11, $\kappa^+ \le \mu^+$. We have to show $\kappa^+ \ne \mu^+$. Suppose $\kappa^+ = \mu^+$. Since μ^+ is inhabited, there is an element $y \cup \{c\}$ of μ^+ with $y \in \mu$ and $c \notin y$. Since $\kappa^+ = \mu^+$, we also have $y \cup \{c\} \in \kappa^+$. Since $y \in \mu$, by Lemma 4.4, y is finite. Since μ^+ is inhabited, μ is also inhabited. Since $\kappa < \mu$, by Lemma 5.9, there exists a separable subset x of y with $x \in \kappa$. By Lemma 4.4, x is finite. By Lemma 3.20, $y - x$ is finite. Since $\kappa \ne \mu$, we have $x \ne y$, by Lemma 5.7. Then, since x is a separable subset of y, $y - x$ is not empty, by Lemma 5.14. Since it is finite, by Lemma 3.4, $y - x$ is inhabited. Hence there exists some $b \in y$ with $b \notin x$. Then $x \cup \{b\} \in \kappa^+$. Then $x \cup \{b\}$ and $y \cup \{c\}$ both belong to κ^+.

Note that $x \cup \{b\}$ and $y \cup \{c\}$ are finite (by Lemma 4.4), and hence have decidable equality (by Lemma 3.3). Hence $y = (y \cup \{c\}) - \{c\}$; then by Lemma 5.10 we have $y \in \kappa$. But from the start we had $y \in \mu$. Then by Lemma 5.7, we have $\kappa = \mu$, contradicting the hypothesis $\kappa < \mu$. Hence the assumption $\kappa^+ = \mu^+$ has led to a contradiction. Hence $\kappa^+ < \mu+$. That completes the proof of the left-to-right direction of the lemma.

Right-to-left: Suppose $\kappa^+ < \mu^+$. Then $\kappa^+ \le \mu^+$ and $\kappa^+ \ne \mu^+$. By Lemma 5.11, $\kappa \le \mu$, and since successor is a function, $\kappa \ne \mu$. That completes the proof of the lemma.

Definition 5.16. *We define names for the first few integers (repeating the definition of* zero*, which has already been given).*

$$\begin{aligned} \mathsf{zero} &= \{\Lambda\} \\ \mathsf{one} &= \mathsf{zero}^+ \\ \mathsf{two} &= \mathsf{one}^+ \\ \mathsf{three} &= \mathsf{two}^+ \\ \mathsf{four} &= \mathsf{three}^+ \end{aligned}$$

Lemma 5.17. *We have*

$$\forall \kappa \in \mathbb{F}\,(\kappa = \mathsf{zero} \ \vee\ \kappa \neq \mathsf{zero}).$$

Proof. By induction on κ. More explicitly, define

$$W := \mathbb{F} \cap ((\mathbb{F} - \{\mathsf{zero}\}) \cup \{\mathsf{zero}\}).$$

We will show that W satisfies the conditions defining $\mathbb{F}$. Specifically $0 \in W$ (which is immediate from the definitions of W and union), and W is closed under (inhabited) Frege successor. Suppose $\kappa \in W$ and κ^+ is inhabited. We have to show $\kappa^+ \in W$. By Lemma 4.16, $\kappa^+ \neq \mathsf{zero}$. By definition of W, $\kappa \in \mathbb{F}$. By definition of $\mathbb{F}$, $\kappa^+ \in \mathbb{F}$; therefore $\kappa^+ \in \mathbb{F} - \{\mathsf{zero}\}$. Therefore $\kappa^+ \in W$, as claimed.

Then by definition of $\mathbb{F}$ (or, if you prefer, "by induction on κ"), $\mathbb{F} \subseteq W$. Then by the definition of union, $\kappa \in \mathbb{F} \to \kappa = \mathsf{zero} \ \vee\ \kappa \neq \mathsf{zero}$. That completes the proof of the lemma.

Theorem 5.18. *For finite cardinals κ and μ, we have*

$$\kappa < \mu \vee \kappa = \mu \vee \mu < \kappa$$

and

$$\neg\,(\kappa < \mu \ \wedge\ \mu < \kappa).$$

Proof. We prove by induction on κ that for all μ we have the assertion in the statement of the lemma. Lemma 4.5 justifies this method of proof. The formula is stratified since the relation $x < y$ is definable.

Base case: We have to prove

$$\mathsf{zero} < \mu \ \vee\ \mathsf{zero} = \mu \ \vee\ \mu < \mathsf{zero}$$

and exactly one of the three holds. If $\mu \leq \mathsf{zero}$, then we would have $x \in \mu$ and x a separable subset of y and $y \in \mathsf{zero}$; but the only member of zero is Λ, so $x = y = \Lambda$. Then $\Lambda \in \mu$ and $\Lambda \in \mathsf{zero}$, so by Lemma 5.7, $\mu = \mathsf{zero}$. Thus $\mu < \mathsf{zero}$ is impossible and $\mu \leq \mathsf{zero}$ if and only if $\mu = \mathsf{zero}$. If $\mu \in \mathbb{F}$ then by Lemma 5.17, $\mu = \mathsf{zero} \vee \mu \neq \mathsf{zero}$; and if $\mu \neq \mathsf{zero}$ then $\mathsf{zero} < \mu$, since Λ is a separable subset of any $x \in \mu$.

Induction step: Suppose κ^+ is inhabited. We have to prove

$$\kappa^+ < \mu \ \vee\ \kappa^+ = \mu \ \vee\ \mu < \kappa^+ \tag{42}$$

By Lemma 5.17, we have $\mu = \mathsf{zero} \ \vee\ \mu \neq \mathsf{zero}$. If $\mu = \mathsf{zero}$, we are done by the base case. If $\mu \neq \mathsf{zero}$, then by Lemma 4.17, $\mu = \lambda^+$ for some $\lambda \in \mathbb{F}$. By Corollary 4.7, λ^+ is inhabited. We have to prove

$$\kappa^+ < \lambda^+ \ \vee \kappa^+ = \mu^+ \ \vee\ \mu^+ < \lambda^+. \tag{43}$$

By the induction hypothesis we have

$$\kappa < \lambda \ \vee \kappa = \mu \ \vee \ \mu < \lambda.$$

and exactly one of the three holds. By Lemma 5.15 and Lemma 5.12, each disjunct is equivalent to one of the disjuncts of (43). That completes the induction step. That completes the proof of the theorem.

Corollary 5.19. *$\mathbb{F}$ has decidable equality. Precisely,*

$$\forall \kappa, \mu \in \mathbb{F} \, (\kappa = \mu \ \vee \ \kappa \neq \mu).$$

Proof. Let $\kappa, \mu \in \mathbb{F}$. We must show $\kappa = \mu \ \vee \kappa \neq \mu$. By Theorem 5.18, we have $\kappa < \mu$ or $\kappa = \mu$ or $\mu < \kappa$, and exactly one of the disjuncts holds. Therefore $\kappa \neq \mu$ is equivalent to $\kappa < \mu \ \vee \ \mu < \kappa$. That completes the proof of the corollary.

Lemma 5.20. *For all $\kappa \in \mathbb{F}$, we have $\kappa \le \kappa$.*

Proof. Suppose $\kappa \in \mathbb{F}$. By Corollary 4.7, κ is inhabited. Let $a \in \kappa$. Since a is a separable subset of a, we have $\kappa \le \kappa$ by the definition of $\le$. That completes the proof.

Lemma 5.21. *For $\kappa, \mu \in \mathbb{F}$ we have*

$$\kappa \le \mu \leftrightarrow \kappa < \mu \ \vee \ \kappa = \mu.$$

Proof. Suppose $\kappa, \mu \in \mathbb{F}$. By Theorem 5.18 we have $\kappa < \mu \ \vee \ \kappa = \mu \ \vee \ \mu < \kappa$, and exactly one of the three disjuncts holds.

Left to right: Suppose $\kappa \le \mu$. By Definition 5.2, there exist a and b with $a \in \kappa$, $b \in \mu$, $a \subseteq b$, and $b = a \cup (b - a)$. By Lemma 4.4, a and b are finite. By Lemma 3.20, $b - a$ is finite. By Lemma 3.4, $b - a$ is empty or inhabited.

Case 1, $b - a = \Lambda$. I say $b = a$. By extensionality, it suffices to prove $t \in b \leftrightarrow t \in a$. Left to right: assume $t \in b$. Since $b = a \cup (b - a)$ we have $t \in a \ \vee \ t \in b - a$. But $t \notin b - a$, since $b - a = \Lambda$. Therefore $t \in a$. Right to left: assume $t \in a$. Since $a \subseteq b$ we have $t \in b$. Therefore $b = a$ as claimed.

Then $a \in \kappa \cap \mu$. Then by Corollary 5.7, $\kappa = \mu$. That completes Case 1.

Case 2, $b - a$ is inhabited. Then a is a proper subset of b. By Lemma 5.8, $\kappa < \mu$. That completes Case 2. That completes the left to right direction.

Right to left: Suppose $\kappa < \mu$. Then by definition of $<$, we have $\kappa \le \mu$. On the other hand, if $\kappa = \mu$ then $\kappa \le \mu$ by Lemma 5.20. That completes the proof of the lemma.

Lemma 5.22. *For $\kappa, \mu \in \mathbb{F}$ we have*

$$\kappa \le \mu \ \wedge \ \mu \le \kappa \rightarrow \kappa = \mu.$$

Proof. By Lemma 5.21, it suffices to prove

$$(\kappa < \mu \ \vee \ \kappa = \mu) \ \wedge \ (\mu < \kappa \vee \mu = \kappa) \rightarrow \kappa = \mu. \tag{44}$$

By Theorem 5.18,

$$\kappa < \mu \ \vee \ \kappa = \mu \ \vee \ \mu < \kappa$$

and exactly one of the three disjuncts holds. Now (44) follows by propositional logic.

Lemma 5.23. *Suppose $\kappa < \mu \le \lambda$, where $\kappa, \mu, \lambda \in \mathbb{F}$. Then $\kappa < \lambda$.*

Proof. By Lemma 5.6, we have $\kappa \leq \lambda$. We must show $\kappa \neq \lambda$. Suppose $\kappa = \lambda$. Since $\kappa < \mu$ we have $\lambda < \mu$. Hence $\lambda \leq \mu$. By hypothesis $\mu \leq \lambda$. By Lemma 5.22, $\mu = \lambda$, contradicting $\mu < \lambda$. That completes the proof of the lemma.

Lemma 5.24. *Let $\kappa, \lambda, \mu \in \mathbb{F}$ and suppose $\kappa \leq \lambda < \mu$ Then $\kappa < \mu$.*

Proof. By Lemma 5.6, we have $\kappa \leq \mu$. Since $\kappa < \mu$ is defined as $\kappa \leq \mu$ and $\kappa \neq \mu$, it only remains to show $\kappa \neq \mu$. Suppose $\kappa = \mu$. Then $\kappa \leq \lambda$ and $\lambda \leq \kappa$. By Theorem 5.18, we have $\kappa = \lambda$, contradiction. That completes the proof of the lemma.

Lemma 5.25. *Let $\kappa, \lambda, \mu \in \mathbb{F}$ and suppose $\kappa < \lambda < \mu$ Then $\kappa < \mu$.*

Proof. Since $\kappa < \lambda$ we have $\kappa \leq \lambda$, by the definition of $<$. Then by Lemma 5.23, $\kappa < \mu$. That completes the proof of the lemma.

Lemma 5.26. *Let $\kappa^+ \in \mathbb{F}$. Suppose κ^+ is inhabited. Then $\kappa < \kappa^+$.*

Proof. Since $\kappa^+ \in \mathbb{F}$ and κ^+ is inhabited, there exists $x \in \kappa^+$. Then $x = y \cup \{c\}$ for some $y \in \kappa$ and $c \notin x$. Then $x - y = \{c\}$. By Lemma 4.4, since $x \in \kappa^+$, x is finite. By Lemma 3.3, x has decidable equality. Therefore $x = y \cup \{c\} = y \cup (x - y)$. Then $y \subseteq x$. It is a proper subset, since $c \in x$ but $c \notin y$. Now, we will use the right-to-left direction of Lemma 5.8. $\kappa < \kappa^+$, substituting κ^+ for μ. That gives us

$$\exists x, y\, (x \in \kappa \ \wedge \ y \in \kappa^+ \ \wedge \ x \subset y \ \wedge \ y = x \cup (y - x) \to \kappa < \kappa^+.$$

Then take (y, x) for (x, y) in the hypothesis. That yields

$$y \in \kappa \ \wedge \ x \in \kappa^+ \ \wedge \ y \subset x \ \wedge \ x = y \cup (x - y) \to \kappa < \kappa^+.$$

Since we have verified all four hypotheses, we may conclude $\kappa < \kappa^+$. That completes the proof of the lemma.

Lemma 5.27. *For all $m \in \mathbb{F}$, we do not have $m^+ \leq m$.*

Proof. Suppose $m \in \mathbb{F}$ and $m^+ \leq m$. By the definition of $\leq$, m^+ is inhabited. Then by Lemma 5.26, we have $m < m^+$, which contradicts Theorem 5.18, since $m^+ \leq m$. That completes the proof of the lemma.

Lemma 5.28. *For $x \in \mathbb{F}$, $x \not< x$.*

Proof. Immediate from Theorem 5.18, since $x = x$.

Lemma 5.29. *For $x \in \mathbb{F}$ we have $x \not< \mathsf{zero}$.*

Proof. Suppose $x < \mathsf{zero}$. We will derive a contradiction.

$x \leq \mathsf{zero}$	by definition of $<$
$a \in x \wedge a \subset b \wedge b \in \mathsf{zero}$	for some a, b, by definition of $\leq$
$b \in \{\Lambda\}$	since $\mathsf{zero} = \{\Lambda\}$
$b = \Lambda$	by Lemma 2.3
$a = \Lambda$	since $a \subset b$
$\Lambda \in x \cap \mathsf{zero}$	by definition of intersection
$x = \mathsf{zero}$	by Lemma 5.7
$\mathsf{zero} < \mathsf{zero}$	since $x < \mathsf{zero}$
$\neg\, \mathsf{zero} < \mathsf{zero}$	by Lemma 5.28

That contradiction completes the proof of the lemma.

Lemma 5.30. *For $\kappa, \mu \in \mathbb{F}$, if $\kappa < \mu$, then $\kappa^+ \le \mu$.*

Proof. Suppose $\kappa < \mu$. Then there exists $a \in \kappa$ and $b \in \mu$ such that $b = a \cup (b - a)$. Then

$$\begin{array}{rl} b \in \mathsf{FINITE} \ \wedge \ a \in \mathsf{FINITE} & \text{by Lemma 4.4} \\ b - a \in \mathsf{FINITE} & \text{by Lemma 3.20} \\ b - a = \Lambda \ \vee \exists u\,(u \in b - a) & \text{by Lemma 3.4} \end{array}$$

We argue by cases.

Case 1, $b - a = \Lambda$. Then $b = a$, so $a \in \kappa \cap \mu$, so by Lemma 5.7, $\kappa = \mu$, contradicting $\kappa < \mu$.

Case 2, $\exists c\,(c \in b - a)$. Fix c. Then

$$\begin{array}{rl} a \cup \{c\} \in \kappa^+ & \text{by the definition of successor} \\ a \cup \{c\} \subseteq b & \text{since } c \in b \\ b = (a \cup \{c\} \cup (b - (a \cup \{c\}) & \text{by Lemma 5.19} \\ \kappa^+ \le \mu & \text{by the definition of } \le. \end{array}$$

That completes the proof of the lemma.

Lemma 5.31. *If $a < b$ and $a, b \in \mathbb{F}$ then $a^+ \in \mathbb{F}$.*

Proof. Suppose $a < b$ and $a, b \in \mathbb{F}$. By the definition of $<$, we have $a \le b$ and $a \ne b$. By the definition of $\le$, there exists $v \in b$ and $u \in a$ with $u \in SSC(v)$. Then

$$\begin{array}{rl} v \in \mathsf{FINITE} & \text{by Lemma 4.4} \\ u \in \mathsf{FINITE} & \text{by Lemma 3.19} \\ v - u \in \mathsf{FINITE} & \text{by Lemma 3.20} \\ v - u \ne \Lambda & \text{by Lemma 5.7, since } a \ne b \\ \exists c\,(c \in v - u) & \text{by Lemma 3.4} \\ c \in v - u & \text{fixing } c \\ u \cup \{c\} \in a^+ & \text{by definition of successor} \\ a^+ \in \mathbb{F} & \text{by Lemma 4.19} \end{array}$$

That completes the proof of the lemma.

Lemma 5.32. *For $\kappa, \mu \in \mathbb{F}$, we have*

$$\kappa \le \mu^+ \to \kappa \le \mu \ \vee \ \kappa = \mu^+.$$

If we also assume $\mu^+ \in \mathbb{F}$ then we have

$$\kappa \le \mu^+ \leftrightarrow \kappa \le \mu \ \vee \ \kappa = \mu^+.$$

Remark. We cannot replace the $\to$ with $\leftrightarrow$ without the extra assumption, because if $\kappa \le \mu$ there is no guarantee that $\mu^+ \in \mathbb{F}$.

Proof. Suppose $\kappa \le \mu^+$. Then by Lemma 5.21,

$$\kappa < \mu^+ \vee \kappa = \mu^+.$$

If $\kappa = \mu^+$ we are done; so we may suppose $\kappa < \mu^+$. Then

$$\begin{aligned} \kappa^+ &\le \mu^+ && \text{by Lemma 5.30} \\ \exists u\,(u \in \mu^+) && &\text{by the definition of } \le \\ \exists u\,(u \in \kappa^+) && &\text{by the definition of } \le \\ \kappa &\le \mu && \text{by Lemma 5.11} \end{aligned}$$

That completes the proof of the lemma.

Lemma 5.33. *For $\kappa, \mu \in \mathbb{F}$, we have*

$$\kappa < \mu^+ \to \kappa < \mu \ \vee \ \kappa = \mu.$$

If we also assume $\mu^+ \in \mathbb{F}$ then we have

$$\kappa < \mu^+ \leftrightarrow \kappa < \mu \ \vee \ \kappa = \mu.$$

Proof. Left to right. Suppose $\kappa < \mu^+$. Then by the definition of $<$, $\kappa \le \mu^+$ and $\kappa \neq \mu^+$. By Lemma 5.32, $\kappa \le \mu$. By Lemma 5.21, $\kappa < \mu \ \vee \ \kappa = \mu$ as desired.

Right to left. Assume $\mu^+ \in \mathbb{F}$. Then μ^+ is inhabited, by Lemma 4.7. If $\kappa = \mu$ then $\kappa < \mu^+$ by Lemma 5.26. If $\kappa < \mu$ then $\kappa < \mu^+$ by Lemma 5.25. That completes the proof of the lemma.

Lemma 5.34. $\forall m \in \mathbb{F}\,(\neg\,(m < \mathsf{zero}))$.

Proof. By definition, $\mathsf{zero} = \{\Lambda\}$. Suppose $m \in \mathbb{F}$ and $m < \mathsf{zero}$. By definition of $<$, $m \le \mathsf{zero}$ and $m \neq \mathsf{zero}$. By definition of $\le$, there exist a and b with $a \in m$ and $b \in \mathsf{zero}$ and $a \in SSC(b)$. Since $\mathsf{zero} = \{\Lambda\}$ we have $b = \Lambda$. The only separable subset of Λ is Λ, so $a = \Lambda$. Then by Lemma 5.7, $m = \mathsf{zero}$. But that contradicts $m \neq \mathsf{zero}$. Therefore the assumptions $m \in \mathbb{F}$ and $m < \mathsf{zero}$ are untenable. That completes the proof of the lemma.

Lemma 5.35. *Every nonempty finite subset of $\mathbb{F}$ has a maximal element.*

Remark. By Lemma 3.4, it does not matter whether use "nonempty" or "inhabited" to state this lemma.

Proof. The formula to be proved is

$$\forall x \in \mathsf{FINITE}\,(x \subseteq \mathbb{F} \to x \neq \Lambda \to \exists m \in x\,\forall t\,(t \in x \to t \le m))$$

The formula is stratified, giving m and t index 0 and x index 1. $\mathbb{F}$ and FINITE are parameters, and do not require an index. Therefore we may proceed by induction on finite sets.

Base case: immediate, since $\Lambda \neq \Lambda$.

Induction step. Let x be a finite subset of $\mathbb{F}$ and $c \in \mathbb{F} - x$. By Lemma 3.4, x is empty or inhabited. If $x = \Lambda$, then c is the maximal element of $x \cup \{c\}$, and we are done. So we may assume x is inhabited. Then by the induction hypothesis, x has a maximal element m. By Theorem 5.18, $c \le m$ or $m < c$. If $c \le m$, then m is the maximal element of $x \cup \{c\}$. If $m < c$, then c is the maximal element of $x \cup \{c\}$, by the transitivity of $\le$. That completes the proof of the lemma.

Lemma 5.36. *For $x \in \mathbb{F}$ and $x^+ \in \mathbb{F}$, we have $x \neq x^+$.*

Proof. Suppose $x = x^+$; then

$$
\begin{array}{rl}
z \in x^+ & \text{for some } z\text{, by Lemma 4.7} \\
z = u \cup \{c\} & \text{for some } u \in c \text{ and } c \notin u\text{, by definition of successor} \\
u \cup \{c\} \in x^+ & \text{by the previous two lines} \\
u \cup \{c\} \in x & \text{since } x = x^+ \\
u \cup \{c\} \in \mathsf{FINITE} & \text{by Lemma 4.4} \\
u \sim u \cup \{c\} & \text{by Lemma 4.9} \\
u \cup \{c\} \neq u & \text{since } c \notin u
\end{array}
$$

Now $u \cup \{c\}$ is a finite set, similar to a proper subset of itself (namely u). Then by definition, $u \cup \{c\}$ is infinite. By Theorem 3.24, it is not finite. But it is finite. That contradiction completes the proof of the lemma.

Lemma 5.37. *For $x \in \mathbb{F}$ and $x^+ \in \mathbb{F}$, we have $x < x^+$.*

Proof. Let $u \in x$ and $u \cup \{c\} \in x^+$, with $c \notin x$. Then by definition of $\leq$ we have $x \leq x^+$. By Lemma 5.36, we have $x \neq x^+$. Then by definition of $<$, we have $x < x^+$. That completes the proof of the lemma.

6. USC, SSC, and similarity

We will replace Rosser and Specker's use of the full power set SC by the separable power set SSC. In this section we prove some lemmas from Specker §2, and some other similar lemmas. For finite sets a, since finite sets have decidable equality, every unit subclass is separable, which is helpful. We begin with Specker's Lemma 2.6, which we take in two steps with the next two lemmas, and after that Specker 2.4 and 2.3.

Lemma 6.1. *Let $y \in SSC(USC(a))$. Then there exists $z \in SSC(a)$ such that $y = USC(z)$.*

Proof. Suppose $y \in SSC(USC(a)$. Define

$$z := \{u : \{u\} \in y\}. \tag{45}$$

That definition is legal since the formula is stratified giving u index 0 and y index 2. Then $y = USC(z)$ since the members of y are the singletons of the members of z. I say that $z \subseteq a$: Suppose $u \in z$. Then

$$
\begin{array}{rl}
\{u\} \in y & \text{by (45)} \\
\{u\} \in USC(a) & \text{since } y \subseteq USC(a) \\
u \in a & \text{by definition of } USC(a)
\end{array}
$$

Therefore $z \subseteq a$, as claimed. It remains to show that z is a separable subset of a; it suffices to show that for $u \in a$, we have $u \in z \ \vee \ u \notin z$. Suppose $u \in a$. Then by (45),

$$
\begin{array}{rl}
& u \in z \ \vee u \notin z \\
\leftrightarrow & \{u\} \in y \ \vee \{u\} \notin y
\end{array}
$$

and that is true since y is a separable subset of $USC(a)$. That completes the proof of the lemma.

Lemma 6.2 (Specker 2.6)**.** $Nc(SSC(USC(a))) = Nc(USC(SSC(a)))$.

Remarks. We follow the proof from [8], p. 368, that Specker cites, checking it constructively with SSC in place of SC. But fundamentally, this lemma is just about shuffling brackets. We have $\{\{p\},\{q\},\{r\}\} \in SSC(USC(a))$ corresponding to $\{\{p,q,r\}\} \in USC(SSC(a))$. It is a useful result but not a deep one.

Proof. Let

$$W := \{u : \exists z\,(u = \langle \{z\}, USC(z)\rangle)\}.$$

The definition is stratified giving z index 1, so $\{z\}$ and $USC(z)$ both get index 2, and u gets index 4. It follows that W is a relation (contains only ordered pairs) and

$$\langle x,y\rangle \in W \leftrightarrow \exists z\,(x = \{z\} \ \wedge \ y = USC(z)). \tag{46}$$

I say that W is (the graph of) a one-one-function mapping $USC(SSC(a))$ onto $SSC(USC(a))$. (Formally there is no distinction between a function and its graph.) For if x is given, then z is uniquely determined, so y is uniquely determined; and if y is given with $y = USC(z)$, then $z = \bigcup y$ is unique, so $x = \{z\}$ is unique. Hence W is a function and one-to-one. It remains to show that W is onto. Let $y \in SSC(USC(a))$. By Lemma 6.1, there exists $z \in SSC(a)$ such that $y = USC(z)$. Then $\langle \{z\}, y\rangle \in W$. Hence y is in the range of W. Since y was an arbitrary member of $SSC(USC(a))$, it follows that W is onto.

We have shown that W is a similarity from $SSC(USC(a))$ to $USC(SSC(a))$. Therefore those two sets have the same cardinal. That completes the proof of the lemma.

Lemma 6.3. *Any two unit classes are similar.*

Proof. Let $\{a\}$ and $\{b\}$ be unit classes. Define $f = \{\langle a,b\rangle\}$. One can verify that $f : \{a\} \to \{b\}$ is a similarity. We omit the 75 inferences required to do so.

Lemma 6.4. *Any set similar to a unit class is a unit class.*

Proof. Let $x \sim \{a\}$. Then let $f : x \to \{a\}$ be a similarity. Since f is onto, there exists $c \in x$ with $f(c) = a$. Let $e \in x$. Then $f(e) \in \{a\}$, so $f(e) = a$. Since f is one to one, $e = c$. Then $x = \{c\}$. That completes the proof of the lemma.

Lemma 6.5. *We have*

$$u \in \mathsf{one} \leftrightarrow \exists a\,(u = \{a\}).$$

Proof. By definition, $\mathsf{one} = \mathsf{zero}^+$ and $\mathsf{zero} = \{\Lambda\}$. For any a, we have $a \notin \Lambda$, so

$$\Lambda \cup \{a\} = \{a\} \in \mathsf{zero}^+ = \mathsf{one}.$$

Conversely, if $u \in \mathsf{one}$, then $u = \Lambda \cup \{a\}$ for some a, by definition of successor, so $u = \{a\}$. That completes the proof of the lemma.

Lemma 6.6. *Suppose a and b are finite sets. Then*

$$a \in SSC(b) \to USC(a) \in SSC(SSC(b)).$$

Proof. Suppose $a \in SSC(b)$. Since b is finite, it has decidable equality, by Lemma 3.3. Therefore $USC(b) \subseteq SSC(b)$. Since $USC(a) \subseteq USC(b)$, we have

$$USC(a) \subseteq SSC(b) \tag{47}$$

It remains to show that $USC(a)$ is a separable subset of $SSC(b)$; that is,

$$SSC(b) = USC(a) \cup (SSC(b) - USC(a)).$$

By extensionality and the definitions of subset and union, it suffices to show

$$t \in SSC(b) \quad \leftrightarrow \quad t \in USC(a) \ \vee \ (t \in SSC(b) \ \wedge \ t \notin USC(a)) \tag{48}$$

Right to left: It suffices to show $t \in USC(a) \to t \in SSC(b)$. Let $t \in USC(a)$. Then $t = \{c\}$ for some $c \in a$. Since b has decidable equality, t is a separable subset of b. That completes the right-to-left direction.

Left to right: suppose $t \in SSC(b)$. Then $t \in \mathsf{FINITE}$, by Lemma 3.19. Then $Nc(t) \in \mathbb{F}$, by Lemma 4.21. Then by Lemma 5.19,

$$Nc(t) = \mathsf{one} \ \vee \ Nc(t) \neq \mathsf{one}.$$

Case 1, $Nc(t) = \mathsf{one}$. By Lemma 6.5, t is a unit class. Since $a \in SSC(b)$, we have

$$x \in b \to x \in a \ \vee \ x \notin a.$$

Since $t \in USC(a)$ if and only if for some x we have $t = \{x\} \ \wedge \ x \in a$, we have

$$t \in SSC(b) \to t \in USC(a) \ \vee \ t \notin USC(a).$$

That completes Case 1.

Case 2,$Nc(t) \neq \mathsf{one}$. Then $Nc(t)$ is not a unit class, by Lemma 6.5 and Lemma 5.7, so the second disjunct on the right holds. That completes the proof of the lemma.

Lemma 6.7 (Specker 2.4)**.** *For any sets a and b*

$$a \sim b \leftrightarrow USC(a) \sim USC(b).$$

Proof. Left-to-right. Suppose $f : a \to b$ is a similarity. Let g be the singleton image of f, namely

$$g := \{\langle \{u\}, \{v\} \rangle : \langle u, v \rangle \in f.$$

The definition is legal since the formula is stratified, giving u and v the same index. Then $g : USC(a) \to USC(b)$ is a similarity. We omit the straightforward proof.

Right-to-left. Let $g : USC(a) \to USC(b)$ be a similarity. Define

$$f := \{\langle u, v \rangle : \langle \{u\}, \{v\} \rangle \in g\}.$$

Again the definition is legal since the formula is stratified, giving u and v the same index. Then $f : a \to b$ is a similarity. We omit the proof.

Lemma 6.8 (Specker 2.3)**.** *For any sets a and b*

$$a \sim b \to SSC(a) \sim SSC(b).$$

Proof. Let $f : a \to b$ be a similarity. Define

$$g := \{\langle u, f``u \rangle : u \in SSC(a)\}$$

where $f``u$ is the image of u under f, i.e., the range of the restriction of f to u. Then $g : SSC(a) \to SSC(b)$. The fact that the values of g are separable subsets of b follows from Lemma 5.4. We omit the proof that g is one-to-one. To prove g is onto, let $y \in SSC(b)$. Then define

$$x = \{u \in a : \exists v \, (v \in y \ \wedge \ \langle u, v \rangle \in f)\}.$$

The formula is stratified, giving u and v index 0 and x and y index 1. Hence x can be defined. We omit the proof that $g(x) = y$. (x can also be defined using the operations of domain and inverse relation, which in turn can be defined by stratified comprehension.) That completes the proof (sketch) of the lemma.

Lemma 6.9. *If a has decidable equality, then $USC(a) \subseteq SSC(a)$.*

Proof. Let $x \in USC(a)$. Then $x = \{u\}$ for some $u \in a$. Then $x \subseteq a$. We must show $a = x \cup (a - x)$. By extensionality, that follows from

$$\forall u\, (u \in a \leftrightarrow u \in x \;\vee\; u \in a - x),$$

which in turn follows from decidable equality on a. That completes the proof of the lemma.

Lemma 6.10. *For all a, b,*

$$a \subseteq b \leftrightarrow USC(a) \subseteq USC(b),$$

Proof. Left to right. Suppose $a \subseteq b$ and $t \in USC(a)$. We must show $t \in USC(b)$. Then $t = \{x\}$ for some $x \in a$. Since $a \subseteq b$ we have $x \in b$. Then $t \in UCS(b)$. That completes the left-to-right direction.

Right to left. Suppose $USC(a) \subseteq USC(b)$ and $t \in a$. We must prove $t \in b$. Since $t \in a$ we have $\{t\} \in USC(a)$. Then $\{t\} \in USC(b)$. Then $\{t\} = \{q\}$ for some $q \in b$. Then $t = q$. Then $t \in b$ as desired. That completes the proof of the lemma.

Lemma 6.11. *For all a, b,*

$$a \in SSC(b) \leftrightarrow UCS(a) \in SSC(USC(b)).$$

Proof. Left to right. Suppose $a \in SSC(b)$. Then $a \subset b$ and

$$b \;=\; a \cup (b - a). \tag{49}$$

By Lemma 6.10,

$$USC(a) \subseteq USC(b) \tag{50}$$

It remains to show that $UCS(a)$ is a stable subset of $USC(b)$; that is,

$$USC(b) \;=\; USC(a) \cup (USC(b) - USC(a)). \tag{51}$$

By extensionality and the definitions of union and set difference, that is equivalent to

$$t \in USC(b) \quad\leftrightarrow\quad t \in USC(a) \;\vee\; (t \in USC(b) \;\wedge\; t \notin USC(a)). \tag{52}$$

Then we need only consider unit classes $t = \{x\}$, and using the fact that $\{x\} \in USC(b) \leftrightarrow t \in b$, and $\{x\} \in USC(a) \leftrightarrow t \in a$, (52) follows from 50. That completes the proof of the lemma.

Lemma 6.12. *For all a, b, we have*

$$a \in SSC(b) \leftrightarrow SSC(a) \subseteq SSC(b).$$

Proof. Left to right: Suppose $a \in SSC(b)$. Then $a \subseteq b$ and

$$b \;=\; a \cup (b - a) \tag{53}$$

Now let $x \in SSC(a)$. We must show $x \in SSC(b)$. Since $x \in SSC(a)$, we have $x \subseteq a$. Since $a \subseteq b$ we have $x \subseteq b$. We have

$$\begin{array}{rl}
x \in SSC(a) & \\
a = x \cup (a - x) & \text{by definition of } SSC(a) \\
b = (x \cup (a - x)) \cup (b - (x \cup (a - x))) & \text{by (53)} \\
b = x \cup (b - x) & \\
x \in SSC(b) & \text{by definition of } SSC(b)
\end{array}$$

That completes the left-to-right direction.

Right to left: Suppose $SSC(a) \subseteq SSC(b)$. We have to show $a \in SSC(b)$; but that follows from $a \in SSC(a)$ and the definition of subset. That completes the right to left direction. That completes the proof of the lemma.

Lemma 6.13. *Let b be a finite set. Then the subset relation on $SSC(b)$ is decidable. That is,*

$$\forall x, y \in SSC(b)\,(x \subseteq y \ \vee\ x \not\subseteq y).$$

Proof. Assume $b \in \mathsf{FINITE}$. By Lemma 3.17, $SSC(b) \in \mathsf{FINITE}$. Then by Lemma 3.3,

$$SSC(b) \in \mathsf{DECIDABLE} \tag{54}$$

We will prove by induction on finite sets y that

$$y \in SSC(b) \to \forall x \in SSC(b)\,(x \subseteq y \ \vee\ x \not\subseteq y). \tag{55}$$

It is legal to proceed by induction, since the formula is stratified.

Base case. When $y = \Lambda$, we will prove

$$\forall x \in SSC(b)\,(x \subseteq \Lambda \vee x \not\subseteq \Lambda).$$

Assume $x \in SSC(b)$. We have $x \subseteq \Lambda$ if and only if $x = \Lambda$, so it suffices to prove $x = \Lambda \ \vee\ x \neq \Lambda$. But that follows from (54). That completes the base case.

Induction step. Let $y = z \cup \{c\}$, with $c \notin z$ and $z \in SSC(b)$ and $y \subseteq b$. Then $c \in b$ The induction hypothesis is

$$z \in SSC(b) \to \forall x \in SSC(b)\,(x \subseteq z \ \vee\ x \not\subseteq z). \tag{56}$$

We have to prove

$$y \in SSC(b) \to \forall x \in SSC(b)\,(x \subseteq y \ \vee\ x \not\subseteq y) \tag{57}$$

Assume $y \in SSC(b)$ and $x \in SSC(b)$. We have to prove $x \subseteq y \ \vee\ x \not\subseteq y$. That is,

$$x \subseteq z \cup \{c\} \ \vee x \not\subseteq z \cup \{c\}$$

We have

$$\begin{array}{rl} y \in SSC(b) & \text{assumed above} \\ z \cup \{c\} \in SSC(b) & \text{since } y = z \cup \{c\} \end{array}$$

I say that $z \in SSC(b)$. To prove that, let $u \in z$. Since $z \cup \{c\} \in SSC(b)$, $u \in z \cup \{c\} \ \vee\ u \notin z \cup \{c\}$. Since $c \notin z$, $u \neq c$. Therefore $u \in z \vee u \notin z$. Then $z \in SSC(b)$ as claimed.

I say that also $x - \{c\} \in SSC(b)$. Since b is finite, it has decidable equality by Lemma 3.3. Then for $y \in b$, we have $y = c \ \vee\ y \neq c$. Since $x \in SSC(b)$ we have $y \in x \ \vee\ y \notin x$. Then a short argument by cases shows $y \in x - \{c\} \ \vee\ y \notin x\{c\}$. Then $x - \{c\} \in SSC(b)$, as claimed.

By (56) and $z \in SSC(b)$, we have

$$\forall x \in SSC(b)\,(x \subseteq z \ \vee\ x \not\subseteq z). \tag{58}$$

Since $x \in SSC(b)$, we have $c \in x \ \vee\ c \notin x$. We argue by cases accordingly.

Case 1: $c \in x$. Then $x \subseteq z \cup \{c\}$ if and only if $x - \{c\} \subseteq z$. By (58), instantiated to $x - \{c\}$ in place of x (which is allowed since $x - \{c\} \in SSC(b)$), we have

$$x - \{c\} \subseteq z \ \vee \ x - \{c\} \not\subseteq z.$$

That completes Case 1.

Case 2: $c \notin x$. Then $x \subseteq z \cup \{c\} \leftrightarrow x \subseteq z$, so (57) follows from the induction hypothesis (56). That completes Case 1. That completes the induction step. That completes the proof of the lemma.

Lemma 6.14. *Suppose a and b are finite sets. Then*

$$a \in SSC(b) \to SSC(a) \in SSC(SSC(b)).$$

Proof. Suppose $a \in SSC(b)$. By Lemma 6.12,

$$SSC(a) \subseteq SSC(b) \tag{59}$$

It remains to show that $SSC(a)$ is a separable subset of $SSC(b)$; that is,

$$SSC(b) = SSC(a) \cup (SSC(b) - SSC(a)).$$

By extensionality and the definitions of subset and union, it suffices to show

$$t \in SSC(b) \quad \leftrightarrow \quad t \in SSC(a) \ \vee \ (t \in SSC(b) \ \wedge \ t \notin SSC(a)) \tag{60}$$

The right-to-left direction follows logically from (59) and the definition of subset.

Ad the left-to-right direction of (60): suppose $t \in SSC(b)$. Then $t \subseteq b$. By Lemma 6.13,

$$t \subseteq a \vee t \not\subseteq a. \tag{61}$$

It remains to prove the left-to-right direction of (60). Suppose $t \in SSC(b)$. We argue by cases using (61).

Case 1: $t \subseteq a$. It suffices to prove $t \in SSC(a)$. It remains to prove $a = t \cup (a - t)$. We have

$$\forall u \in b\,(u \in t \ \vee \ u \notin t) \qquad \text{since } t \in SSC(b)$$
$$\forall u \in a\,(u \in t \ \vee \ u \notin t) \qquad \text{since } a \subseteq b$$

Then $a = t \cup (a - t)$ by the definitions of union and set difference. That completes Case 1.

Case 2: $t \not\subseteq a$. Then $t \notin SSC(a)$. Since $t \in SSC(b)$, the second disjunct on the right of (60) holds. That completes Case 2. That completes the proof of the lemma.

Lemma 6.15. *For all a and $c \notin a$, we have*

$$USC(a \cup \{c\}) = USC(a) \cup \{\{c\}\}.$$

Proof. By extensionality it suffices to verify the two sides have the same members.

Left to right: Let $x \in USC(a \cup \{c\})$. Then $x = \{u\}$ for some $u \in a \cup \{c\}$. Then $u \in a \ \vee \ a = c$. If $u \in a$ then $x \in USC(a)$ and hence $x \in USC(a) \cup \{\{c\}\}$. That completes the left-to-right direction.

Right to left: Let $x \in USC(a) \cup \{\{c\}\}$. Then $x \in USC(a) \ \vee \ x = \{c\}$. If $x \in USC(a)$, then $x \in USC(a \cup \{c\})$ by Lemma 6.10. If $x = \{c\}$, then $x \in USC(a \cup \{c\})$ by definition of USC. That completes the proof of the lemma.

Lemma 6.16. *For all a, b we have*

$$USC(a - b) = USC(a) - USC(b).$$

Proof. By the definitions of USC and set difference, using about 50 straightforward inferences, which we choose to omit.

Lemma 6.17. $USC(\Lambda) = \Lambda$.

Proof. Suppose $x \in USC(\Lambda)$. By definition of USC, there exists $a \in \Lambda$ such that $x = \{a\}$. But that contradicts the definition of Λ. That completes the proof of the lemma.

Lemma 6.18. *For every x and a,*

$$x \in a \leftrightarrow \{x\} \in USC(a).$$

Proof. Left to right, by definition of $USC(a)$. Right to left: if $\{x\} \in USC(a)$, then for some $y \in a$, $\{x\} = \{y\}$. Then by extensionality $x = y$. That completes the proof of the lemma.

Lemma 6.19. $SSC(\Lambda) = \{\Lambda\}$.

Proof. The only subset of Λ is Λ, and it is a stable subset.

Lemma 6.20. *Suppose $a \sim b$ and a is inhabited. Then b is inhabited.*

Proof. Let $f : a \to b$ be a similarity. Since a is inhabited, there exists some $c \in a$. Fix c. Then $f(c) \in b$. Hence b is inhabited. That completes the proof of the lemma.

Lemma 6.21 (Bounded DNS)**.** *Let P be any set, and let $y \in \mathbb{F}$. Then*

$$\neg\neg\, \forall x\, (x \in \mathbb{F} \to x < y \to x \in P) \leftrightarrow \forall x\, (x \in \mathbb{F} \to x < y \to \neg\neg\, x \in P).$$

Remarks. This lemma is closely related to Lemma 3.28, and can be derived from that lemma, but here we just prove it directly.

Proof. The left-to-right direction is logically valid. We prove the right-to-left implication by induction on y. The formula to be proved is stratified, giving x and y index 0, so induction is legal.

Base case: by Lemma 5.29, $x < 0$ can never hold. That completes the base case.

Induction step: The key fact will be Lemma 5.33:

$$x < y^+ \leftrightarrow x < y \;\vee\; x = y. \tag{62}$$

Assume y^+ is inhabited (as for any proof by induction). Then

$\forall x\, (x \in \mathbb{F} \to x < y^+ \to \neg\neg\, x \in P)$	assumption
$\forall x\, (x \in \mathbb{F} \to (x < y \;\vee\; x = y) \to \neg\neg\, P(x)$	by 62)
$\forall x\, (x \in \mathbb{F} \to (x < y \to \neg\neg\, x \in P \;\wedge\; x = y \to \neg\neg\, P(x))$	by logic
$\forall x\, (x \in \mathbb{F} \to (x < y \to \neg\neg\, x \in P) \;\wedge\; \neg\neg\, y \in P$	by logic
$\neg\neg\, \forall x\, (x \in \mathbb{F} \to (x < y \to x \in P) \;\wedge\; \neg\neg\, y \in P$	induction hyp.
$\neg\neg\, \forall x\, (x \in \mathbb{F} \to x \le y \to x \in P)$	by 62)

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

7. Cardinal exponentiation

Specker 4.1 follows Rosser in defining 2^m for cardinals m. They define 2^m to be the cardinal of $SC(a)$ where $USC(a) \in m$. That definition requires some modification to be of use constructively. It is *separable* subsets of a that correspond to functions from a to 2, so it makes sense to use $SSC(a)$, the class of separable subsets of a, instead of $SC(a)$.

Definition 7.1. *For finite cardinals m, we define*

$$2^m = \{u : \exists a\,(USC(a) \in m \ \wedge\ u \sim SSC(a)\}.$$

The following lemma shows that our definition is classically equivalent to Specker's definition.

Lemma 7.2. *Let $m \in \mathbb{F}$ and $USC(a) \in m$. Then $SSC(a) \in 2^m$, and $2^m = Nc(SSC(a))$.*

Remark. This is Specker's definition of 2^m, but our definition avoids a case distinction as to whether m does or does not contain a set of the form $USC(a)$.

Proof. Suppose $m \in \mathbb{F}$ and $USC(a) \in m$. I say that 2^m is a cardinal, i.e., it is closed under similarity. Suppose u and v are members of 2^m. Then there exist a and b such that $USC(a)$ and $USC(b)$ are both in m and $u \sim SSC(a)$ and $v \sim SSC(b)$. Then by Lemma 4.9, $USC(a) \sim USC(b)$. By Lemma 6.7, $a \sim b$. By Lemma 6.8, $SSC(a) \sim SSC(b)$. By Lemma 2.10, $u \sim v$. Hence, as claimed, 2^m is a cardinal.

Therefore 2^m and $Nc(SSC(a))$ are both closed under similarity. Since they both contain $SSC(a)$, they each consist of all sets similar to $SSC(a)$. Hence by extensionality, they are equal. That completes the proof of the lemma.

Remark. We note that $2^m \neq \Lambda$ does not *a priori* imply that 2^m is inhabited, so we must carefully distinguish these two statements as hypotheses of lemmas. 2^m is inhabited if m contains a set of the form $USC(a)$. $2^m \neq \Lambda$ means not-not m contains such a set.

Lemma 7.3. *The graph of the exponentiation function*

$$\{\langle m, 2^m\rangle : m \in \mathbb{F}\}$$

is definable in INF.

Proof. We have to show that the relation is definable by a formula that can be stratified, giving the two members of ordered pairs the same index. The formula in Definition 7.1 is

$$2^m = \{u : \exists a\,(USC(a) \in m \ \wedge\ u \sim SSC(a)\}.$$

Stratify it, giving a index 0, $USC(a)$ and $SSC(a)$ and u index 1, m index 2. Then 2^m gets one index higher than u, namely 2, which is the same index that m gets. That completes the proof.

Lemma 7.4. *If $m \in \mathbb{F}$ and 2^m is inhabited, then there exists a such that $USC(a) \in m$ and $SSC(a) \in 2^m$.*

Proof. Suppose 2^m is inhabited. Then by Definition 7.1, there exists a with $USC(a) \in m$, and 2^m contains any set similar to $SSC(a)$. Since $SSC(a) \sim SSC(a)$, by Lemma 2.10, we have $SSC(a) \in 2^m$. That completes the proof of the lemma.

Lemma 7.5. *Let m be a finite cardinal. If 2^m is inhabited, then 2^m is a finite cardinal.*

Proof. Suppose m is a finite cardinal and 2^m is inhabited. By Definition 7.1, there exists a such that $USC(a) \in m$ and $SSC(a) \in 2^m$. Then $Nc(SSC(a)) = 2^m$, by Definition 7.1. We have

$$\begin{aligned} USC(a) &\in \mathsf{FINITE} && \text{by Lemma 4.4} \\ a &\in \mathsf{FINITE} && \text{by Lemma 3.10} \\ SSC(a) &\in \mathsf{FINITE} && \text{by Lemma 3.17} \\ Nc(SSC(a)) &\in \mathbb{F} && \text{by Lemma 4.21} \\ 2^m &\in \mathbb{F} && \text{since } Nc(SSC(a)) = 2^m \end{aligned}$$

That completes the proof of the lemma.

Lemma 7.6. $2^{\mathsf{zero}} = \mathsf{one}$.

Proof. $\mathsf{zero} = \{\Lambda\}$. It therefore contains $\Lambda = USC(\Lambda)$. Hence 2^{zero} is inhabited and contains $SSC(\Lambda)$. But Λ has only one subset, namely Λ, which is a separable subset, so $SSC(\Lambda) = \{\Lambda\} = \mathsf{zero}$. Thus $2^{\mathsf{zero}} = Nc(\mathsf{zero}) = \mathsf{one}$. That completes the proof of the lemma.

Lemma 7.7. $2^{\mathsf{one}} = \mathsf{two}$.

Proof. one is the set of all singletons. It therefore contains $\{\mathsf{zero}\} = USC(\mathsf{zero})$. Then 2^{one} contains $SSC(\mathsf{zero})$. There are exactly two subsets of $\{\Lambda\}$, namely Λ and $\{\Lambda\}$, and both are separable. Hence 2^{one} contains the two-element set $SSC(\mathsf{zero}) = \{\Lambda, \{\Lambda\}\}$. That set belongs to $\mathsf{two} = \mathsf{one}^+$ since it is equal to $\{\{\Lambda\}\} \cup \{\Lambda\}$, and the singleton $\{\{\Lambda\}\}$ belongs to one and $\{\Lambda\} \notin \{\{\Lambda\}\}$. Therefore 2^{one} and one^+ have a common element. Both are cardinals, by Lemma 7.5. Then by Lemma 5.7, $2^{\mathsf{one}} = \mathsf{two}$. That completes the proof of the lemma.

Lemma 7.8. $2^{\mathsf{two}} = \mathsf{four}$.

Proof. By definition, $\mathsf{four} = \mathsf{three}^+ = \mathsf{two}^{++}$. One can show (but we omit the details) that

$$USC(\{\mathsf{one}, \mathsf{two}\}) = \{\{\mathsf{one}\}, \{\mathsf{two}\}\} \in \mathsf{two}$$

Therefore, by the definition of exponentiation,

$$SSC(\{\mathsf{one}, \mathsf{two}\}) = \{\Lambda, \{\mathsf{one}\}, \{\mathsf{two}\}, \{\mathsf{one}, \mathsf{two}\}\} \in 2^{\mathsf{two}}$$

One can explicitly exhibit the ordered pairs of a similarity between the last-mentioned set and $\{\mathsf{one}, \mathsf{two}, \mathsf{three}, \mathsf{four}\} \in \mathsf{four}$. We omit the details. Then by Lemma 4.8, $2^{\mathsf{two}} = \mathsf{four}$. That completes the proof of the lemma.

Lemma 7.9. *We have*

$$u \in \mathsf{two} \leftrightarrow \exists a, b\, (a \neq b \ \wedge \ u = \{a, b\}).$$

Proof. We have $\mathsf{two} = \mathsf{one}^+$. If $a \neq b$ then by Lemma 6.5, $\{a\} \in \mathsf{one}$, and $\{a\} \cup \{b\} = \{a, b\} \in \mathsf{two}$. Conversely, If $u \in \mathsf{two}$ then $u = v \cup \{b\}$, where $v \in \mathsf{one}$ and $b \notin v$. By Lemma 6.5, $v = \{a\}$ for some a, so $u = \{a, b\}$. That completes the proof of the lemma.

Lemma 7.10. *We have*

$$u \in \mathsf{three} \leftrightarrow \exists a, b, c\,(a \neq b\ \wedge b \neq c\ \wedge a \neq c\ \wedge\ u = \{a, b, c\}).$$

Proof. We have $\mathsf{three} = \mathsf{two}^+$. Assume a, b, c are pairwise distinct. Then by Lemma 7.9, $\{a, b\} \in \mathsf{two}$. Since $\mathsf{three} = two^+$, $\{a, b\} \cup \{c\} = \{a, b, c\} \in \mathsf{three}$. Conversely, If $u \in \mathsf{three}$ then $u = v \cup \{c\}$, where $v \in \mathsf{two}$ and $c \notin v$. By Lemma 7.9, $v = \{a, b\}$ for some a, b with $a \neq b$. Since $c \notin v$, $a \neq c$ and $b \neq c$. Therefore $u = \{a, b, c\}$ with a, b, c pairwise distinct. That completes the proof of the lemma.

Lemma 7.11. *We have* $\mathsf{zero} < \mathsf{one} < \mathsf{two} < \mathsf{three} < four$.

Proof. Since each of these numbers is defined as the successor of the one listed just before it, the lemma is a consequence of Lemma 5.37.

Lemma 7.12. *For* $m \in \mathbb{F}$, *we have* $m < \mathsf{one} \leftrightarrow m = \mathsf{zero}$.

Proof. Let $m \in \mathbb{F}$ and $m < \mathsf{one}$. By Theorem 5.18, $m < \mathsf{zero} \vee\ = \mathsf{zero}\ \vee\ \mathsf{zero} < m$. By Lemma 5.29, $m < \mathsf{zero}$ is ruled out. It remains to rule out $\mathsf{zero} < m$. Assume $\mathsf{zero} < m$. Then

$m < \mathsf{one}$	by hypothesis
$m^+ \leq \mathsf{one}$	by Lemma 5.30
$m^+ \leq \mathsf{zero}^+$	since $\mathsf{zero}^+ = \mathsf{one}$
$m \leq \mathsf{zero}$	by Lemma 5.11
$\mathsf{zero} < \mathsf{zero}$	by Lemma 5.23, since $\mathsf{zero} \leq m < \mathsf{zero}$
$\mathsf{zero} \not< \mathsf{zero}$	by Lemma 5.29

That completes the proof of the lemma.

Lemma 7.13. *For* $m \in \mathbb{F}$, *we have*

$$m < \mathsf{two} \leftrightarrow m = \mathsf{zero}\ \vee\ m = \mathsf{one}.$$

Proof. Left to right. Assume $m \leq \mathsf{two}$. We have

$\mathsf{zero} \neq \mathsf{one}$	by Lemma 5.36
$\{\mathsf{zero}, \mathsf{one}\} \in \mathsf{two}$	by Lemma 7.9
$m \leq \mathsf{two}$	by Definition 5.2
$a \in m \wedge a \in SSC(\{\mathsf{zero}, \mathsf{one}\})$	for some a, by Lemma 5.9
$a \neq \{\mathsf{zero}, \mathsf{one}\}$	since $m \neq \mathsf{two}$
$\mathsf{zero} \in a \vee \mathsf{zero} \notin a$	since $a \in SSC(\{\mathsf{zero}, \mathsf{one}\})$
$\mathsf{one} \in a \vee \mathsf{one} \notin a$	since $a \in SSC(\{\mathsf{zero}, \mathsf{one}\})$

An argument by cases (about 170 steps, which we omit) shows that $a = \Lambda$, or $a = \{\mathsf{zero}\}$, or $a = \{\mathsf{one}\}$. Then $a = \mathsf{zero}$ or one, by Lemma 5.7. That completes the left to right direction.

Right to left: we have $\mathsf{zero} < \mathsf{two}$ and $\mathsf{one} < \mathsf{two}$ by Lemma 7.11. That completes the proof of the lemma.

Lemma 7.14. *For all* a, a *is a unit class if and only if* $USC(a)$ *is a unit class.*

Proof. Left to right. Suppose $a = \{x\}$. Then the only unit subset of a is $\{a\}$, so $USC(a)$ is a unit class.

Right to left. Suppose $USC(a) = \{u\}$. Then $u \in a$. Let $t \in a$. Then $\{t\} \in USC(a)$, so $\{t\} = u$. Hence every element of a is equal to u. Hence $a = \{u\}$. That completes the proof of the lemma.

Lemma 7.15. *For all* $x \in \mathbb{F}$, $x \le \mathsf{zero} \to x = \mathsf{zero}$.

Proof. Suppose $x \in \mathbb{F}$ and $x \le \mathsf{zero}$. By the definition of $\le$, there exists a, b such that $a \in x$, $b \in \mathsf{zero}$, $a \subseteq b$, and $b = (a \cup b) - a$. Then

$$\begin{array}{rl} b = \Lambda & \text{by definition of zero} \\ a = \Lambda & \text{since } a \subseteq b \\ \Lambda \in x \cap \mathsf{zero} & \text{by definition of } \cap \\ x = \mathsf{zero} & \text{by Lemma 5.7} \end{array}$$

That completes the proof of the lemma.

Lemma 7.16 (Specker 4.6*). *If m is a finite cardinal and 2^m is inhabited, then $m < 2^m$.*

Proof. Since $\mathbb{F}$ has decidable equality, by Corollary 5.19

$$m = \mathsf{zero} \ \vee \ m = \mathsf{one} \vee (m \ne \mathsf{zero} \ \wedge \ m \ne \mathsf{one}.)$$

We argue by cases.

Case 1, $m = \mathsf{zero}$. Then by Lemma 7.6, $2^m = \mathsf{one}$, and we have to show $\mathsf{zero} < \mathsf{one}$, which follows from the definition of $<$ by exhibiting the separable subset Λ of the set $\{\Lambda\}$, and noting that $\Lambda \in \mathsf{zero}$ while $\{\Lambda\} \in \mathsf{one}$.

Case 2, $m = \mathsf{one}$. Then by Lemma 7.7, $2^m = \mathsf{two}$, and we have to show $\mathsf{one} < \mathsf{two}$, which follows from $\mathsf{zero} < \mathsf{one}$ by Corollary 4.7 and Lemma 5.11, or more directly, from the definition of $<$ by exhibiting the separable subset $\{\Lambda\}$ of $\{\{\Lambda\}, \Lambda\}$, the former of which belongs to one while the latter belongs to two.

Case 3, $m \ne \mathsf{zero}$ and $m \ne \mathsf{one}$. By hypothesis, 2^m is inhabited. Then there exists a such that $USC(a) \in m$. Since $m \in \mathbb{F}$, we have

$$\begin{array}{rl} USC(a) \in \mathsf{FINITE} & \text{by Lemma 4.4} \\ a \in \mathsf{FINITE} & \text{by Lemma 3.10} \\ SSC(a) \in \mathsf{FINITE} & \text{by Lemma 3.17} \\ a \in \mathsf{DECIDABLE} & \text{by Lemma 3.3} \end{array}$$

Then by Lemma 3.18, $USC(a)$ is a separable subset of $SSC(a)$. Now with $u = USC(a)$ and $v = SSC(a)$ we have proved that u is a separable subset of v and $u \in m$ and $v \in 2^m$. Then by Definition 5.2 we have $m \le 2^m$.

By definition $m < 2^m$ means $m \le 2^m$ and $m \ne 2^m$. It remains to prove that $m \ne 2^m$. Suppose $m = 2^m$. As just proved, we have $USC(a) \subseteq SSC(a)$. I say that it is a proper subset, $USC(a) \subset SSC(a)$. It suffices to prove $USC(a) \ne SSC(a)$. We have to produce an element of $SSC(a)$ that does not belong to $USC(a)$. We propose a as this element. We have $a \in SSC(a)$ since a is a separable subset of itself. It remains to show that $a \notin USC(a)$. Assume $a \in USC(a)$. Then a is a unit class. By Lemma 7.14, $USC(a)$ is also a unit class. Any two unit classes are similar, so $USC(a) \sim \mathsf{zero}$. Since $\mathsf{zero} \in \mathsf{one}$, $USC(a) \in \mathsf{one}$, by Lemma 4.8. Then

$m \cap \mathsf{one}$ is inhabited, since it contains $USC(a)$. Then by Lemma 5.7, $m = \mathsf{one}$, contradiction. That completes the proof that $USC(a)$ is a proper subset of $SSC(a)$.

We have

$USC(a) \subset SSC(a)$	as proved above
$USC(a) \sim SSC(a)$	by Lemma 4.9, since $USC(a) \in m$ and $SSC(a) \in 2^m$
$SSC(a)$ is infinite	since $SSC(a) \sim USC(a) \subset SSC(a)$
$\neg\,(SSC(a) \in \mathsf{FINITE})$	by Theorem 3.24
$SSC(a) \in \mathsf{FINITE}$	by Lemma 3.17, since $a \in \mathsf{FINITE}$

That is a contradiction. That completes the proof of the lemma.

Lemma 7.17. *For all $m \in \mathbb{F}$,*

$$\exists u\,(u \in 2^m) \to m^+ \leq 2^m.$$

Proof. Suppose $m \in \mathbb{F}$ and $\exists u\,(u \in 2^m)$. Then

$m < 2^m$	by Lemma 7.16
$2^m \in \mathbb{F}$	by Lemma 7.5
$m^+ \leq 2^m$	by Lemma 5.30

That completes the proof of the lemma.

Lemma 7.18 (Specker 4.8)**.** *Let $m, n \in \mathbb{F}$. If $m \leq n$ and 2^n is inhabited, then 2^m is inhabited and $2^m \leq 2^n$.*

Proof. Suppose $m \leq n$ and 2^n is inhabited. Then

$\exists u\,(u \in n)$	by Corollary 4.7
$\exists b\,(USC(b) \in n)$	by Lemma 7.4
$\exists b\,(USC(b) \in m)$	by Lemma 7.4

Since $m \leq n$, by Lemma 5.9 there is a separable subset x of $USC(b)$ such that $x \in m$. Let $a = \bigcup x$. Then using the definitions of $\bigcup$ and USC, we have $x = USC(a)$. Therefore 2^m is inhabited. Now $2^m = NC(SSC(a))$ and $2^n = NC(SSC(b))$.

I say that b is finite. We have

$USC(b) \in n$	
$USC(b) \in \mathsf{FINITE}$	by Lemma 4.4
$b \in \mathsf{FINITE}$	by Lemma 3.10

I say that a is also finite. We have

$x \in \mathsf{FINITE}$	by Lemma 4.4, since $x \in m$

Every member of x is a unit class, since $x = USC(a)$). Every unit class is finite. Therefore every member of x is finite. Moreover, since the members of x are unit classes, distinct members of x are disjoint. Since x is also finite, $a = \bigcup x$ is a finite union of disjoint finite sets. Hence a is finite, by Lemma 3.25.

Since $x = USC(a)$ is a separable subset of $USC(b)$, we have

$$\begin{array}{rl} USC(a) \in SSC(USC(b)) & \\ a \in SSC(b) & \text{by Lemma 6.11 (right to left)} \\ SSC(a) \in SSC(SSC(b)) & \text{by Lemma 6.14, since } a \text{ and } b \text{ are finite} \end{array}$$

Then $SSC(a)$ belongs to 2^m, and is a separable subset of $SSC(b)$, which belongs to 2^n. Therefore, by Definition 5.2, $2^m \le 2^n$. That completes the proof of the lemma.

8. Addition

Specker uses addition in §5 of his paper, and relies on Rosser for its associativity and commutativity. Those properties can be proved (as is very well-known) by induction from the two fundamental "defining equations":

$$\begin{aligned} x + y^+ &= (x+y)^+ \\ x + \mathsf{zero} &= x \end{aligned}$$

In the present context, where the main point of the paper is to prove that there are infinitely many finite cardinals, we need to bear in mind the possibility that successor or addition may "overflow". We have arranged that successor is always defined (for any argument whatever); and if there is a largest natural number then when we take its successor we get the empty set, which can be thought of as the computer scientist's "not a number." We need to define addition with similar behavior; if $x+y$ should "overflow", it should produce "not a number", but still be defined. Then the equations above should be valid without further qualification, i.e., without insisting that x and y should be members of $\mathbb{F}$. If we assume only that those equations are valid for $x, y \in \mathbb{F}$, then the inductive proofs of associativity and commutativity do not go through.

The proofs of associativity and commutativity proceed via another important property, "successor shift":

$$x^+ + y = x + y^+$$

Normally this property is proved by induction from the "defining equations." In the present context, that does not work, because if x and y are restricted to $\mathbb{F}$, then when we try to use successor shift to prove the associative law, we need $x + y \in \mathbb{F}$, which we do not want to assume, as the statement of the associative law should cover the case when $x+y$ overflows. Therefore, we prove below that successor shift is generally valid, i.e., without restricting x and y to $\mathbb{F}$. Once we have these *three* equations generally valid, then the usual proofs of associativity and commutativity by induction go through without difficulty. But in fact, it is simpler and more general to verify them directly from the definition of addition, and then we have associativity and commutativity of addition for all sets, not just finite cardinals.

Definition 8.1 (Specker 3.1, Rosser 373). *For any sets x and y we define*

$$x + y := \{z : \exists u, v\, (u \in x \ \wedge\ v \in y \ \wedge\ u \cap v = \Lambda \ \wedge\ z = u \cup v)\}$$

The formula in the definition is stratified, giving u, v, and z index 1 and x and y index 2. Then x, y, and z all get the same index, so addition is definable as a function in INF. (See Definition 2.2 for ordered triples.)

Lemma 8.2. *Addition satisfies the "defining equations" and successor shift:*

$$\begin{array}{rcl} x + \mathsf{zero} & = & x \\ x + y^+ & = & (x+y)^+ \\ x + y^+ & = & x^+ + y \end{array}$$

Remark. Addition is defined on any arguments, not just on $\mathbb{F}$.

Proof. Ad $x + \mathsf{zero} = x$. By extensionality, it suffices to show $z \in x + \mathsf{zero} \leftrightarrow z \in x$. Left to right: suppose $z \in x + \mathsf{zero}$. Then $z = u \cup v$, where u and v are disjoint and $u \in x$ and $v \in \mathsf{zero}$. Since $\mathsf{zero} = \{\Lambda\}$, we have $v = \lambda$, so $z = u \cup \Lambda = u \in x$. That completes the left-to-right implication.

Right-to-left: Let $z \in x$. Then $z \cup \Lambda \in x + \mathsf{zero}$, by the definition of addition. Since $z \cup \Lambda = z$, we have $z \in x + \mathsf{zero}$ as desired. That completes the proof of $x + \mathsf{zero} = x$.

Ad $x + y^+ = (x+y)^+$. By extensionality, it suffices to show the two sides have the same members. Left to right: We have

$$\begin{array}{rl} z \in x + y^+ & \text{assumption} \\ z = u \cup v & \text{where } u \in z \text{ and } v \in y^+ \text{ and } u \cap v = \Lambda \\ v = w \cup \{c\} & \text{where } w \in y \text{ and } c \notin w\text{, by definition of } y^+ \\ z = (u \cup w) \cup \{c\} & \text{by associativity of union} \\ u \cup w \in x + y & \text{by definition of addition} \\ c \notin u \cup w & \text{since } c \notin w \text{ and } u \cap v = \Lambda \\ z \in (x+y)^+ & \text{by definition of successor} \end{array}$$

That completes the left to right implication.

Right to left:

$$\begin{array}{rl} z \in (x+y)^+ & \text{assumption} \\ z = w \cup \{c\} & \text{where } c \notin w \text{ and } w \in x + y \\ w = u \cup v & \text{where } u \in x \text{ and } v \in y \text{ and } u \cap v = \Lambda \\ z = u \cup (v \cup \{c\}) & \text{by the associativity of union} \\ c \notin v & \text{since } c \notin w = u \cup v \\ v \cup \{c\} \in y^+ & \text{by definition of successor} \\ u \cap (v \cup \{c\}) = \Lambda & \text{since } u \cap v = \Lambda \text{ and } c \notin u \\ u \cup (v \cup \{c\}) \in x + y^+ & \text{by definition of addition} \\ (u \cup v) \cup \{c\} \in x + y^+ & \text{by the associativity of union} \\ z \in x + y^+ & \text{since } z = w \cup \{c\} = (u \cup v) \cup \{c\} \end{array}$$

That completes the proof of the right to left direction. That completes the proof of $x + y^+ = (x+y)^+$.

Ad successor shift. We must prove

$$z \in x + y^+ \leftrightarrow z \in x^+ + y.$$

Left to right:

$$\begin{array}{rl} z \in x + y^+ & \text{assumption} \\ z = u \cup (v \cup \{c\}) & \text{where } u \in x,\ v \in y, \text{ and } c \notin v, \text{ and } u \cap (v \cup \{c\}) = \Lambda \\ z = (u \cup \{c\}) \cup v & \text{by the associativity and commutativity of union} \\ c \notin u & \text{since } u \cap (v \cup \{c\}) = \Lambda \\ u \cup \{c\} \in x^+ & \text{by the definition of successor} \\ (u \cup \{c\}) \cap v = \Lambda & \text{by the associativity and commutativity of union} \\ z \in x^+ + y & \text{by the definition of addition} \end{array}$$

That completes the left to right direction.

Right to left:

$$\begin{array}{rl} z \in x^+ + y & \text{assumption} \\ z = (u \cup \{c\}) \cup v & \text{where } u \in x,\ v \in y,\ c \notin u, \text{ and } (u \cup \{c\}) \cap v = \Lambda \\ z = (u \cup v) \cup \{c\} & \text{by the associativity and commutativity of union} \\ c \notin u \cup v & \text{since } c \notin u \text{ and } (u \cup \{c\}) \cap v\ \Lambda \\ u \cup v \in x + y & \text{by the definition of addition} \\ z \in (x + y)^+ & \text{by the definition of successor} \end{array}$$

That completes the right to left direction. That completes the proof of the lemma.

Lemma 8.3. *Addition obeys the associative and commutative laws and left identity (without restriction to* $\mathbb{F}$*)*

$$\begin{array}{rcl} \mathsf{zero} + x & = & x \\ (x + y) + z & = & x + (y + z) \\ x + y & = & y + x \end{array}$$

Remark. We call attention to the fact that, even when x, y, z are assumed to be in $\mathbb{F}$, the expressions in the equations might "overflow", and the equations contain implicitly the assertion that the overflows "match", i.e., one side overflows if and only if the other does. Here "overflow" means to have the value Λ.

Proof. These laws are immediate consequences of the definition of addition, via the associative and commutative laws of set union. We omit the proofs.

Lemma 8.4. *For all* $m \in \mathbb{F}$*, we have* $m^+ = m + \mathsf{one}$*.*

Proof. We have

$$\begin{array}{rl} m + \mathsf{one} = m + \mathsf{zero}^+ & \text{by definition of } \mathsf{one} \\ m + \mathsf{one} = m^+ + \mathsf{zero} & \text{by Lemma 8.2} \\ m + \mathsf{one} = m^+ & \text{by Lemma 8.2} \end{array}$$

That completes the proof of the lemma.

Lemma 8.5. $\mathsf{one} + \mathsf{one} = \mathsf{two}$.

Proof.

$$\begin{array}{rl} \mathsf{two} = \mathsf{one}^+ & \text{by definition of } \mathsf{two} \\ \mathsf{two} = \mathsf{one} + \mathsf{one} & \text{by Lemma 8.4} \end{array}$$

Lemma 8.6. *Suppose $\kappa, \mu \in \mathbb{F}$, and $\kappa + \mu$ is inhabited. Then $\kappa + \mu \in \mathbb{F}$.*

Remark. This lemma addresses the problem of possible "overflow" of addition. If there are enough elements to find disjoint members of κ and μ then adding κ and μ will not overflow.

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

Base case: $\kappa + \mathsf{zero} = \kappa$ is in $\mathbb{F}$ because $\kappa \in \mathbb{F}$.

Induction step: Suppose $\kappa + \mu^+$ is inhabited and μ^+ is inhabited. Then $\kappa + \mu^+ = (\kappa + \mu)^+$ is inhabited. By the induction hypothesis, $\kappa + \mu \in \mathbb{F}$. Then by Lemma 4.19, $(\kappa + \mu)^+ \in \mathbb{F}$. Since $(\kappa + \mu)^+ = \kappa + \mu^+$, we have $\kappa + \mu^+ \in \mathbb{F}$. That completes the induction step. That completes the proof of the lemma.

Lemma 8.7. *Suppose $p, q, r \in \mathbb{F}$ and $p + q + r \in \mathbb{F}$. Then $p + q$ and $q + r$ are also in $\mathbb{F}$. Similarly, if $p, q, r, s \in \mathbb{F}$ and $p + q + r + s \in \mathbb{F}$, then $p + q + r \in \mathbb{F}$.*

Proof. By Corollary 4.7, $p + q + r$ is inhabited. Let $u \in p + q + r$. Then by the definition of addition, $u = a \cup b \cup c$ with $a \in p$, $b \in q$, $c \in r$, and a, b, c pairwise disjoint. Then $a \cup b \in p + q$ and $b \cup c \in q + r$. Then by Lemma 8.6, $p + q \in \mathbb{F}$ and $q + r \in \mathbb{F}$. That completes the proof of the three summand case. The case of four summands is treated similarly. We omit the details.

Lemma 8.8. *If $p \in \mathbb{F}$ and $p + q^+ \in \mathbb{F}$, then $p^+ \in \mathbb{F}$.*

Remark. It is not assumed that $q \in \mathbb{F}$.

Proof. Suppose $p \in \mathbb{F}$ and $p + q^+ \in \mathbb{F}$. By Corollary 4.7, there exists $u \in p + q^+$. Then by Definition 8.1, there exist a and b with $a \in p$ and $b \in q^+$ and $a \cap b = \Lambda$. By definition of successor, $b = x \cup \{c\}$ for some x and c, so $c \in b$. Since $a \cap b = \Lambda$, we have $c \notin a$. Then $a \cup \{c\} \in p^+$. Then $p^+ \in \mathbb{F}$. That completes the proof of the lemma.

Lemma 8.9. *If $p, q \in \mathbb{F}$ and $p + q^+ \in \mathbb{F}$, then $p + q \in \mathbb{F}$.*

Proof. We have

$$\begin{array}{rl} p + q^+ \in \mathbb{F} & \text{by hypothesis} \\ p + q + \mathsf{one} \in \mathbb{F} & \text{by definition of } \mathsf{one} \text{ and Lemma 8.2} \\ p + q \in \mathbb{F} & \text{by Lemma 8.7} \end{array}$$

That completes the proof of the lemma.

Lemma 8.10. *For $a, b, p, q \in \mathbb{F}$, if $b + q \in \mathbb{F}$ we have*

$$a \le b \ \wedge \ p \le q \to a + p \le b + q$$

Proof. Suppose $a, b, p, q \in \mathbb{F}$ and $b + q \in \mathbb{F}$. Suppose also $a \le b$, $p \le q$. Then

$$w \in b + q \qquad \text{for some } w\text{, by Lemma 4.7, since } b + q \in \mathbb{F}$$

By the definition of addition, there exist u, v with $w = u \cup v$, $u \in b$, $v \in q$, and $u \cap v = \Lambda$. By Lemma 5.9, since $a \le b$ there exists $r \in a$ with $r \in SSC(u)$. By Lemma 5.9, since $p \le q$, there exists $s \in p$ with $s \in SSC(v)$. Then one can verify that $r \cup s \in SSC(u \cup v)$. (We omit the details of that verification.) Since $u \cup v = w$ we have $r \cup s \in SSC(w)$. We have $r \cap s = \Lambda$, since $r \subseteq u$, $s \subseteq v$, and $u \cap v = \Lambda$. Then $r \cup s \in a + p$, by the definition of addition. Then $a + p \le b + q$, as witnessed by $r \cup s \in a + p$, $r \cup s \in SSC(w)$, and $w \in b + q$. That completes the proof of the first assertion of the lemma.

Lemma 8.11. *For $a, p, b, q \in \mathbb{F}$, if $b + q \in \mathbb{F}$ we have*

$$a < b \ \wedge \ p \leq q \to a + p < b + q$$

Remark. It is not assumed that $a + p \in \mathbb{F}$, which would make the proof easier.

Proof. Suppose $a < b$ and $p \leq q$. Then

$$\begin{array}{rl} a^+ \leq b & \text{by Lemma 5.30} \\ \exists u\,(u \in a^+) & \text{by the definition of addition} \\ a^+ \in \mathbb{F} & \text{by Lemma 4.19} \\ a^+ + p \leq b + q & \text{by Lemma 8.10} \\ (a+p)^+ \leq b + q & \text{by Lemma 8.3} \\ \exists u\,(u \in (a+p)^+) & \text{by the definition of } \leq \\ \exists u\,(u \in a + p) & \text{by definition of successor} \\ a + p \in \mathbb{F} & \text{by Lemma 8.6} \\ (a+p)^+ \in \mathbb{F} & \text{by Lemma 4.19} \\ a + p < (a+p)^+ & \text{by Lemma 5.37} \\ a + p < b + q & \text{by Lemma 5.23} \end{array}$$

That completes the proof of the lemma.

Lemma 8.12. *For $m \in \mathbb{F}$ we have*

$$USC(x) \in m \to SSC(x) \in 2^m.$$

Proof. Suppose $USC(x) \in m$. By Definition 7.1, 2^m contains all sets similar to $SSC(x)$. By Lemma 2.10, $SSC(x)$ is one of those sets, so $SSC(x) \in 2^m$. That completes the proof of the lemma.

Lemma 8.13. *For all z we have $2^z \neq \mathsf{zero}$.*

Proof. Suppose $2^z = \mathsf{zero}$. Then

$$\begin{array}{rl} \Lambda \in \mathsf{zero} & \text{by Definition 5.16} \\ \Lambda \in 2^z & \text{since } 2^z = \mathsf{zero} \\ \Lambda \ \sim SSC(a) \ \wedge \ USC(a) \in x & \text{by Definition 7.1} \\ SSC(a) = \Lambda & \text{since only } \Lambda \text{ is similar to } \Lambda \end{array}$$

But $a \in SSC(a)$, contradiction. That completes the proof of the lemma.

Lemma 8.14. *Suppose $x \sim y$, and $a \notin x$ and $b \notin y$. Then*

$$x \cup \{a\} \sim y \cup \{b\}.$$

Proof. Extend a similarity $f : x \to y$ by defining $f(a) = b$. We omit the details.

Lemma 8.15. *Let p and q be disjoint finite sets. Then $Nc(p \cup q) = Nc(p) + Nc(q)$.*

Proof. We have

$p \cup q \in \mathsf{FINITE}$	by Lemma 3.11
$Nc(p \cup q) \in \mathbb{F}$	by Lemma 4.21
$Nc(p) \in \mathbb{F}$	by Lemma 4.21
$Nc(q) \in \mathbb{F}$	by Lemma 4.21
$p \cup q \in Nc(p \cup q)$	by Lemma 4.11
$p \in Nc(p)$	by Lemma 4.11
$q \in Nc(q)$	by Lemma 4.11
$p \cup q \in Nc(p) + Nc(q)$	by the definition of addition
$Nc(p \cup q) \cap Nc(p) + Nc(q) \neq \Lambda$	since both contain $p \cup q$
$Nc(p) + Nc(q) \in \mathbb{F}$	by Lemma 8.6
$Nc(p \cup q) = Nc(p) + Nc(q)$	by Lemma 5.7

That completes the proof of the lemma.

Lemma 8.16. *For $p, q, r \in \mathbb{F}$, if $q + p \in \mathbb{F}$ we have*

$$\begin{array}{rcl} q + p & = & r + p \to q = r \\ p + q & = & p + r \to q = r. \end{array}$$

Proof. The two formulas are equivalent, by Lemma 8.3. We prove the first one by induction on p, which is legal since the formula is stratified. More precisely we prove by induction on p that

$$\forall q, r \in \mathbb{F}\,(q + p \in \mathbb{F} \to q + p = r + p \to q = r).$$

Base case, $p = 0$. Suppose $q + 0 = r + 0$. Then $q = r$ by the right identity property of addition, Lemma 8.2. That completes the base case.

Induction step. Suppose $q + p^+ = r + p^+$ and $q + p^+ \in \mathbb{F}$. Then

$(q + p)^+ = (r + p)^+$	by Lemma 8.2
$q + p \in \mathbb{F}$	by Lemma 8.9
$r + p \in \mathbb{F}$	by Lemma 8.9
$\exists u\,(u \in q + p)$	by Lemma 4.7
$\exists u\,(u \in r + p)$	by Lemma 4.7
$(q + p)^+ = q + p^+$	by Lemma 8.2
$(r + p)^+ = r + p^+$	by Lemma 8.2
$(q + p)^+ \in \mathbb{F}$	equality substitution
$(r + p)^+ \in \mathbb{F}$	equality substitution
$\exists u\,(u \in (q + p)^+)$	by Lemma 4.7
$\exists u\,(u \in (r + p)^+)$	by Lemma 4.7
$q + p = r + p$	by Lemma 5.12, since $(q + p)^+ = (r + p)^+$
$q = r$	by the induction hypothesis

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

Lemma 8.17. *Let $b \in \mathsf{FINITE}$ and $c \notin b$. Then*

$$Nc(SSC(b \cup \{c\}) = Nc(SSC(b)) + Nc(SSC(b)).$$

Proof. Define

$$R := \{x \cup \{c\} : x \in SSC(b)\}.$$

The definition can be rewritten in stratified form, so R can be defined in INF. Define $f : x \mapsto x \cup \{c\}$, which can also be defined in INF:

$$f := \{\langle x, x \cup \{c\}\rangle : x \in SSC(b)\}.$$

The formula is stratified, since all the occurrences of x can be given index 0, and $\{c\}$ and $SSC(b)$ are just parameters. Then $f : SSC(b) \to R$ is a similarity. (We omit the 150 steps required to prove that.)

We first note that if $x \in SSC(b \cup \{c\})$ and $c \in x$, then $x = (x - c) \cup \{c\}$, since x is finite and therefore has decidable equality. Similarly $b \cup \{c\}$ has decidable equality, so every $x \in SSC(b \cup \{c\})$ either contains c or not. If $c \in x$ then $x \in R$. If $c \notin x$ then $x \in SSC(b)$. Therefore

$$
\begin{aligned}
SSC(b \cup \{c\}) &= SSC(b) \cup R \\
SSC(b) &\sim R && \text{since } f : SSC(b) \to R \text{ is a similarity} \\
Nc(SSC(b)) &= Nc(R) && \text{by Lemma 4.12} \\
SSC(b) \cap R &= \Lambda && \text{since } c \notin b \\
SSC(b) &\in \mathsf{FINITE} && \text{by Lemma 3.17} \\
R &\in \mathsf{FINITE} && \text{by Lemma 3.14}
\end{aligned}
$$

$$
\begin{aligned}
Nc(SSC(b \cup \{c\})) &= Nc(SSC(b)) + Nc(R) && \text{by Lemma 8.15} \\
Nc(SSC(b \cup \{c\})) &= Nc(SSC(b)) + Nc(SSC(b)) && \text{since } Nc(SSC(b)) = Nc(R)
\end{aligned}
$$

That completes the proof of the lemma.

Lemma 8.18. *For $p \in \mathbb{F}$, if $2^{p^+} \in \mathbb{F}$, then $2^{p^+} = 2^p + 2^p$.*

Proof. Suppose $p \in \mathbb{F}$ and $2^{p^+} \in \mathbb{F}$. Then

$$
\begin{aligned}
&\exists u\,(u \in 2^{p^+}) && \text{by Lemma 4.7} \\
&USC(a) \in p^+ && \text{for some } a \in p, \text{ by definition of exponentiation} \\
&u \in p^+ \wedge q \in u && \text{for some } q, u, \text{ by Lemma 4.15} \\
&u \sim USC(a) && \text{by Lemma 4.9, since both are in } p^+ \\
&w \in USC(a) && \text{for some } w, \text{ by Lemma 6.20} \\
&c \in a \wedge w = \{c\} && \text{for some } c, \text{ by definition of } USC(a) \\
&USC(a) \in \mathsf{FINITE} && \text{by Lemma 4.4} \\
&a \in \mathsf{FINITE} && \text{by Lemma 3.10} \\
&a \in \mathsf{DECIDABLE} && \text{by Lemma 3.3} \\
&b := a - \{c\} && \text{definition of } b \\
&a = b \cup \{c\} && \text{since } a \in \mathsf{DECIDABLE} \\
&USC(a) = USC(b) \cup \{\{c\}\} && \text{by Lemma 6.15} \\
&SSC(b \cup \{c\}) \in 2^{p^+} && \text{by definition of exponentiation} \\
&Nc(SSC(b \cup \{c\}) = 2^{p^+} && \text{by Lemma 4.11}
\end{aligned}
$$

(63) $\quad Nc(SSC(b \cup \{c\}) = Nc(SSC(b)) + Nc(SSC(b)) \qquad$ by Lemma 8.17

$$
\begin{array}{rl}
USC(a) \in \mathsf{DECIDABLE} & \text{by Lemma 3.3} \\
USC(b) = USC(a) - \{\{c\}\} & \text{since } USC(a) \in \mathsf{DECIDABLE} \\
USC(b) \in p & \text{by Lemma 5.10} \\
SSC(b) \in 2^p & \text{by the definition of exponentiation} \\
SSC(b) \in Nc(SSC(b)) & \text{by Lemma 4.11} \\
SSC(b) \in \mathsf{FINITE} & \text{by Lemma 3.17} \\
Nc(SSC(b)) \in \mathbb{F} & \text{by Lemma 4.21} \\
Nc(SSC(b)) = 2^p & \text{by Lemma 5.7}
\end{array}
$$

Then $2^{p^+} = 2^p + 2^p$ as desired, by (63). That completes the proof of the lemma.

Lemma 8.19. *For $m \in \mathbb{F}$, $2^m = \mathsf{one} \leftrightarrow m = \mathsf{zero}$.*

Proof. Left to right. We have

$$
\begin{array}{rl}
2^m = \mathsf{one} & \text{assumption} \\
2^{\mathsf{two}} = \mathsf{four} & \text{by Lemma 7.8} \\
\mathsf{two} \le m \to 2^{\mathsf{two}} \le 2^m & \text{by Lemma 7.18} \\
\mathsf{two} \le m \to \mathsf{four} \le \mathsf{one} & \text{by transitivity of } \le \\
\mathsf{one} < \mathsf{four} & \text{by Lemma 7.11} \\
\mathsf{two} \not\le m & \text{otherwise } \mathsf{one} < \mathsf{four} \ \land\ \mathsf{four} \le \mathsf{one} \\
m < \mathsf{two} \lor \mathsf{two} \le m & \text{by Theorem 5.18} \\
m < \mathsf{two} & \text{since } \mathsf{two} \not\le m \\
m = \mathsf{zero} \ \lor\ m = \mathsf{one} & \text{by Lemma 7.13} \\
2^{\mathsf{one}} = \mathsf{two} & \text{by Lemma 7.7} \\
\mathsf{one} \ne \mathsf{two} & \text{by Lemma 5.36} \\
m \ne \mathsf{one} & \text{since } 2^m = \mathsf{zero} \\
m = \mathsf{zero} & \text{since } m = \mathsf{zero} \lor m = \mathsf{one} \text{ but } m \ne \mathsf{one}
\end{array}
$$

Right to left. Suppose $m = \mathsf{zero}$. Then $2^m = 2^{\mathsf{zero}} = \mathsf{one}$, by Lemma 7.6. That completes the proof of the lemma.

Lemma 8.20. *For $n, m \in \mathbb{F}$, if $2^n = 2^m$ and 2^n is inhabited, then $n = m$.*

Remark. The reader is invited to try a direct proof using the definition of exponentiation. It would work if we had the converse of Lemma 6.8. The only proof of that converse that we know requires this lemma. Therefore, we give a more complicated (but correct) proof by induction.

Proof. We prove by induction on n that for $n \in \mathbb{F}$ with 2^n inhabited, we have

$$\exists u\,(u \in 2^n) \to \forall m \in \mathbb{F}\,(2^n = 2^m \to n = m) \tag{64}$$

The formula is stratified giving n and m both index 0, so it is legal to proceed by induction.

The base case follows from Lemma 8.19.

Induction step. Suppose $2^{n^+} = 2^m$ and n^+ is inhabited. We have $m = \mathsf{zero} \ \lor\ m \ne \mathsf{zero}$, by Lemma 5.19.

Case 1, $m = \mathsf{zero}$. Then by Lemma 8.19, $n^+ = \mathsf{zero}$, contradiction.

Case 2, $m \neq \mathsf{zero}$. Then

$$\begin{array}{rl} \exists r \in \mathbb{F}\,(m = r^+) & \text{by Lemma 4.17} \\ 2^{n^+} = 2^{r^+} & \text{since } 2^{n^+} = 2^m \\ 2^n + 2^n = 2^r + 2^r & \text{by Lemma 8.18} \\ r < n \ \vee \ r = n \ \vee \ n < r & \text{by Theorem 5.18} \end{array}$$

We argue by cases.

Case 1, $r < n$. Then

$$\begin{array}{rl} 2^r \le 2^n & \text{by Lemma 7.18} \\ 2^r \neq 2^n & \text{by the induction hypothesis} \\ 2^r < 2^n & \text{by the definition of } < \\ 2^{n^+} \in \mathbb{F} & \text{by Lemma 7.5} \\ 2^{r^+} = 2^r + 2^r & \text{by Lemma 8.18} \\ 2^r + 2^r < 2^n + 2^n & \text{by Lemma 8.11} \\ 2^n + 2^n = 2^{n+} & \text{by Lemma 8.18} \\ 2^{r^+} < 2^{n+} & \text{by Lemma 5.23} \end{array}$$

But that contradicts $2^{n^+} = 2^{r^+}$. That completes Case 1.

Case 2, $n < r$, similarly leads to a contradiction. We omit the steps.

Case 3, $n = r$. Then $2^n = 2^r$. Substituting 2^n for 2^r in the identity $2^r + 2^r = 2^r + 2^r$, we have $2^n + 2^n = 2^r + 2^r$. Then $2^{n^+} = 2^{r^+} = 2^m$ as desired. That completes the induction step. That completes the proof of the lemma.

Lemma 8.21. *Let $m, n \in \mathbb{F}$. If $m < n$ and 2^n is inhabited, then 2^m is inhabited and $2^m < 2^n$.*

Proof. Suppose $m < n$ and 2^n is inhabited. Then

$$\begin{array}{rl} m \le n & \text{by the definition of } < \\ 2^m \le 2^n & \text{by Lemma 7.18} \\ m \neq n & \text{by the definition of } < \\ 2^m \neq 2^n & \text{by Lemma 8.20} \\ 2^m < 2^n & \text{by the definition of } < \end{array}$$

That completes the proof of the lemma.

Lemma 8.22. *For $p, q \in \mathbb{F}$ we have*

$$p \le q \leftrightarrow \exists k \in \mathbb{F}\,(p + k = q).$$

Proof. By induction on q. The formula is stratified, giving all variables index 0.

Base case, $p \le \mathsf{zero} \leftrightarrow \exists k \in \mathbb{F}, p + k = \mathsf{zero}$. Left to right: Suppose $p \le \mathsf{zero}$. Then $p = \mathsf{zero} \ \vee \ p < \mathsf{zero}$, by Lemma 5.21. But $p \not< \mathsf{zero}$ by Lemma 5.29. Hence $p = \mathsf{zero}$. Then $p + k = \mathsf{zero} + k = \mathsf{zero}$ by Lemma 8.3. . Right to left. Suppose $p + k = \mathsf{zero}$. Then by the definition of addition, there exists sets $a \in p$ and $b \in k$ such that $a \cup b \in \mathsf{zero}$. By definition of zero, $\mathsf{zero} = \{\Lambda\}$, so $a \cup b = \Lambda$. Then $a = \Lambda$.

Then $\Lambda \in p$ and $\Lambda \in \mathsf{zero}$. Then by Lemma 5.7, $p = \mathsf{zero}$. That completes the base case.

Induction step. Assume q^+ is inhabited. We have to show

$$p \le q^+ \leftrightarrow \exists k \in \mathbb{F}\,(p + k = q^+).$$

Left to right: suppose $p \le q^+$. Then $p = q^+ \ \vee\ p \le q$, by Lemma 5.32.

Case 1, $p \le q$. Then by the induction hypothesis, there exists $k \in \mathbb{F}$ such that $p + k = q$. We have

$$\begin{array}{rl} \exists u\,(u \in q^+) & \text{by hypothesis} \\ \exists u\, u \in (p+k)^+ & \text{since } p + k = q \\ p + (k^+) = (p+k)^+ = q^+ & \text{by Lemma 8.2} \\ \exists u\,(u \in k^+) & \text{by the definition of addition} \\ k^+ \in \mathbb{F} & \text{by Lemma 4.19} \end{array}$$

That completes Case 1.

Case 2, $p = q^+$. Then taking $k = \mathsf{zero}$ we have

$$p + k = p + \mathsf{zero} = p = q^+.$$

That completes Case 2.

Right to left. Suppose $k \in \mathbb{F}$ and $p + k = q^+$. We have to show $p \le q^+$. By definition of addition, there exist a and b with $a \in p$ and $b \in k$, and $a \cap b = \Lambda$ and $a \cup b \in q^+$. Then a is a separable subset of $a \cup b$, so $p \le q^+$ by the definition of $\le$. That completes the induction step. That completes the proof of the lemma.

9. Definition of multiplication

In this section we show how to define multiplication and derive its usual arithmetical properties. Some care is required to make sure that the equations for multiplication work without assuming $\mathbb{F}$ is finite; the equations must have the property that if one side is in $\mathbb{F}$, so is the other side. That is, if one side "overflows", so does the other side. To arrange this, we must first ensure that addition has the same property. This ultimately goes back to the theorem that successor never takes the value zero, not just on an integer argument but on any argument whatever. Secondly, care must be taken throughout the development of multiplication that one does not assume everything is an integer. We need the equation $x \cdot y^+ = x \cdot y + x$ to be true without assuming $x \cdot y \in \mathbb{F}$. It will, however, be fine to assume $x \in \mathbb{F}$ and $y \in \mathbb{F}$, and indeed, we need to use induction on y to prove that equation. But we must leave open the possibility that $x \cdot y = \Lambda$, so we can deal with "overflow."[6]

We must not assume that it is decidable whether the value of $x \cdot y$ is an integer or is Λ. We must therefore be careful about what exactly is the domain of multiplication. The class $\mathbb{F}$ is too small, as explained above. The class NC of all cardinals is too large, because we cannot prove in INF that NC is closed under successor.

[6]Specker did not need (or develop) the theory of multiplication. He proved Specker 6.8 by an argument resting on the theorem that the universe and the power set of the universe have the same cardinal. That fails constructively because we replace the power set by the separable power set SSC, and the universe is not a separable subset of the universe (unless logic is classical). Our constructive proof of Specker 6.8 instead uses multiplication, in the law $2^p \cdot 2^q = 2^{p+q}$. That explains why we had to develop multiplication and Specker did not.

Definition 9.1. *The class of SF of "semifinite cardinals" is defined to be the least class containing* zero *and closed under successor.*

Remark. Compare to the least class closed under inhabited successor, which is $\mathbb{F}$, or nonempty successor, which gives a class called $\mathbb{H}$ that is not used in this paper. For all we know at this point, $\mathbb{F}$ might be finite, and then Λ would be a successor, so Λ might belong to SF, while it certainly does not belong to $\mathbb{F}$.

Lemma 9.2. *SF is closed under successor.*

Proof. Let $x \in SF$. Then x belongs to every set w containing 0 and closed under successor. Then $x^+ \in w$. Since w was arbitrary, $x^+ \in SF$. That completes the proof of the lemma.

Lemma 9.3. *$\mathbb{F} \subseteq SF$.*

Proof. By Lemma 9.2, SF is closed under successor. In particular it is closed under inhabited successor; therefore by definition of $\mathbb{F}$, we have $\mathbb{F} \subseteq SF$. That completes the proof of the lemma.

Lemma 9.4. *Let $x \in SF$. Then $x = \mathsf{zero} \ \lor \ \exists u \in SF\,(u^+ = x)$.*

Proof. Let
$$w := \{x \in SF : x = \mathsf{zero} \ \lor \ \exists u \in SF\,(u^+ = x)\}.$$
Evidently w contains zero. I say that w is closed under successor. Suppose $x \in w$. Then

$$\begin{array}{rl} x \in SF & \text{by definition of } w \\ x^+ \in SF & \text{by Lemma 9.2} \\ \exists u \in SF\,(u^+ = x^+) & \text{since } x \text{ is such a } u \\ x^+ \in w & \text{by definition of } w \end{array}$$

That completes the proof that w is closed under successor. Then by definition of SF, we have $SF \subseteq w$. That completes the proof of the lemma.

Lemma 9.5. *SF is closed under addition.*

Proof. Let $x \in SF$. Define
$$w := \{y \in SF : x + y \in SF\}.$$
I say that w contains zero and is closed under successor. It contains zero since $x + \mathsf{zero} = x$. Suppose $y \in w$; that is, $x + y \in SF$. Then $(x+y)^+ \in SF$. But $(x+y)^+ = x + y^+$ by Lemma 8.2. Hence $y^+ \in w$. Since w was arbitrary, $SF \subseteq w$. That completes the proof of the lemma.

Definition 9.6. *The graph of multiplication is defined as the intersection $\mathbb{G}$ of all relations w satisfying*

$$\begin{array}{c} x \in SF \to \langle x, \mathsf{zero}, \mathsf{zero}\rangle \in w \\ x \in SF \to \langle \mathsf{zero}, x, \mathsf{zero}\rangle \in w \\ \langle x, y, z\rangle \in w \to \langle x, y^+, z + x\rangle \in w \end{array}$$

These formulas are stratifiable, giving x, y, z all the same index, the relation $\mathbb{G}$ is definable in INF.

Lemma 9.7. *The graph of multiplication $\mathbb{G}$ is definable in* INF

Proof. The formula in the definition is stratifiable, giving x, y, and z index 0 and w index 1.

Lemma 9.8. *The graph of multiplication satisfies the conditions on w used in the definition of multiplication. That is,*

$$x \in SF \to \langle x, \mathsf{zero}, \mathsf{zero}\rangle \in \mathbb{G}$$
$$x \in SF \to \langle \mathsf{zero}, x, \mathsf{zero} \in \mathbb{G}$$
$$\langle x, y, z\rangle \in G \to \langle x, y^+, z + x\rangle \in \mathbb{G}$$

Proof. Let w satisfy the "multiplication conditions" mentioned in the definition. Since $\mathbb{G}$ is the intersection of all such w, the first two assertions of the lemma are immediate. To prove the third assertion: Suppose $\langle x, y, z\rangle \in w$. Then $\langle x, y^+, z + x\rangle \in w$. Since w was arbitrary, $\langle x, y^+, z + x\rangle$ belongs to the intersection of all such w. That is,$\langle x, y^+, z + x\rangle \in \mathbb{G}$. That completes the proof of the lemma.

Lemma 9.9. *For all x, y, z we have*

$$\langle x, y, z\rangle \in \mathbb{G} \to x \in SF \ \wedge \ y \in SF \ \wedge \ z \in SF.$$

Proof. Define

$$w := \{\langle x, y, z\rangle \in \mathbb{G} : x \in SF \ \wedge \ y \in SF \ \wedge \ z \in SF\}.$$

I say that w satisfies the conditions used in the definition of $\mathbb{G}$. The first two conditions are immediate, since $\mathsf{zero} \in SF$. The third condition follows from the closure of SF under successor and addition, Lemmas 9.2 and 9.5. That completes the proof of the lemma.

Lemma 9.10. *Suppose $\langle x, y, z\rangle \in \mathbb{G}$. Then*

$$z = \mathsf{zero} \ \vee \exists u \in SF\,(u^+ = z).$$

Proof. Suppose $\langle x, y, z\rangle \in \mathbb{G}$. By Lemma 9.9, we have $z \in SF$. By Lemma 9.4, $z = \mathsf{zero}$ or $\exists u \in SF\,(u^+ = z)$. That completes the proof of the lemma.

Lemma 9.11. *Let $x \in SF$ and $y \in SF$. Then $x+y = \mathsf{zero} \to x = \mathsf{zero} \wedge y = \mathsf{zero}$.*

Proof. Define

$$w := \{y : y \in SF \ \wedge \ \forall x \in SF\,(x + y = \mathsf{zero} \to x = \mathsf{zero} \ \wedge \ y = \mathsf{zero}\}.$$

Then $0 \in w$, since $x + \mathsf{zero} = x$ holds without any condition on x. And w is closed under successor, since $x + y^+ = (x + y)^+$ also holds without any precondition. Therefore, by definition of SF, we have $SF \subseteq w$. That completes the proof of the lemma.

Lemma 9.12. $\langle \mathsf{zero}, y, z\rangle \in \mathbb{G} \to z = \mathsf{zero}$.

Proof. Define

$$w := \{\langle x, y, z\rangle \in \mathbb{G} : x = \mathsf{zero} \to z = \mathsf{zero}\}.$$

The formula is stratified, giving x, y, and z index 0; G is a parameter. Therefore the definition is legal.

I say that w satisfies the conditions defining $\mathbb{G}$. Ad the first condition: We have $\langle \mathsf{zero}, y, \mathsf{zero}\rangle \in w$ and $\langle x, \mathsf{zero}, \mathsf{zero}\rangle \in w$.

Ad the second condition. Suppose $\langle x, y, z\rangle \in w$. Then

$$
\begin{array}{rl}
\langle x, y, z\rangle \in \mathbb{G} & \text{by definition of } w \\
\langle x, y^+, z + x\rangle \in w \in G & \text{by Lemma 9.8} \\
x = \mathsf{zero} \to z = \mathsf{zero} & \text{by definition of } w
\end{array}
$$

Suppose $x = \mathsf{zero}$. Then

$$z + x = \mathsf{zero} + x = x = \mathsf{zero}.$$

That completes the verification of the second condition.

Then by definition of $\mathbb{G}$, $\mathbb{G} \subseteq w$. That completes the proof of the lemma.

Lemma 9.13. *Suppose* $\langle x, y, z\rangle \in \mathbb{G}$. *Then*

$$
\begin{array}{ll}
 & z = \mathsf{zero} \to x = \mathsf{zero} \ \vee \ y = \mathsf{zero} \\
\textit{and} & z \neq \mathsf{zero} \to \exists p, q, r\, (x = p^+ \ \wedge \ y = q^+ \ \wedge \ p \in SF \ \wedge \ q \in SF \\
 & \wedge \ \langle x, q, r\rangle \in \mathbb{G} \ \wedge \ z = r + x = (r + p)^+)
\end{array}
$$

Proof. Define

$$
\begin{array}{rcl}
w & := & \{\, \langle x, y, z\rangle \in \mathbb{G} : (z = \mathsf{zero} \to x = \mathsf{zero} \ \vee \ y = \mathsf{zero}) \\
 & & \wedge \ z \neq \mathsf{zero} \to \exists p, q, r\, (x = p^+ \ \wedge \ y = q^+ \ \wedge \ p \in SF \ \wedge \ q \in SF \\
 & & \wedge \ \langle x, q, r\rangle \in \mathbb{G} \ \wedge \ z = r + x = (r + p)^+) \,\}
\end{array}
$$

The formula is stratified, so the definition is legal. I say that w satisfies the conditions in the definition of $\mathbb{G}$.

The first condition is

$$\forall y\, (y \in SF \to \langle y, \mathsf{zero}, \mathsf{zero}\rangle \in w \ \wedge \ \langle \mathsf{zero}, y, \mathsf{zero}\rangle \in w) \tag{65}$$

This requires about 50 simple inferences, using the definition of $\mathbb{G}$ several times. We omit those steps.

The second condition is

$$\forall u, v, t\, (\langle u, v, t\rangle \in w \to \langle u, v^+, t + u\rangle \in w) \tag{66}$$

We have

$$
\begin{array}{rl}
\langle u, v, t\rangle \in w & \text{assumption} \\
\langle u, v, t\rangle \in \mathbb{G} & \text{by definition of } w \\
\langle u, v^+, t + u\rangle \in \mathbb{G} & \text{by Lemma 9.8}
\end{array}
$$

To prove $\langle u, v^+, t + u\rangle \in w$, it remains to check the other two conditions in the definition of w. We have

$$
\begin{array}{lrl}
 & \langle u, v, t\rangle \in \mathbb{G} & \text{by assumption} \\
 & t \in SF \ \wedge \ u \in SF & \text{by Lemma 9.9} \\
(67) & t + u = \mathsf{zero} \to u = \mathsf{zero} & \text{by Lemma 9.11}
\end{array}
$$

That is the first of the two conditions.

Now we still must prove

$$t + u \neq \mathsf{zero} \to \exists p, q\, (u = p^+ \ \wedge \ v^+ = q^+ \ \wedge \ q \in SF \ \wedge \ p \in SF) \tag{68}$$

To prove (68):

$$\begin{array}{rl} t+u \neq \mathsf{zero} & \text{assumption} \\ t+u \in SF & \text{by Lemma 9.9} \\ v^+ \neq \mathsf{zero} & \text{by Lemma 4.16} \\ u = \mathsf{zero} \ \vee\ \exists p \in SF\,(u = p^+) & \text{by Lemma 9.4} \end{array}$$

If $u = p^+$ then we are done, using p and v to instantiate the quantified variables p and q in (68). So we may assume $u = \mathsf{zero}$. Then $t + u = t + \mathsf{zero} = t$, and we have

$$\langle \mathsf{zero}, v, t\rangle \in \mathbb{G} \qquad \text{since } \langle u, v, t\rangle \in \mathbb{G}$$

Then by Lemma 9.12, $t = \mathsf{zero}$. Then, since $u = \mathsf{zero}$, we have $t + u = \mathsf{zero}$, contradicting the assumption that $t + u \neq \mathsf{zero}$. That completes the proof of (68), and that in turn completes the proof of (66). Together with (65), this shows that w satisfies the conditions in Definition 9.6. Therefore, $\mathbb{G} \subseteq w$. That completes the proof of the lemma.

Lemma 9.14. *Let $m \in SF$ be inhabited. Then $m \in \mathbb{F}$.*

Proof. Let $w := \{m \in SF : \exists u\,(u \in m)\}$. I say that w contains zero and is closed under successor. First, zero is inhabited, so $\mathsf{zero} \in w$. Second, suppose $m \in w$. Then let $u \in m$. Suppose m^+ is inhabited. Then by Lemma 4.19, $m^+ \in \mathbb{F}$. Therefore w is closed under successor, as claimed. Then by definition of SF, we have $SF \subseteq w$. That completes the proof of the lemma.

Lemma 9.15. *Let $x \in SF$. Then $x^+ \in \mathbb{F} \to x \in \mathbb{F}$.*

Proof. We have

$$\begin{array}{rl} \exists u\,(u \in x^+) & \text{by Lemma 4.7} \\ u \in x^+ & \text{fixing } u \\ p \in x & \text{where } u = p \cup \{c\}\text{, by definition of } x^+ \\ x \in \mathbb{F} & \text{by Lemma 9.14} \end{array}$$

That completes the proof of the lemma.

Lemma 9.16. $y \in \mathbb{F} \to \forall x, z, t\,(\langle x, y, z\rangle \in \mathbb{G} \to \langle x, y, t\rangle \in \mathbb{G} \to z = t)$.

Remarks. We do not assume that x, z, t are in $\mathbb{F}$, and we do not claim that z exists, only that it is unique (if it exists).

Proof. By induction on y, which is legal since the formula is stratified, as discussed after Definition 9.6.

Base case: Suppose $\langle x, \mathsf{zero}, z\rangle \in \mathbb{G}$. I say that $z = \mathsf{zero}$. By Lemma 9.4, $z = \mathsf{zero} \vee \exists p\,(p^+ = z)$. If $z = 0$, we are done; so we may assume $z = p^+$. Then by Lemma 9.13, $\mathsf{zero} = q^+$ for some q. But that contradicts Lemma 4.16. That completes the proof that $z = 0$.

Now assume $\langle x, \mathsf{zero}, t\rangle \in \mathbb{G}$. We will prove $t = \mathsf{zero}$, and hence $z = t$. Here is the proof: By Lemma 9.4, we have $t = \mathsf{zero} \ \vee\ \exists p\,(p^+ = t)$. If $t = \mathsf{zero}$, we are done, so we may assume $t = p^+$. Then

$$\begin{array}{rl} t \in SF & \text{by Lemma 9.9} \\ t \neq \mathsf{zero} & \text{by Lemma 4.16} \end{array}$$

Now by Lemma 9.13, since $\langle x, \mathsf{zero}, t\rangle \in \mathbb{G}$, there exist r, b, and c with

$$\begin{aligned} t &= (c+r)^+ \\ \mathsf{zero} &= b^+ \\ x &= r^+ \end{aligned}$$

But $\mathsf{zero} = b^+$ contradicts Lemma 4.16. That completes the proof that $t = \mathsf{zero}$. That completes the base case.

Induction step: Suppose $y \in \mathbb{F}$ and y^+ is inhabited (as always in an induction proof). Then $y^+ \in \mathbb{F}$, and $\langle x, y^+, z\rangle \in \mathbb{G}$ and $\langle x, y^+, t\rangle \in \mathbb{G}$. We have to prove $z = t$. Then By Lemmas 9.4 and 4.16, we have

$$z = \mathsf{zero} \ \vee \ z \neq \mathsf{zero}.$$

Similarly

$$t = \mathsf{zero} \ \vee \ t \neq \mathsf{zero}.$$

We argue by cases:

Case 1: $z = \mathsf{zero}$ and $t = \mathsf{zero}$. Then $z = t = \mathsf{zero}$.

Case 2: $z \neq \mathsf{zero}$ and $t = \mathsf{zero}$. Then by Lemma 9.13, since $z \neq \mathsf{zero}$ we have $x = \mathsf{zero}$, and since $t = \mathsf{zero}$ we have $x \neq \mathsf{zero}$, contradiction. That completes Case 2.

Case 3: $z = \mathsf{zero}$ and $t \neq \mathsf{zero}$. Interchange 'z' and 't' in the proof of Case 3.

Case 4: $z \neq \mathsf{zero}$ and $t \neq \mathsf{zero}$. Then by Lemma 9.13,

$$\exists p, q, r\,(x = p^+ \ \wedge \ y^+ = q^+ \ \wedge \ z = (r+p)^+ \ \wedge \ \langle x, q, r\rangle \in \mathbb{G}).$$

Similarly

$$\exists a, b, c\,(x = a^+ \ \wedge \ y^+ = b^+ \ \wedge \ t = (c+a)^+ \ \wedge \ \langle x, b, c\rangle \in \mathbb{G}).$$

Fixing particular a, b, c, p, q, r, we have

$$\begin{aligned}
q^+ = y^+ &= b^+ && \\
y &\in \mathbb{F} && \text{by Lemma 9.15, since } y^+ \in \mathbb{F} \\
q &\in \mathbb{F} && \text{by Lemma 9.15, since } q^+ = y^+ \\
b &\in \mathbb{F} && \text{by Lemma 9.15, since } b^+ = y^+ \\
q = y &= b && \text{by Lemma 5.12} \\
r &= c && \text{by the induction hypothesis} \\
z = (r+p)^+ &= r + p^+ && \text{by Lemma 8.2} \\
z &= c + p^+ && \text{since } r = c \\
z &= c + x && \text{since } p^+ = x \\
z &= c + a^+ && \text{since } a^+ = x \\
t = (c+a)^+ &= c + a^+ && \text{by Lemma 8.2} \\
z &= t && \text{by the previous two lines}
\end{aligned}$$

That completes Case 4.

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

Definition 9.17.

$$x \cdot y := \{u : \exists z\, (\langle x, y, z\rangle \in \mathbb{G} \ \wedge \ u \in z\}.$$

The formula is stratified, giving x, y, and z index 1 and u index 0. $\mathbb{G}$ is a parameter.

Lemma 9.18. *Let $x \in SF$. Then $x \cdot \mathsf{zero} = \mathsf{zero}$.*

Proof. Suppose $x \in SF$. By extensionality, it suffices to show

$$t \in x * \mathsf{zero} \leftrightarrow t \in \mathsf{zero} \tag{69}$$

Left to right: We have

$$\begin{array}{rl} t \in x * \mathsf{zero} & \text{assumption} \\ x = \mathsf{zero} \ \vee \exists u\, (x = u^+) & \text{by Lemma 9.4} \end{array}$$

In case $x = \mathsf{zero}$, we $z = \mathsf{zero}$ by Lemma 9.12. Then since $t \in z$, we have $t \in zero$ and are done.

Therefore we may assume $x = u^+$ for some u. We have

$$\begin{array}{rl} z \in SF & \text{by Lemma 9.9} \\ z = \mathsf{zero} \ \vee \ \exists p\, (z = p^+) & \text{by Lemma 9.4} \end{array}$$

In case $z = 0$, we are done, since we have $t \in z$. Therefore we may assume $z = p^+$. Then

$$\begin{array}{rl} z \neq \mathsf{zero} & \text{by Lemma 4.16} \\ u^+ = a^+ \wedge \mathsf{zero} = b^+ & \text{for some } a, b, \text{ by Lemma 9.13} \\ b^+ \neq \mathsf{zero} & \text{by Lemma 4.16} \end{array}$$

That contradiction completes the proof of the left-to-right direction of (69).

Right to left: Assume $t \in \mathsf{zero}$. We have to prove $t \in x \cdot \mathsf{zero}$. By Definition 9.17, it suffices to prove $\langle x, \mathsf{zero}, z\rangle \in \mathbb{G}$ for some z. We take $z = \mathsf{zero}$; we have $\langle x, \mathsf{zero}, \mathsf{zero}\rangle \in \mathbb{G}$ by Lemma 9.8. That completes the proof of the lemma.

Lemma 9.19. *Let $x \in \mathbb{F}$. Then $\mathsf{zero} \cdot x = \mathsf{zero}$.*

Remark. We have to assume $x \in \mathbb{F}$, not just $x \in SF$, because we have not proved that $y \in SF \ \wedge \ y^+ = t^+ \to t \in SF$, whereas we have proved in Lemma 9.15 that $y \in SF \ \wedge \ y^+ \in \mathbb{F} \ \wedge \ y^+ = t^+ \to t \in \mathbb{F}$. With the weaker assumptions we cannot hope to prove $y = t$ (at least not without first proving $\mathbb{F}$ is not finite), since possibly y is the maximum integer and $t = \Lambda$. In that case, $y^+ = t^+ = \Lambda$ but $y \neq t$.
Proof. Assume $x \in \mathbb{F}$. By extensionality, it suffices to prove

$$t \in \mathsf{zero} \cdot x \leftrightarrow t \in \mathsf{zero} \tag{70}$$

Left to right: We have

$$\begin{array}{rl} t \in \mathsf{zero} \cdot x & \text{assumption} \\ \langle \mathsf{zero} x z\rangle \in \mathbb{G} & \text{for some } z, \text{ by Definition 9.17} \\ z \in SF & \text{by Lemma 9.9} \\ z = \mathsf{zero} \ \vee \ \exists u \in SF\, (u^+ = z) & \text{by Lemma 9.13} \end{array}$$

If $z = \mathsf{zero}$ we are done, since $t \in z$. So we may assume $z = u^+$ and $u \in SF$. Then

$$\begin{array}{rl} z \neq \mathsf{zero} & \text{by Lemma 4.16} \\ \mathsf{zero} = p^+ & \text{by Lemma 9.13} \end{array}$$

That contradicts Lemma 4.16. That completes the proof of the left-to-right direction of (70).

Right to left: Assume $t = \mathsf{zero}$. By Definition 9.17, it suffices to prove $\langle \mathsf{zero}, x, z\rangle \in \mathbb{G}$ for some z with $t \in z$. We can take $z = \mathsf{zero}$, since $\langle \mathsf{zero}, x, \mathsf{zero}\rangle \in \mathbb{G}$ by Lemma 9.8. That completes the proof of the lemma.

Lemma 9.20. *Suppose $x \in SF$ and $y \in \mathbb{F}$ and $y^+ \in \mathbb{F}$ and $x \cdot y \in SF$. Then*

$$(\forall z \in SF\,(\langle x, y, z\rangle \in \mathbb{G} \leftrightarrow z = x \cdot y)) \to x \cdot y^+ = x \cdot y + x.$$

Proof. Assume $x \in SF$ and $y \in \mathbb{F}$ and $y^+ \in \mathbb{F}$. Then assume

$$\forall z \in SF\,(\langle x, y, z\rangle \in \mathbb{G} \leftrightarrow z = x \cdot y) \tag{71}$$

By extensionality, it suffices to prove

$$u \in x \cdot y^+ \leftrightarrow u \in x \cdot y + x \tag{72}$$

We separately prove the two directions of (72).

Left to right. Assume $u \in x \cdot y^+$. By Definition 9.17, we have

$$u \in x \cdot y^+ \leftrightarrow \exists z\,(\langle x, y^+, z\rangle \in \mathbb{G} \ \wedge \ u \in z)$$

Since $u \in x \cdot y$ we have, for some z,

$$\begin{array}{rl} \langle x, y^+, z\rangle \in \mathbb{G} \ \wedge \ u \in z & \text{by Lemma 9.8} \\ z \in SF & \text{by Lemma 9.9} \\ \langle x, q, p\rangle \in \mathbb{G} \ \wedge \ q^+ = y^+ \ \wedge \ z = p + x & \text{for some } p, q, \text{ by Lemma 9.13} \\ q \in \mathbb{F} & \text{by Lemma 9.15, since } y^+ \in \mathbb{F} \text{ and } q^+ = y^+ \\ q = y & \text{by Lemma 5.12} \\ \langle x, y, p\rangle \in \mathbb{G} \ \wedge \ u \in p + x & \text{since } q = y \\ p = x \cdot y & \text{by (71)} \end{array}$$

Therefore

$$\langle x, y, x \cdot y\rangle \in \mathbb{G} \ \wedge \ u \in x \cdot y + x$$

By (71) this becomes

$$u \in x \cdot y + x$$

That completes the proof of the left-to-right direction of (72).

To prove the right-to-left direction: Assume $u \in x \cdot y + x$. We have to prove $u \in x \cdot y^+$. By Definition 9.17, it suffices to prove

$$\exists z\,(\langle x, y^+, z\rangle \in \mathbb{G} \ \wedge \ u \in z. \tag{73}$$

Take $z = x{\cdot}y{+}z$. By (71) and the hypothesis that $x{\cdot}y \in SF$, we have $\langle x, y, x{\cdot}y\rangle \in \mathbb{G}$. Then by Lemma 9.8, we have (73). That completes the proof of the lemma.

Lemma 9.21. *Suppose $x \in SF$ and $y \in \mathbb{F}$ and $y^+ \in \mathbb{F}$. Suppose*

$$x \cdot y \in SF \ \wedge \ \forall z \in SF\,(\langle x, y, z\rangle \in \mathbb{G} \leftrightarrow z = x \cdot y). \tag{74}$$

Then

$$x \cdot y^+ \in SF \ \wedge \ \forall z \in SF\,(\langle x, y^+, z\rangle \in \mathbb{G} \leftrightarrow z = x \cdot y^+).$$

Proof. Assume (74). We have to prove

$$x \cdot y^+ \in SF \tag{75}$$

and also that for $z \in SF$ we have

$$\langle x, y^+, z\rangle \in \mathbb{G} \leftrightarrow z = x \cdot y^+. \tag{76}$$

Therefore we can prove (76) by cases according as $x = \mathsf{zero}$ or not.

Case 1, $x = \mathsf{zero}$. We need the fact that if $\langle \mathsf{zero}, y, z\rangle \in \mathbb{G}$, then $z = \mathsf{zero}$, which is easily proved by SF-induction. After that observation, (76) is immediate when $x = \mathsf{zero}$. That completes the case $x = \mathsf{zero}$.

Case 2, $x \neq \mathsf{zero}$. By Lemma 9.20, since we have $x \cdot y \in SF$ by (74),

$$x \cdot y^+ = x \cdot y + x \tag{77}$$

We prove both directions of (76).

Left to right: We have

$$\begin{array}{rl}
\langle x, y^+, z\rangle \in \mathbb{G} & \text{by assumption} \\
y^+ \neq \mathsf{zero} & \text{by Lemma 4.16} \\
z \neq \mathsf{zero} & \text{by Lemma 9.13, since } x \neq \mathsf{zero} \\
\exists p, q\,(\langle x, q, p\rangle \in \mathbb{G} \ \wedge \ q^+ = y^+ \ \wedge \ z = p + x) & \text{by Lemma 9.13} \\
\langle x, q, p\rangle \in \mathbb{G} \ \wedge \ q^+ = y^+ \ \wedge \ z = p + x & \text{fixing } p \text{ and } q
\end{array}$$

Since $y^+ \in \mathbb{F}$ and $q^+ = y^+$, Lemma 9.15 tells us $q \in \mathbb{F}$, so by Lemma 5.12, $q = y$.

$$\begin{array}{rl}
\langle x, y, p\rangle \in \mathbb{G} \ \wedge \ z = p + x & \text{since } q = y \\
p = x \cdot y & \text{by (74) with } z \text{ instantiated to } p \\
z = x \cdot y + x & \text{since } z = p + x \text{ and } p = x \cdot y \\
z = x \cdot y^+ & \text{by (77)}
\end{array}$$

That completes the proof of the left-to-right direction of (76).

Right to left: It suffices to show

$$\langle x, y^+, x \cdot y^+\rangle \in \mathbb{G}.$$

We have

$$\begin{array}{rl}
\langle x, y, x \cdot y\rangle \in \mathbb{G} & \text{by (74)} \\
\langle x, y^+, x \cdot y + x\rangle \in \mathbb{G} & \text{by Lemma 9.8} \\
\langle x, y^+, x \cdot y^+\rangle \in \mathbb{G} & \text{by (77)}
\end{array}$$

That completes the proof of (76).

It remains to prove (75). We have

$$x \cdot y^+ \in SF \qquad \text{by Lemma 9.9}$$

That completes the proof of the lemma.

Lemma 9.22. *For all* $y \in \mathbb{F}$,

$$\forall x \in \mathbb{F}\, (x \cdot y \in SF \ \wedge\ \forall z\, (\langle x, y, z\rangle \in \mathbb{G} \leftrightarrow z = x \cdot y))$$

Proof. We will proceed by induction on y. That is legal since the formula is stratified, giving x, y, and z all index 0. $\mathbb{G}$ and $\mathbb{F}$ and SF are parameters.

Base case. When $y = 0$ we have to prove

$$x \cdot \mathsf{zero} \in SF$$
$$\langle x, \mathsf{zero}, z\rangle \in \mathbb{G} \leftrightarrow z = x \cdot \mathsf{zero}$$

We have $x \cdot \mathsf{zero} = \mathsf{zero}$ by Lemma 9.18. and $\mathsf{zero} \in SF$ by Lemma 9.3. Therefore it suffices to prove

$$\langle x, \mathsf{zero}, z\rangle \in \mathbb{G} \leftrightarrow z = \mathsf{zero}$$

The right-to-left implication follows from Lemma 9.8. It remains to prove the left-to-right implication. We have

$$\begin{array}{rl} \langle x, \mathsf{zero}, z\rangle \in \mathbb{G} & \text{assumption} \\ x \in SF & \text{by Lemma 9.9} \\ z = \mathsf{zero} \ \vee\ \exists u \in SF\, (u^+ = z) & \text{by Lemma 9.4} \end{array}$$

If $z = 0$ we are done, so we may assume $z = u^+$. Then

$$\begin{array}{rl} z \neq \mathsf{zero} & \text{by Lemma 4.16} \\ \exists p \in SF\, (p^+ = \mathsf{zero}) & \text{by Lemma 9.13} \end{array}$$

But that contradicts Lemma 4.16. That completes the base case.

The induction step has been proved in Lemma 9.21 That completes the proof of the theorem.

Theorem 9.23. *Assume* $x, y \in \mathbb{F}$ *and* $y^+ \in \mathbb{F}$. *Then* $x \cdot y^+ = x \cdot y + x$.

Remark. Note that we do not assume $x \cdot y^+ \in \mathbb{F}$. The equation is valid even if "overflow" occurs, i.e., if the product is "too big to fit in $\mathbb{F}$." In that case, both sides will be Λ, but the important point is that the equations are valid without assuming that we know whether overflow occurs or not.

Proof. Assume $x, y \in \mathbb{F}$ and $y^+ \in \mathbb{F}$. By Lemma 9.3, $x \in SF$. By Lemma 9.22,

$$x \cdot y \in SF \ \wedge\ \forall z\, (\langle x, y, z\rangle \in \mathbb{G} \leftrightarrow z = x \cdot y).$$

The theorem follows from that by Lemma 9.20. That completes the proof of the theorem.

10. Properties of multiplication

Lemma 10.1. *Multiplication satisfies the right distributive law: Assume* $x, y, z \in \mathbb{F}$*, and* $(y + z) \in \mathbb{F}$*. Then*

$$x \cdot (y + z) = x \cdot y + x \cdot z.$$

Remark. The values are in SF, and may or may not be in $\mathbb{F}$. If one side is in $\mathbb{F}$, the other is also; or put another way, if one side "overflows", so does the other. We call the reader's attention to the use of SF in the proof to accomplish this aim.

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

Base case: using Lemmas 8.2 and 9.18, we have

$$x \cdot (y + \mathsf{zero}) = x \cdot y = x \cdot y + \mathsf{zero} = x \cdot y + x \cdot \mathsf{zero}.$$

Induction step:

$$\begin{array}{rl}
\exists u\,(u \in z^+) & \text{by induction hypothesis} \\
z^+ \in \mathbb{F} & \text{by Lemma 4.19} \\
x \cdot z^+ = x \cdot z + x & \text{by Theorem 9.23} \\
y \in SF & \text{by Lemma 9.3} \\
z \in SF & \text{by Lemma 9.3} \\
y + z \in SF & \text{by Lemma 9.5} \\
y + z^+ \in \mathbb{F} & \text{by the induction hypothesis} \\
(y+z)^+ \in \mathbb{F} & \text{by Lemma 8.2} \\
(y+z)^+ \in \mathbb{F} & \text{by Lemma 9.15} \\
x \cdot (y + z^+) = x \cdot ((y+z)^+) & \text{by Lemma 8.2} \\
= x \cdot (y+z) + x & \text{by Theorem 9.23} \\
= (x \cdot y + x \cdot z) + x & \text{by the induction hypothesis} \\
= x \cdot y + (x \cdot z + x) & \text{by the associativity of addition} \\
= x \cdot y + x \cdot z^+ & \text{by Theorem 9.23}
\end{array}$$

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

Lemma 10.2. *Multiplication satisfies the left distributive law: Assume $x, y, z \in \mathbb{F}$, and $x + y \in \mathbb{F}$. Then*

$$(x + y) \cdot z = x \cdot z + y \cdot z.$$

Proof. By induction on z.

Base case: $(x + y) \cdot \mathsf{zero} = \mathsf{zero} = \mathsf{zero} + \mathsf{zero} = x \cdot \mathsf{zero} + y \cdot \mathsf{zero}$.

Induction step:

$$\begin{array}{rl}
(x+y) \cdot z^+ = (x+y) \cdot z + (x+y) & \text{by Theorem 9.23} \\
= (x \cdot z + y \cdot z) + (x+y) & \text{by the induction hypothesis} \\
= (x \cdot z + x) + (y \cdot z + y) & \text{by commutativity and associativity} \\
= x \cdot z^+ + y \cdot z^+ & \text{by Theorem 9.23}
\end{array}$$

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

Lemma 10.3. *Let $x \in \mathbb{F}$. Then $\mathsf{one} \cdot x = x$.*

Proof. By induction on x, which is legal as the formula is stratified.

Base case:

$$\begin{array}{rl}
\mathsf{one} \in SF & \text{by Lemma 9.3} \\
\mathsf{one} \cdot \mathsf{zero} = \mathsf{zero} & \text{by Lemma 9.18}
\end{array}$$

That completes the base case.

Induction step:

$$
\begin{aligned}
\mathsf{one} \cdot x^+ &= \mathsf{one} \cdot x + \mathsf{one} && \text{by Theorem 9.23} \\
&= x + \mathsf{one} && \text{by the induction hypothesis} \\
&= x + \mathsf{zero}^+ && \text{by definition of } \mathsf{one} \\
&= x^+ && \text{by Lemma 8.2}
\end{aligned}
$$

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

Lemma 10.4. *Multiplication is commutative: For $x, y \in \mathbb{F}$, $x \cdot y = y \cdot x$.*

Remark. It is not assumed that $x \cdot y$ and/or $y \cdot x$ are in $\mathbb{F}$. Therefore (as long as x and y are both in $\mathbb{F}$) the equation is valid. In particular if one side is in $\mathbb{F}$ so is the other side.

Proof. We proceed by induction on y, which is legal since the formula is stratified.

Base case: Assume $x \in \mathbb{F}$. We have to prove $x \cdot \mathsf{zero} = \mathsf{zero} \cdot x$. We have

$$
\begin{aligned}
x &\in SF && \text{by Lemma 9.3} \\
x \cdot \mathsf{zero} &= \mathsf{zero} && \text{by Lemma 9.18} \\
\mathsf{zero} \cdot x &= \mathsf{zero} && \text{by Lemma 9.19} \\
x \cdot \mathsf{zero} &= \mathsf{zero} \cdot x && \text{since both sides equal } \mathsf{zero}
\end{aligned}
$$

That completes the base case.

Induction step:

$$
\begin{aligned}
x \cdot y^+ &= x \cdot y + x && \text{by Theorem 9.23} \\
&= y \cdot x + x && \text{by the induction hypothesis} \\
&= y \cdot x + \mathsf{one} \cdot x && \text{by Lemma 10.3} \\
&= (y + \mathsf{one}) \cdot x && \text{by Lemma 10.2} \\
&= (y + \mathsf{zero}^+) \cdot x && \text{by definition of } \mathsf{one} \\
&= y^+ \cdot x && \text{by Lemma 8.2}
\end{aligned}
$$

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

Lemma 10.5. *Suppose $x \in SF$ and $u \in \mathbb{F}$ and $x + u \in \mathbb{F}$. Then $x \in \mathbb{F}$.*

Proof. By induction on u. The formula is stratified, so induction is legal.

Base case: $x + \mathsf{zero} = x$, by Lemma 8.2. Therefore the hypothesis $x + u \in \mathbb{F}$ becomes $x \in \mathbb{F}$. That completes the base case.

Induction step. Suppose u^+ is inhabited. Then

$$
\begin{aligned}
x + u^+ &\in \mathbb{F} && \text{by assumption} \\
x + u^+ &= (x + u)^+ && \text{by Lemma 8.2} \\
(x + u)^+ &\in \mathbb{F} && \text{by the previous two lines} \\
x &\in SF && \text{by hypothesis} \\
u &\in SF && \text{by Lemma 9.3} \\
(x + u) &\in SF && \text{by Lemma 9.5} \\
x + u &\in \mathbb{F} && \text{by Lemma 9.15} \\
x &\in \mathbb{F} && \text{by the induction hypothesis}
\end{aligned}
$$

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

Lemma 10.6. *Let $y \in \mathbb{F}$ and $z \in \mathbb{F}$ and $z^+ \in \mathbb{F}$. Suppose $y \cdot z^+ \in \mathbb{F}$. Then $y \cdot z \in \mathbb{F}$.*

Proof. Let $y \in \mathbb{F}$ and $z \in \mathbb{F}$. Suppose $y \cdot z^+ \in \mathbb{F}$. Then

$$\begin{array}{rl} y \in SF \ \wedge \ z \in SF & \text{by Lemma 9.3} \\ y \cdot z \in SF & \text{by Lemma 9.22} \\ y \cdot z^+ = y \cdot z + y & \text{by Theorem 9.23} \\ y \cdot z + y \in \mathbb{F} & \text{since } y \cdot z^+ \in \mathbb{F} \\ y \cdot z \in \mathbb{F} & \text{by Lemma 10.5} \end{array}$$

That completes the proof of the lemma.

Lemma 10.7. *Assume $x, y, z \in \mathbb{F}$, $x \cdot y \in \mathbb{F}$, and $y \cdot z \in \mathbb{F}$. Then $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.*

Proof. By induction on z.

Base case: We have $x \in SF$, $y \in SF$, and $x \cdot y \in SF$, by Lemma 9.3. Then

$$\begin{array}{rl} (x \cdot y) \cdot \mathsf{zero} = \mathsf{zero} & \text{by Lemma 9.18} \\ = x \cdot \mathsf{zero} = \mathsf{zero} & \text{by Lemma 9.18} \\ x \cdot (y \cdot \mathsf{zero}) & \text{by Lemma 9.18} \\ x \cdot (y \cdot \mathsf{zero}) = (x \cdot y) \cdot \mathsf{zero} & \text{by the previous three lines} \end{array}$$

That completes the base case.

Induction step: We have

$$\begin{array}{rl} \exists u \, (u \in z^+) & \text{by the induction hypothesis} \\ z^+ \in \mathbb{F} & \text{by Lemma 4.19} \\ y \cdot z^+ \in \mathbb{F} & \text{by the induction hypothesis} \\ y \cdot z \in \mathbb{F} & \text{by Lemma 10.6} \\ (x \cdot y) \cdot z^+ = (x \cdot y) \cdot z + x \cdot y & \text{by Theorem 9.23} \\ (x \cdot y) \cdot z^+ = x \cdot (y \cdot z) + x \cdot y & \text{by the induction hypothesis} \\ y \cdot z^+ = y \cdot z + y & \text{by Theorem 9.23} \\ (y \cdot z + y) \in \mathbb{F} & \text{since } y \cdot z^+ \in \mathbb{F} \\ (x \cdot y) \cdot z^+ = x \cdot (y \cdot z + y) & \text{by Lemma 10.1} \\ = x \cdot (y \cdot z^+) & \text{by Theorem 9.23} \end{array}$$

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

Lemma 10.8. *For $x \in \mathbb{F}$ we have $x \cdot \mathsf{one} = x$.*

Proof. We have

$$\begin{array}{rl} x \in \mathbb{F} & \text{by assumption} \\ x \in SF & \text{by Lemma 9.3} \\ \mathsf{one} \in \mathbb{F} & \text{by Lemma 4.20} \\ \mathsf{zero}^+ \in \mathbb{F} & \text{since } \mathsf{one} = \mathsf{zero}^+ \\ x \cdot \mathsf{zero}^+ = x \cdot \mathsf{zero} + x & \text{by Theorem 9.23} \\ x \cdot \mathsf{one} = x \cdot \mathsf{zero} + x & \text{since } \mathsf{one} = \mathsf{zero}^+ \\ = \mathsf{zero} + x & \text{since } x \cdot \mathsf{zero} = \mathsf{zero} \text{ by Lemma 9.18} \\ = x & \text{by Lemma 8.3} \end{array}$$

That completes the proof of the lemma.

Lemma 10.9. $\mathsf{two} = \mathsf{one} + \mathsf{one}$.

Proof. By definition $\mathsf{two} = \mathsf{one}^+$ and $\mathsf{one} = \mathsf{zero}^+$. Therefore it suffices to prove $\mathsf{zero}^{++} = \mathsf{zero}^+ + \mathsf{zero}^+$. By Lemma 8.2, that is equivalent to $\mathsf{zero}^{++} = \mathsf{zero}^{++} + \mathsf{zero}$; but that follows from Lemma 8.2. That completes the proof of the lemma.

Lemma 10.10. *For all $x \in \mathbb{F}$, we have $x + x = x \cdot \mathsf{two}$.*

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

$$\begin{aligned} x + x &= x \cdot \mathsf{one} + x \cdot \mathsf{one} && \text{by Lemma 10.8} \\ &= x \cdot (\mathsf{one} + \mathsf{one}) && \text{by Lemma 10.1} \\ &= x \cdot \mathsf{two} && \text{by Lemma 10.9} \end{aligned}$$

That completes the proof of the lemma.

Lemma 10.11. *Let $p, q \in \mathbb{F}$ and $p + q \in \mathbb{F}$. Then $p \le p + q$ and $q \le p + q$.*

Proof. Suppose $p, q \in \mathbb{F}$ and $p + q \in \mathbb{F}$. We have

$$\begin{aligned} u &\in q && \text{for some } u\text{, by Lemma 4.7} \\ \Lambda &\in \mathsf{zero} && \text{by the definition of zero} \\ \Lambda \subseteq u \ \wedge\ u &= \Lambda \cup (u - \Lambda) && \text{by the definitions of subset and difference} \\ \mathsf{zero} &\le q && \text{by the definition of } \le \\ p &\le p && \text{by Lemma 5.20} \\ p + \mathsf{zero} &\le p + q && \text{by Lemma 8.10} \\ p &\le p + q && \text{by Lemma 8.2} \end{aligned}$$

That is the first assertion of the lemma. By Lemma 8.3, we have $p + q = q + p$, so $q + p \in \mathbb{F}$ and as above we have $q \le q + p$. Therefore also $q \le p + q$. That completes the proof of the lemma.

Lemma 10.12. *Let $p, q \in \mathbb{F}$. Suppose $p + q \in \mathbb{F}$ and $2^{p+q} \in \mathbb{F}$. Then 2^p, 2^q, and $2^p \cdot 2^q$ are in $\mathbb{F}$, and*

$$2^{p+q} = 2^p \cdot 2^q.$$

Proof. By induction on q. That is legal since the formula of the lemma is stratified, giving p and q index 0.

Base case, $q = \mathsf{zero}$. Then

$$2^p + \mathsf{zero} = 2^p = 2^p \cdot 1 = 2^p \cdot 2^{\mathsf{zero}}.$$

That completes the base case.

Induction step. Suppose $p + q^+ \in \mathbb{F}$ and $2^{p+q^+} \in \mathbb{F}$, and as always in induction proofs, suppose q^+ is inhabited. Then

$$
\begin{array}{rl}
p + q \in \mathbb{F} & \text{by Lemma 8.9} \\
2^{p+q^+} = 2^{(p+q)^+} & \text{by Lemma 8.2} \\
2^{p+q^+} = 2^{p+q} + 2^{p+q} & \text{by Lemma 8.18} \\
p + q \le p + q^+ & \text{by Lemma 5.37} \\
\exists u\,(u \in 2^{p+q}) & \text{by Lemma 7.18} \\
2^{p+q} \in \mathbb{F} & \text{by Lemma 7.5}
\end{array}
$$

Now I say that $2^q \cdot \mathsf{two} \in \mathbb{F}$. Here is the proof:

$$
\begin{array}{rl}
2^{p+q} + 2^{p+q} = 2^{p+q} \cdot \mathsf{two} & \text{by Lemma 10.10} \\
2^{p+q^+} = 2^{p+q} \cdot \mathsf{two} & \text{since } 2^{p+q^+} = 2^{p+q} + 2^{p+q} \\
2^{p+q} \cdot \mathsf{two} \in \mathbb{F} & \text{since } 2^{p+q^+} \in \mathbb{F} \\
p \le p + q & \text{by Lemma 10.11} \\
2^q \le 2^{p+q} & \text{by Lemma 7.18, since } q \le p + q \\
2^q \in \mathbb{F} & \text{by Lemma 7.5} \\
2^q + 2^q \le 2^{p+q} + 2^{p+q} & \text{by Lemma 8.10} \\
2^q \cdot \mathsf{two} \le 2^{p+q} \cdot \mathsf{two} & \text{by Lemma 10.10} \\
\exists u\,(u \in 2^q \cdot \mathsf{two}) & \text{by the definition of } \le \\
\exists u\,(u \in 2^q + 2^q) & \text{since } 2^q + 2^q = 2^q \cdot \mathsf{two} \\
2^q + 2^q \in \mathbb{F} & \text{by Lemma 8.6} \\
2^q \cdot \mathsf{two} \in \mathbb{F} & \text{since } 2^q + 2^q = 2^q \cdot \mathsf{two}
\end{array}
$$

That completes the proof that $2^q \cdot \mathsf{two} \in \mathbb{F}$. Continuing, we have

$$
\begin{array}{rl}
2^{p+q^+} = (2^p \cdot 2^q) \cdot \mathsf{two} & \text{by the induction hypothesis} \\
2^p \in \mathbb{F} \ \wedge \ 2^q \in \mathbb{F} & \text{also by the induction hypothesis} \\
2^{p+q^+} = 2^p \cdot (2^q \cdot \mathsf{two}) & \text{by Lemma 10.7, since } 2^q \cdot \mathsf{two} \in \mathbb{F} \\
2^{p+q^+} = 2^p \cdot (2^q + 2^q) & \text{by Lemma 10.10} \\
= 2^p \cdot 2^{q^+} & \text{by Lemma 8.18}
\end{array}
$$

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

11. Results about $\mathbb{T}$

Here we constructivize Specker's §5.

Definition 11.1.

$$\mathbb{T}(\kappa) \quad = \quad \{u : \exists x\,(x \in \kappa \ \wedge \ u \sim USC(x))\}$$

The formula is stratified, giving x index 0, u and κ index 1. We will use $\mathbb{T}(\kappa)$ only when κ is a finite cardinal, although that is not required by the definition. Note that $\mathbb{T}(\kappa)$ has one type higher than κ. Thus we cannot define the graph of $\mathbb{T}$ or the graph of $\mathbb{T}$ restricted to $\mathbb{F}$.

Lemma 11.2. *If* $\kappa \in \mathbb{F}$, *then*

$$x \in \kappa \leftrightarrow USC(x) \in \mathbb{T}\kappa.$$

Proof. Left to right:

$$\begin{array}{rl} x \in \kappa & \text{by hypothesis} \\ USC(x) \sim USC(x) & \text{by Lemma 2.10} \\ USC(x) \in \mathbb{T}(\kappa) & \text{by Definition 11.1} \end{array}$$

That completes the left-to-right direction.

Right to left:

$$\begin{array}{rl} USC(x) \in \mathbb{T}\kappa & \text{by hypothesis} \\ \exists z\,(z \in \kappa \ \wedge\ USC(z) \sim USC(x)) & \text{by definition of } \mathbb{T} \\ z \sim x & \text{by Lemma 6.7} \\ x \in \kappa & \text{by Lemma 4.8} \end{array}$$

That completes the right-to-left direction. That completes the proof.

Lemma 11.3. *If* $\kappa \in \mathbb{F}$ *then for every* $x \in \kappa$, $\mathbb{T}(\kappa) = Nc(USC(x))$.

Proof. Suppose $\kappa \in \mathbb{F}$. Then κ is inhabited, by Corollary 4.7. Let $x \in \kappa$. Then

$$\begin{array}{rl} x \in \mathsf{FINITE} & \text{by Lemma 4.4} \\ USC(x) \in \mathsf{FINITE} & \text{by Lemma 3.10} \\ Nc(USC(x)) \in \mathbb{F} & \text{by Lemma 4.21} \\ USC(x) \in \mathbb{T}(\kappa) & \text{by Lemma 11.2} \\ USC(x) \sim USC(x) & \text{by Lemma 2.10} \\ USC(x) \in Nc(USC(x)) & \text{by Definition 4.10} \end{array}$$

We remark that we cannot finish the proof at this point by Lemma 5.7, because we do not yet know $\mathbb{T}(\kappa) \in \mathbb{F}$. Instead: by extensionality it suffices to prove

$$\forall u\,(u \in \mathbb{T}(\kappa) \leftrightarrow u \in Nc(USC(x))) \tag{78}$$

Left to right: Suppose $u \in \mathbb{T}(\kappa)$. By definition of $\mathbb{T}$, there exists $w \in \kappa$ with $u \sim USC(w)$. Then

$$\begin{array}{rl} w \sim x & \text{by Lemma 4.9, since } w \in \kappa \text{ and } x \in \kappa \\ USC(w) \sim USC(x) & \text{by Lemma 6.7} \\ u \sim USC(x) & \text{by Lemma 2.10 (transitivity of } \sim\text{), since } u \sim USC(w) \end{array}$$

That completes the proof of the right-to-left direction of (78).

Right to left: Suppose $u \in Nc(USC(x))$. Then $u \sim USC(x)$. Since $x \in \kappa$, we have $u \in \mathbb{T}(\kappa)$ by the definition of $\mathbb{T}$. That completes the proof of the lemma.

Lemma 11.4. *If* $\kappa \in \mathbb{F}$ *and* $x \in \kappa$ *then* $\kappa = Nc(x)$.

Proof. Let $\kappa \in \mathbb{F}$ and $x \in \kappa$. By extensionality, it suffices to prove that for all u,

$$u \in \kappa \leftrightarrow u \in Nc(x).$$

Left to right: Suppose $u \in \kappa$. Then

$$\begin{array}{rl} u \sim x & \text{by Lemma 4.9} \\ x \sim u & \text{by Lemma 2.10} \\ u \in Nc(x) & \text{by Definition 4.10} \end{array}$$

Right to left: Suppose $u \in Nc(x)$. Then

$$\begin{array}{rl} u \sim x & \text{by Definition 4.10} \\ u \in \kappa & \text{by Lemma 4.8} \end{array}$$

That completes the proof of the lemma.

Lemma 11.5. *If $Nc(x) \in \mathbb{F}$, then $\mathbb{T}(Nc(x)) = Nc(USC(x))$.*

Proof. By Lemma 11.3, with $\kappa = Nc(x)$.

Lemma 11.6. *If $m \in \mathbb{F}$ then $Tm \in \mathbb{F}$.*

Remark. Since the graph of $\mathbb{T}$ is not definable, we cannot express the lemma as $\mathbb{T} : \mathbb{F} \to \mathbb{F}$.

Proof. Let $m \in \mathbb{F}$. By Corollary 4.7, m is inhabited. Let $a \in m$. Then

$$\begin{array}{rl} USC(a) \in \mathbb{T}m & \text{by Lemma 11.2} \\ a \in \mathsf{FINITE} & \text{by Lemma 4.4} \\ USC(a) \in \mathsf{FINITE} & \text{by Lemma 3.10} \\ Nc(USC(a)) \in \mathbb{F} & \text{by Lemma 4.21} \\ \mathbb{T}m \in \mathbb{F} & \text{by Lemma 11.3} \end{array}$$

That completes the proof of the lemma.

Lemma 11.7. *Every singleton has cardinal* one*. That is,* $\forall x\, (Nc(\{x\}) = \mathsf{one})$.

Proof. By definition, $\mathsf{one} = \mathsf{zero}^+$ and $\mathsf{zero} = \{\Lambda\}$. Then the members of one are sets of the form $\Lambda \cup \{r\}$, by the definition of successor. But $\Lambda \cup \{r\} = \{r\}$. Hence the members of one are exactly the unit classes. Let x be given; then by definition of Nc, $Nc(\{x\})$ contains exactly the sets similar to $\{x\}$. By Lemma 6.3, that is exactly the unit classes. Hence Nc({x}) and one have the same members, namely all unit classes. By extensionality, $Nc(\{x\}) = \mathsf{one}$. That completes the proof.

Lemma 11.8. *For all $m \in \mathbb{F}$ with an inhabited successor, we have*

$$\mathbb{T}(m^+) = (\mathbb{T}m)^+.$$

Proof. Since m^+ is inhabited, there is an $x \in m$ and $a \notin x$ (so $x \cup \{a\} \in m^+$). Then

$$\begin{array}{rcll} m^+ \in \mathbb{F} & & & \text{by Lemma 4.19} \\ \mathbb{T}(m^+) & = & Nc(USC(x \cup \{a\})) & \text{by Lemma 11.3} \\ & = & Nc(USC(x) \cup \{\{a\}\}) & \text{by Lemma 6.15} \\ & = & (Nc(USC(x)))^+ & \text{by Lemma 4.13} \\ & = & (\mathbb{T}m)^+ & \text{by Lemma 11.3} \end{array}$$

That completes the proof of the lemma.

Lemma 11.9 (Specker 5.2)**.** $\mathbb{T}(\mathsf{zero}) = \mathsf{zero}$.

Proof. We have $USC(\Lambda) = \Lambda$ as there are no singleton subsets of Λ. Since $\mathsf{zero} = Nc(\Lambda)$, by Lemma 11.5 we have $\mathbb{T}(\mathsf{zero}) = Nc(USC(\Lambda)) = Nc(\Lambda) = \mathsf{zero}$. That completes the proof that $\mathbb{T}(\mathsf{zero}) = \mathsf{zero}$.

Lemma 11.10 (Specker 5.2)**.** $\mathbb{T}(\mathsf{one}) = \mathsf{one}$.

Proof.

$$
\begin{array}{rl}
\{\Lambda\} \in \mathsf{one} & \text{by definition of } \mathsf{one} \\
\mathbb{T}(\mathsf{one}) = Nc(USC(\{\Lambda\}) & \text{by Lemma 11.3} \\
\mathbb{T}(\mathsf{one}) = Nc(\{\{\Lambda\}\}) & \text{since } USC(\{\Lambda\}) = \{\{\Lambda\}\} \\
Nc(\{\{\Lambda\}\}) = \mathsf{one} & \text{by Lemma 11.7} \\
\mathbb{T}(\mathsf{one}) = \mathsf{one} & \text{by the two previous lines}
\end{array}
$$

That completes the proof of the lemma.

Lemma 11.11 (Specker 5.2)**.** $\mathbb{T}(\mathsf{two}) = \mathsf{two}$.

Proof. We have

$$
\begin{array}{rcll}
\mathbb{T}(\mathsf{two}) & = & \mathbb{T}(\mathsf{one}^+) & \text{since } \mathsf{two} = \mathsf{one}^+ \\
& = & (\mathbb{T}(\mathsf{one}))^+ & \text{by Lemma 11.8} \\
& = & \mathsf{one}^+ & \text{by Lemma 11.10} \\
& = & \mathsf{two}. &
\end{array}
$$

That completes the proof of the lemma.

Lemma 11.12 (Specker 5.5)**.** *Let* $m, n \in \mathbb{F}$. *Then*

$$n < m \to \mathbb{T}n < \mathbb{T}m.$$

Remarks. Specker 5.5 asserts that for cardinal numbers p and q we have $p \le q \leftrightarrow \mathbb{T}p \le \mathbb{T}q$. Specker does not prove a version of that lemma with strict inequality. We are able to do so, because we deal only with finite cardinals. (It might fail at limit cardinals.)

Proof. The formula in the lemma is stratified, with the relation $<$ occurring as a parameter. Therefore we can prove by induction that for $n \in \mathbb{F}$,

$$\forall m \in \mathbb{F}\,(n < m \to \mathbb{T}n < \mathbb{T}m).$$

Base case, $n = \mathsf{zero}$. Suppose $\mathsf{zero} < m$; we must show $\mathbb{T}\mathsf{zero} < \mathbb{T}m$. Since $\mathbb{T}\mathsf{zero} = \mathsf{zero}$, we have to show $\mathsf{zero} < \mathbb{T}m$. By Theorem 5.18, we have

$$\mathbb{T}m < \mathsf{zero} \ \vee \ \mathbb{T}m = \mathsf{zero} \ \vee \ \mathsf{zero} < \mathbb{T}m$$

and only one of the three disjuncts holds. Therefore it suffices to rule out the first two disjuncts, as the third is the desired conclusion. By Lemma 5.34, the first one is impossible. We turn to the second. Suppose $\mathbb{T}m = \mathsf{zero}$. Since $m \in \mathbb{F}$, by Lemma 4.7 we have $a \in m$ for some a. Then $USC(a) \in \mathbb{T}m$, by definition of $\mathbb{T}$. Since $\mathbb{T}m = \mathsf{zero}$, we have $USC(a) \in \mathsf{zero}$. Since $\mathsf{zero} = \{\Lambda\}$, we have $USC(a) = \Lambda$. Then $a = \Lambda$. Since $\Lambda \in \mathsf{zero}$, by Lemma 5.7 and the fact that $a \in m$, we have $m = \mathsf{zero}$. But that contradicts the assumption $\mathsf{zero} < m$, by Lemma 5.34. That completes the base case.

Induction step. Suppose $n^+ < m$ and n^+ is inhabited. We must show $\mathbb{T}(n^+) < \mathbb{T}m$. We have

$m \neq \mathsf{zero}$	since $n^+ < m$ and nothing is less than zero
$m = r^+$	for some $r \in \mathbb{F}$, by Lemma 4.17
$n^+ < r^+$	since $n^+ < m$ and $m = r^+$
$n < r$	by Lemma 5.15
$\mathbb{T}n < \mathbb{T}r$	by the induction hypothesis
$\exists a\,(a \in m)$	by Lemma 4.7
$\exists a\,(a \in r^+)$	since $m = r^+$
$(\mathbb{T}r)^+ = \mathbb{T}(r^+)$	by Lemma 11.8
$\exists u\,(u \in n^+)$	by the definition of $\leq$, since $n^+ < r^+$
$(\mathbb{T}n)^+ = \mathbb{T}(n^+)$	by Lemma 11.8, since n^+ is inhabited
$\mathbb{T}(r^+) \in \mathbb{F}$	by Lemma 11.6
$\mathbb{T}(n^+) \in \mathbb{F}$	by Lemma 11.6
$\exists u\,(u \in \mathbb{T}(r^+))$	by Lemma 4.7
$\exists u\,(u \in \mathbb{T}(n^+))$	by Lemma 4.7
$\exists u\, u \in (\mathbb{T}n)^+$	since $(\mathbb{T}n)^+ = \mathbb{T}(n^+)$
$\exists u\, u \in (\mathbb{T}r)^+$	since $(\mathbb{T}r)^+ = \mathbb{T}(r^+)$
$(\mathbb{T}n)^+ < (\mathbb{T}r)^+$	by Lemma 5.13
$\mathbb{T}(n^+) < \mathbb{T}(r^+)$	since $(\mathbb{T}n)^+ = \mathbb{T}(n^+)$ and $(\mathbb{T}r)^+ = \mathbb{T}(r^+)$
$\mathbb{T}(n^+) < \mathbb{T}m$	since $r^+ = m$

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

Lemma 11.13 (Specker 5.3)**.** *Let $m, n \in \mathbb{F}$ and suppose $n + m \in \mathbb{F}$. Then*

$$\mathbb{T}(n + m) = \mathbb{T}n + \mathbb{T}m.$$

Remark. This theorem can be proved directly from the definitions involved, but we need it only for finite cardinals, and it is simpler to prove it by induction.

Proof. By induction on m we prove

$$\forall n \in \mathbb{F}\,(n + m \in \mathbb{F} \to \mathbb{T}(n + m) = \mathbb{T}n + \mathbb{T}m). \tag{79}$$

The formula is stratified, since $\mathbb{T}$ raises indices by one.

Base case, $m = \mathsf{zero}$. We have to prove $\mathbb{T}(n + \mathsf{zero}) = \mathbb{T}n + \mathbb{T}(\mathsf{zero})$. Since $\mathbb{T}(\mathsf{zero}) = \mathsf{zero}$ by Lemma 11.9, and $n + \mathsf{zero} = n$ by Lemma 8.2, that reduces to $\mathbb{T}n = \mathbb{T}n$. That completes the base case.

Induction step. The induction hypothesis is (79). We suppose that m^+ is inhabited and that $n + m^+ \in \mathbb{F}$. We must prove $\mathbb{T}(n + m^+) = \mathbb{T}n + \mathbb{T}(m^+)$. In order to apply the induction hypothesis, we need $n + m \in \mathbb{F}$. Since $n + m^+ \in \mathbb{F}$, it is inhabited, by Corollary 4.7. By Lemma 8.2, $(n + m)^+$ is inhabited. Hence it has a member, which must be of the form $x \cup \{a\}$ where $x \in n + m$. Thus $n + m$ is inhabited. Then by Lemma 8.6, $n + m \in \mathbb{F}$. Therefore, by the induction hypothesis (79), we have

$$\mathbb{T}(n + m) = \mathbb{T}n + \mathbb{T}m.$$

Taking the successor of both sides, we have

$$\begin{array}{rcll}
(\mathbb{T}(n+m))^+ & = & (\mathbb{T}n + \mathbb{T}m)^+ & \\
\mathbb{T}((n+m)^+) & = & (\mathbb{T}n + \mathbb{T}m)^+ & \text{by Lemma 11.8} \\
\mathbb{T}(n+m^+) & = & (\mathbb{T}n + \mathbb{T}m)^+ & \text{by Lemma 8.2} \\
 & = & \mathbb{T}n + (\mathbb{T}m)^+ & \text{by Lemma 8.2} \\
 & = & \mathbb{T}n + \mathbb{T}(m^+) & \text{by Lemma 11.8}
\end{array}$$

That is the desired goal. That completes the induction step. That completes the proof of the lemma.

Lemma 11.14 (Specker 5.8)**.** *For $m \in \mathbb{F}$, $2^{\mathbb{T}m}$ is inhabited.*

Proof. Let $m \in \mathbb{F}$. Then

$$\begin{array}{rl}
u \in m & \text{for some } u\text{, by Lemma 4.7} \\
USC(u) \in \mathbb{T}m & \text{by Definition 11.1} \\
SSC(u) \in 2^{\mathbb{T}m} & \text{by the definition of exponentiation}
\end{array}$$

That completes the proof of the lemma.

Lemma 11.15. *For $m \in \mathbb{F}$, $2^{\mathbb{T}m} \in \mathbb{F}$.*

Proof. Suppose $m \in \mathbb{F}$. Then $\exists x\,(x \in 2^{\mathbb{T}m})$, by Lemma 11.14. Then by the definition of exponentiation, for some u we have

$$SSC(u) \in 2^{\mathbb{T}m} \ \wedge\ USC(u) \in \mathbb{T}m.$$

Then

$$\begin{array}{rl}
\mathbb{T}m \in \mathbb{F} & \text{by Lemma 11.6} \\
USC(u) \in \mathsf{FINITE} & \text{by Lemma 4.4} \\
u \in \mathsf{FINITE} & \text{by Lemma 3.10} \\
USC(u) \in \mathbb{T}m & \text{by definition of } \mathbb{T} \\
SSC(u) \in \mathsf{FINITE} & \text{by Lemma 3.17} \\
SSC(u) \in 2^{\mathbb{T}m} & \text{by Lemma 8.12} \\
2^{\mathbb{T}m} \in \mathbb{F} & \text{by Lemma 7.5}
\end{array}$$

That completes the proof of the lemma.

Lemma 11.16. *Suppose $m \in \mathbb{F}$. Then $(\mathbb{T}m)^+ \in \mathbb{F}$.*

Proof. Suppose $m \in \mathbb{F}$. Then

$$\begin{array}{rl}
2^{\mathbb{T}m} \in \mathbb{F} & \text{by Lemma 11.15} \\
\mathbb{T}m \in \mathbb{F} & \text{by Lemma 11.6} \\
\exists u\,(u \in 2^{\mathbb{T}m}) & \text{by Lemma 4.7} \\
\mathbb{T}m < 2^{\mathbb{T}m} & \text{by Lemma 7.16} \\
(\mathbb{T}m)^+ \in \mathbb{F} & \text{by Lemma 5.31}
\end{array}$$

That completes the proof of the lemma.

Lemma 11.17 (Specker 5.9)**.** *For $m \in \mathbb{F}$, if 2^m is inhabited, then $2^{\mathbb{T}m} = \mathbb{T}(2^m)$.*

Proof. Suppose 2^m is inhabited. Then there exists a with $USC(a) \in m$. Then

$2^m = Nc(SSC(a))$	by Lemma 7.2
$SSC(a) \in 2^m$	by Lemma 8.12
$USC(SSC(a)) \in \mathbb{T}(2^m)$	by Lemma 11.2
$USC(USC(a)) \in \mathbb{T}m$	by Lemma 11.2
$Tm \in \mathbb{F}$	by Lemma 11.6
$SSC(USC(a)) \in 2^{Tm}$	by Lemma 8.12
$2^m \in \mathbb{F}$	by Lemma 7.5
$2^{Tm} \in \mathbb{F}$	by Lemma 7.5
$Nc(SSC(USC(a))) = Nc(USC(SSC(a)))$	by Lemma 6.2
$2^{Tm} = Nc(SSC(USC(a)))$	by Lemma 11.4
$\mathbb{T}(2^m) = Nc(USC(SSCa))$	by Lemma 11.3
$2^{Tm} = \mathbb{T}(2^m)$	from the last three equations

That completes the proof of the lemma.

Lemma 11.18. *For $n, m \in \mathbb{F}$, we have*

$$\mathbb{T}n = \mathbb{T}m \to n = m$$

Proof. Suppose $\mathbb{T}n = \mathbb{T}m$. By Lemma 4.7, we can find $a \in n$ and $b \in m$. Then

$USC(a) \in \mathbb{T}n$	by definition of $\mathbb{T}$
$USC(b) \in \mathbb{T}m$	by definition of $\mathbb{T}$
$\mathbb{T}n = \mathbb{T}m$	by hypothesis
$USC(a) \in \mathbb{T}n$	by the previous two lines
$\mathbb{T}m \in \mathbb{F}$	by Lemma 11.6
$USC(a) \sim USC(b)$	by Lemma 4.9
$a \sim b$	by Lemma 6.7
$b \in n$	by Lemma 4.8
$n = m$	by Lemma 5.7

That completes the proof of the lemma.

Lemma 11.19 (Converse to Specker 5.3)**.** *Let $a, b, c \in \mathbb{F}$. Then*

$$\mathbb{T}a + \mathbb{T}b \in \mathbb{F} \to \mathbb{T}a + \mathbb{T}b = \mathbb{T}c \to a + b = c.$$

Remark. It is not assumed that $a + b \in \mathbb{F}$. Indeed, that follows from the stated conclusion.

Proof. The formula is stratified, giving a, b, and c all index zero. Therefore we may proceed by induction on b.

Base case: We have

$$\begin{aligned}
\mathbb{T}a + \mathbb{T}\mathsf{zero} &= \mathbb{T}c && \text{by assumption}\\
\mathbb{T}a + \mathsf{zero} &= \mathbb{T}c && \text{by Lemma 11.9}\\
\mathbb{T}a &= \mathbb{T}c && \text{by Lemma 8.2}\\
a &= c && \text{by Lemma 11.18}\\
a + \mathsf{zero} &= c && \text{by Lemma 8.2}
\end{aligned}$$

That completes the base case.

Induction step: We have

$$\begin{aligned}
\mathbb{T}a + \mathbb{T}(b^+) &= \mathbb{T}c && \text{by assumption}\\
\exists u\,(u &\in b^+) && \text{by assumption}\\
b^+ &\in \mathbb{F} && \text{by Lemma 4.19}\\
\mathbb{T}(b^+) &= (\mathbb{T}b)^+ && \text{by Lemma 11.8}\\
\mathbb{T}a + (\mathbb{T}b)^+ &= \mathbb{T}c && \text{by the preceding lines}\\
(\mathbb{T}a + \mathbb{T}b)^+ &= \mathbb{T}c && \text{by Lemma 8.2}\\
c &\neq \mathsf{zero} && \text{by Lemmas 11.9 and 4.16}\\
c &= r^+ && \text{for some } r\text{, by Lemma 4.17}\\
(\mathbb{T}a + \mathbb{T}b)^+ &= \mathbb{T}(r^+) && \text{by the preceding two lines}\\
(\mathbb{T}a + \mathbb{T}b)^+ &= (\mathbb{T}r)^+ && \text{by Lemma 11.8}\\
\mathbb{T}a + \mathbb{T}(b^+) &\in \mathbb{F} && \text{by assumption}\\
(\mathbb{T}a + \mathbb{T}b)^+ &\in \mathbb{F} && \text{by Lemmas 11.8 and 8.2}\\
\exists u\,(u &\in (\mathbb{T}a + \mathbb{T}b)^+) && \text{by Lemma 4.7}\\
\exists u\,(u &\in (\mathbb{T}a + \mathbb{T}b)) && \text{by definition of successor}\\
\exists u\,(u &\in (\mathbb{T}r)^+) && \text{by Lemma 4.7}\\
\mathbb{T}r &\in \mathbb{F} && \text{by Lemma 11.6}\\
\mathbb{T}a &\in \mathbb{F} && \text{by Lemma 11.6}\\
\mathbb{T}b &\in \mathbb{F} && \text{by Lemma 11.6}\\
\mathbb{T}a + \mathbb{T}b &\in \mathbb{F} && \text{by Lemma 8.6}\\
\mathbb{T}a + \mathbb{T}b &= \mathbb{T}r && \text{by Lemma 5.12}\\
a + b &= r && \text{by the induction hypothesis}\\
(a + b)^+ &= r^+ && \text{by the preceding line}\\
a + b^+ &= r^+ && \text{by Lemma 8.2}\\
a + b^+ &= c && \text{since } r^+ = c
\end{aligned}$$

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

Lemma 11.20. *For $n, m \in \mathbb{F}$, we have*

$$n < m \leftrightarrow \mathbb{T}n < \mathbb{T}m.$$

Proof. Left to right is Lemma 11.12.

Right to left. Suppose $\mathbb{T}n < \mathbb{T}m$. By Theorem 5.18, we have $n < m$ or $n = n$ or $m < n$. We argue by cases.

Case 1, $n < m$. Then we are done, since that is the desired conclusion.

Case 2, $n = m$ then $\mathbb{T}n = \mathbb{T}m$. By Lemma 11.6, $\mathbb{T}n \in \mathbb{F}$ and $\mathbb{T}m \in \mathbb{F}$, so by Theorem 5.18, $\mathbb{T}n = \mathbb{T}m$ contradicts $\mathbb{T}n < \mathbb{T}m$. That completes Case 2.

Case 3, $m < n$. Then $\mathbb{T}m < \mathbb{T}n$ by Lemma 11.12. That completes the proof of the lemma.

Lemma 11.21. *Suppose $p, q \in \mathbb{F}$ and $p < \mathbb{T}q$. Then there exists $r \in \mathbb{F}$ such that $p = \mathbb{T}r$.*

Proof. By induction on p we will prove

$$\forall q \in \mathbb{F}\,(p < \mathbb{T}q \to \exists r \in \mathbb{F}\,(p = \mathbb{T}r)) \tag{80}$$

The formula is stratified, giving q and r index 0 and p index 1, so induction is legal.

Base case, $p = 0$. Then $r = \mathsf{zero}$ satisfies $p = \mathbb{T}r$, by Lemma 11.9. That completes the base case.

Induction step. The induction hypothesis is (80). Suppose $p^+ < \mathbb{T}q$ and p^+ is inhabited. Then

$$\begin{array}{ll} p < p^+ & \text{by Lemma 5.26} \\ p < \mathbb{T}q & \text{by Lemma 5.25} \\ p = \mathbb{T}r & \text{for some } r\text{, by (80)} \end{array}$$

Now I say that r^+ is inhabited. To prove that:

$$\begin{array}{rl} \mathbb{T}r = p < p^+ < \mathbb{T}q & \text{as already proved} \\ \mathbb{T}r < \mathbb{T}q & \text{from the previous line} \\ r < q & \text{by Lemma 11.20} \\ r^+ \le q & \text{by Lemma 5.30} \\ \exists u\,(u \in r^+) & \text{by the definition of } \le \end{array}$$

That completes the proof that r^+ is inhabited. Then since $p = \mathbb{T}r$, we have

$$p^+ = (\mathbb{T}r)^+ = \mathbb{T}(r^+) \qquad \text{by Lemma 11.8}$$

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

Lemma 11.22. *Suppose $p \in \mathbb{F}$ and 2^p is inhabited. Then $p = \mathbb{T}\,q$ for some $q \in \mathbb{F}$.*

Proof. Suppose $p \in \mathbb{F}$ and 2^p is inhabited. Then by definition of exponentiation, for some a we have $USC(a) \in p$ and $SSC(a) \in 2^p$. By definition of $\mathbb{T}$ we have $p = \mathbb{T}(Nc(a))$. By Lemma 4.21, we have $Nc(a) \in \mathbb{F}$. That completes the proof of the lemma.

Lemma 11.23. *Let $e \in \mathbb{F}$ and $e + e \in \mathbb{F}$. Then $e^+ \in \mathbb{F}$.*

Proof. By Theorem 5.19, $e = \mathsf{zero} \ \vee \ e \neq \mathsf{zero}$. If $e = \mathsf{zero}$ then $e^+ = \mathsf{one}$, so we are done by Lemma 4.20. Therefore we may assume $e \neq \mathsf{zero}$. We have

$$\begin{array}{rl} e \le e + e & \text{by Lemma 10.11} \\ e < e + e \ \vee \ e = e + e & \text{by Lemma 5.21} \end{array}$$

We argue by cases.

Case 1, $e < e + e$. Then

$$\begin{array}{rl} e^+ \leq e + e & \text{by Lemma 5.30} \\ \exists u\,(u \in e^+) & \text{by the definition of } \leq \\ e^+ \in \mathbb{F} & \text{by Lemma 4.19} \end{array}$$

That completes Case 1.

Case 2, $e = e + e$. It seems that it should be easy to prove $e = \mathsf{zero}$, but we did not find an easy proof. So we prove it another way:

$$\begin{array}{rl} e = t^+ & \text{by Lemma 4.17, since } e \neq \mathsf{zero} \\ e + e = (t+t)^{++} & \text{by Lemma 8.2} \\ (t+t)^{++} \in \mathbb{F} & \text{since } e + e \in \mathbb{F} \\ e \in SF & \text{by Lemma 9.3} \\ e^+ \in SF & \text{by Lemma 9.2} \\ e^+ + t \in \mathbb{F} & \text{by Lemma 8.2} \\ e^+ \in \mathbb{F} & \text{by Lemma 10.5} \end{array}$$

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

Lemma 11.24. *If $\mathbb{T}c$ is even, then c is even. More precisely, if $c, a \in \mathbb{F}$ and $\mathbb{T}c = a + a$ and $a + a \in \mathbb{F}$, then there exists $b \in \mathbb{F}$ with $c = b + b$.*

Proof. The formula is stratified, giving b and c index 0 and a index 1. $\mathbb{F}$ is just a parameter, so it does not need an index. Therefore we can proceed by induction on a.

Base case: Suppose $\mathbb{T}c = \mathsf{zero} + \mathsf{zero}$ and $c \in \mathbb{F}$. We have

$$\begin{array}{rl} \mathbb{T}c \in \mathbb{F} & \text{by Lemma 11.6} \\ \mathbb{T}c \in SF & \text{by Lemma 9.3} \\ a \in SF & \text{by Lemma 9.3} \\ a = \mathsf{zero} & \text{by Lemma 9.11} \\ \mathbb{T}c = \mathsf{zero} & \text{since } \mathbb{T}c = a + a = \mathsf{zero} + \mathsf{zero} = \mathsf{zero} \\ \mathbb{T}\,\mathsf{zero} = \mathsf{zero} & \text{by Lemma 11.9} \\ c = \mathsf{zero} & \text{by Lemma 11.18} \\ \exists b\,(c = b + b) & \text{namely, } b = \mathsf{zero} \end{array}$$

Induction step: Suppose a^+ is inhabited and $\mathbb{T}c = a^+ + a^+$, and $a^+ + a^+ \in \mathbb{F}$. Then

$$\begin{array}{rl}
\mathbb{T}\,c = (a+a)^{++} & \text{by Lemma 8.2} \\
a \in SF & \text{by Lemma 9.3} \\
a + a \in SF & \text{by Lemma 9.5} \\
(a+a)^+ \in \mathbb{F} & \text{by Lemma 9.15} \\
(a+a) \in \mathbb{F} & \text{by Lemma 9.15} \\
\mathbb{T}\,c \neq \mathsf{zero} & \text{by Lemma 4.16} \\
\mathsf{one} \neq (a+a)^{++} & \text{by Lemma 5.12} \\
\mathbb{T}\,c \neq \mathsf{one} & \text{since } T\,c = (a+a)^{++} \\
c \neq \mathsf{zero} & \text{by Lemma 11.9} \\
c = r^+ & \text{for some } r \in \mathbb{F}\text{, by Lemma 4.17} \\
r \neq \mathsf{zero} & \text{since if } r = \mathsf{zero} \text{ then } r^+ = c = \mathsf{one}\text{, so } \mathbb{T}\,c = \mathsf{one} \\
r = t^+ & \text{for some } t \in \mathbb{F}\text{, by Lemma 4.17} \\
c = t^{++} & \text{by the preceding lines} \\
\mathbb{T}\,c = (\mathbb{T}\,t)^{++} & \text{by Lemma 11.8} \\
(a+a)^{++} = (\mathbb{T}\,t)^{++} & \text{since } \mathbb{T}c = (a+a)^{++} \\
\mathbb{T}\,t \in \mathbb{F} & \text{by Lemma 11.6} \\
\mathbb{T}\,t = a + a & \text{by Lemma 5.12} \\
t = e + e & \text{for some } e \in \mathbb{F}\text{, by the induction hypothesis} \\
t^{++} = (e^+ + e^+) & \text{by Lemma 8.2} \\
c = b + b & \text{with } b = e^+\text{, by the preceding lines} \\
e^+ \in \mathbb{F} & \text{by Lemma 11.23, since } e + e = t \in \mathbb{F}
\end{array}$$

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

Lemma 11.25. *For all p, q, if $p + q = \mathsf{zero}$ then $p = \mathsf{zero}$.*

Remark. No additional hypothesis is needed.

Proof. By definition, $\mathsf{zero} = \{\Lambda\}$. By the definition of addition, there exist a and b with $a \in p$ and $b \in q$ and $a \cap b = \Lambda$, such that $a \cup b \in \mathsf{zero}$. Then $a \cup b = \Lambda$. It follows that $a = \Lambda$ and $b = \Lambda$. On the other hand, if a or b had a non-empty member, then by the definition of addition, $a+b$ would have a non-empty member, so zero would have a non-empty member. Therefore $p = q = \{\Lambda\} = \mathsf{zero}$. That completes the proof of the lemma.

Lemma 11.26. *For $x, y \in \mathbb{F}$,*

$$x + x = y + y \to x = y.$$

Proof. The formula is stratified; we prove it by induction on x, in the form

$$\forall y \in F\,(x + x = y + y \to x = y).$$

Base case: Suppose $\mathsf{zero} + \mathsf{zero} = y + y$. Then $\mathsf{zero} = y + y$. By Lemma 11.25, $y = \mathsf{zero}$. That completes the base case.

Induction step: Suppose $x^+ + x^+ = y + y$, and suppose (as always in induction proofs) that x^+ is inhabited. Then

$$\begin{array}{rl} x^+ + x^+ = (x+x)^{++} & \text{by Lemma 8.2} \\ y \neq \mathsf{zero} & \text{by Lemma 4.16} \\ y = r^+ & \text{for some } r\text{, by Lemma 4.17} \\ (x+x)^{++} = (r+r)^{++} & \text{by Lemma 8.2} \\ x+x = r+r & \text{by Lemma 5.12} \\ x = r & \text{by the induction hypothesis} \\ x^+ = r^+ & \text{by the preceding line} \\ x^+ = y & \text{since } y = r^+ \end{array}$$

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

Lemma 11.27. *Let $p \in \mathbb{F}$. Then*

$$2^p \in \mathbb{F} \leftrightarrow \exists q \in \mathbb{F}\,(p = \mathbb{T}q).$$

Proof. Suppose $p \in \mathbb{F}$. Left to right:

$$\begin{array}{rl} 2^p \in \mathbb{F} & \text{assumption} \\ \exists u\,(u \in 2^p) & \text{by Lemma 4.7} \\ USC(a) \in p & \text{for some } a\text{, by the definition of exponentiation} \\ USC(a) \in \mathsf{FINITE} & \text{by Lemma 4.4} \\ a \in \mathsf{FINITE} & \text{by Lemma 3.10} \\ Nc(a) \in \mathbb{F} & \text{by Lemma 4.21} \\ a \in Nc(a) & \text{by Lemma 4.11} \\ USC(a) \in \mathbb{T}(Nc(a)) & \text{by definition of } \mathbb{T} \\ \mathbb{T}(Nc(a)) \in \mathbb{F} & \text{by Lemma 11.6} \\ USC(a) \in p \cap \mathbb{T}(Nc(a)) & \text{by definition of intersection} \\ p = \mathbb{T}(Nc(a)) & \text{by Lemma 5.7} \\ \exists q \in \mathbb{F}\,(p = \mathbb{T}a) & \text{namely } q = Nc(a) \end{array}$$

That completes the proof of the left-to-right direction.

Right to left: Suppose $p = \mathbb{T}q$ and $q \in \mathbb{F}$. Then

$$\begin{array}{rl} u \in q & \text{for some } u\text{, by Lemma 4.7} \\ USC(u) \in \mathbb{T}q & \text{by definition of } \mathbb{T} \\ \mathbb{T}q \in \mathbb{F} & \text{by Lemma 11.6} \\ SSC(u) \in 2^{\mathbb{T}q} & \text{by definition of exponentiation} \\ SSC(u) \in 2^p & \text{since } p = \mathbb{T}q \\ 2^p \in \mathbb{F} & \text{by Lemma 7.5} \end{array}$$

That completes the proof of the right-to-left direction. That completes the proof of the lemma.

12. Cartesian products

The Cartesian product of two sets is defined as usual; the definition is stratified, so it can be given in INF. But because ordered pairs raise the types by two, the cardinality of $A \times B$ is not the product of the cardinalities of A and B, but instead it is the product of $\mathbb{T}^2$ of those cardinalities. In this section we provide a proof of this fact, in the interest of setting down the fundamental facts about the theory of finite sets.

Lemma 12.1. *Let A have decidable equality. Suppose Y is a finite subset of A, and $a \in A$. Then $\{a\} \times Y$ is finite. If $\kappa = Nc(Y)$ then $\mathbb{T}^2\kappa = Nc(\{a\} \times Y)$.*

Proof. Consider the map $f : USC^2(Y) \to \{a\} \times Y$ defined by

$$f = \{\langle\{\{y\}\}, \langle a, y\rangle\rangle : y \in Y\}.$$

The formula is stratified, giving y and a index 0, so $\langle a, y\rangle$ gets index 2, as does $\{\{y\}\}$. Y gets index 1. Since the formula is stratified, f can be defined in INF. I say that f is a similarity from $USC^2(Y)$ to Y. We omit the straightforward verification of that fact.

Then we have

$USC^2(Y) \sim \{a\} \times Y$	since f is a similarity
$USC(Y) \in \mathsf{FINITE}$	by Lemma 3.10
$USC^2(Y) \in \mathsf{FINITE}$	by Lemma 3.10
$Y \in \mathsf{FINITE}$	by Lemma 4.23
$Nc(USC^2(Y) = \mathbb{T}^2\kappa$	by definition of $\mathbb{T}$
$Nc(Y) = \mathbb{T}^2\kappa$	by Lemma 4.8

That completes the proof of the lemma.

Lemma 12.2. *Let A be a set with decidable equality. Let X and Y be finite subsets of A. Then $X \times Y$ is finite. Moreover, if $\kappa = Nc(X)$ and $\mu = Nc(Y)$, then*

$$\mathbb{T}^2(\kappa) \cdot \mathbb{T}^2(\mu) = Nc(X \times Y).$$

Remarks. Without $\mathbb{T}^2$, the formula is not stratified. It is not necessary to *assume* that $(\mathbb{T}^2\kappa) \cdot \mathbb{T}^2(\mu) \in \mathbb{F}$. That will, of course, be a consequence, by Lemma 4.21.

Proof. Let A have decidable equality, and let Y be a finite subset of A. The formula to be proved is

$$X \subseteq A \to X \in \mathsf{FINITE} \to (X \times Y \in \mathsf{FINITE} \wedge \mathbb{T}^2(Nc(X)) \cdot \mathbb{T}^2(Nc(Y)) = Nc(X \times Y))\}.$$

That formula (and the hypotheses listed before it) are stratified, giving X and Y index 1, A index 2; then $X \times Y$ gets index 3, $Nc(X \times Y)$ gets index 4, $\kappa = Nc(X)$ gets index 2, and $\mathbb{T}^2(\kappa)$ gets index 4; since multiplication is a function, the whole left-hand side gets index 4. FINITE is just parameter. Therefore we may proceed by induction on finite sets X.

Base case: $X = \Lambda$. We have $\Lambda \times Y = \Lambda$, which is finite. It has cardinality zero. Since $\mathbb{T}\,\mathsf{zero} = \mathsf{zero}$ by Lemma 11.9, we have

$$(T^2\,\mathsf{zero}) \cdot (\mathbb{T}^2\mu) = \mathsf{zero} \cdot (\mathbb{T}^2\mu) = \mathsf{zero}$$

by Lemma 9.19. That completes the base case.

Induction step. Suppose $a \notin X$. Let $\mu = Nc(Y)$ and $\kappa = Nc(X)$. Then $Nc(X \cup \{c\}) = \kappa^+$, by definition of successor. Assume $X \cup \{a\} \subseteq A$; that is, $a \in X$. We have to show $(X \cup \{a\}) \times Y$ is finite and has cardinality $\mathbb{T}^2(\kappa^+) \cdot \mathbb{T}^2\mu$. We have

$$(X \cup \{a\}) \times Y \quad = \quad (X \times Y) \cup (\{a\} \times Y) \tag{81}$$

(as can be verified using the definitions of product and union). Now $X \times Y \in \mathsf{FINITE}$ since $X \in Z$ and $X \subseteq A$, and $\{a\} \times Y$ is finite, as shown above. The two sets on the right of (81) are finite, and both are subsets of $A \times A$, which has decidable equality since A has decidable equality. Therefore Lemma 3.11 is applicable, and we conclude that the union of the two sets on the right of (81), which is $X \times Y$, is finite. We have now proved

$$(X \cup \{a\}) \times Y \in \mathsf{FINITE}.$$

It remains to show that its cardinality is $\mathbb{T}^2(\kappa^+) \cdot \mathbb{T}^2\mu$. We have

$$\begin{array}{rll}
\kappa^+ = Nc(X \cup \{a\}) & & \text{by definition of successor} \\
\kappa^+ \in \mathbb{F} & & \text{by Lemma 4.21} \\
Nc((X \cup \{a\}) \times Y) = Nc((X \times Y) \cup (\{a\} \times Y)) & & \text{by (81)} \\
= Nc(X \times Y) + Nc(\{a\} \times Y) & & \text{by the definition of addition} \\
= \mathbb{T}^2(\kappa) \cdot \mathbb{T}^2\mu + Nc(\{a\} \times Y) & & \text{by the induction hypothesis} \\
= \mathbb{T}^2(\kappa) \cdot \mathbb{T}^2\mu + \mathbb{T}^2\mu & & \text{by Lemma 12.1} \\
= \mathbb{T}^2(\kappa) \cdot \mathbb{T}^2\mu + \mathsf{one} \cdot \mathbb{T}^2\mu & & \text{by Lemma 10.3} \\
\mathbb{T}^2\kappa + \mathsf{one} = \mathbb{T}^2(\kappa^+) \in \mathbb{F} & & \text{since } \kappa^+ \in \mathbb{F} \\
Nc((X \cup \{a\}) \times Y) = (\mathbb{T}^2(\kappa) + \mathsf{one}) \cdot \mu & & \text{by Lemma 10.2,}
\end{array}$$

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

13. Onto and one-to-one for maps between finite sets

In this section, we prove the well-known theorems that for maps f from a finite set X to itself, f is one-to-one if it is onto, and vice-versa. These theorems are somewhat more difficult to prove constructively than classically, but they are provable.

In treating this subject rigorously one has to distinguish the relevant concepts precisely. Namely, we have

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

$Rel(f)$ 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.

Definition 13.1. *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.*

In this section we will prove that either one of the conditions "one-to-one" and "onto" implies the other, if all the other conditions are assumed.

Remark. We do not need to specify $range(f) \subseteq X$, because that follows from $dom(f) \subseteq X$ and $f : X \to X$. The reader can check that none of the conditions in the definition are superfluous.

Lemma 13.2. *Let $X \in \mathsf{FINITE}$ and $f : X \to X$. Suppose $dom(f) = X$ and $Rel(f)$. Then $f \in \mathsf{FINITE}$.*

Proof. Since X is finite, X has decidable equality, by Lemma 3.3. I say that

$$x \in X \to y \in X \to \langle x, y\rangle \in f \ \vee \ \langle x, y\rangle \notin f. \tag{82}$$

To prove (82), let $x \in X$ and $y \in X$. Since $f : X \to X$, there exists $z \in X$ with $\langle x, z\rangle \in f$, and $\langle x, y\rangle \in f \leftrightarrow y = z$. Since X has decidable equality, we have $y = z \ \vee \ y \neq z$. But that implies (82). That is, f is a separable subset of $X \times X$. By Lemma 3.19, $f \in \mathsf{FINITE}$. That completes the proof of the lemma.

Lemma 13.3 (Decidable pre-image)**.** *Let X be a finite set and $f : X \to X$, with $dom(f) = X$ and $Rel(f)$. Then for $y \in X$,*

$$\exists x \in X\,(\langle x, y\rangle \in f) \ \vee \ \neg\exists x \in X\,(\langle x, y\rangle \in f).$$

Proof. Let $y \in X$. Define

$$Z := \{x \in X : \exists y \in X\,(\langle x, y\rangle \in f)\}.$$

The formula is stratified, giving x and y index 0, f index 3, and X index 1. Therefore the definition is legal. Then

$f \subseteq X \times X$	since $dom(f) = X$
$f \in \mathsf{FINITE}$	by Lemma 13.2
$X \in \mathsf{DECIDABLE}$	by Lemma 3.3
$X \times X \in \mathsf{FINITE}$	by Lemma 12.2
f is a separable relation on X	by Lemma 3.18
$Z \in \mathsf{FINITE}$	by Lemma 3.21
$Z = \Lambda \ \vee \ \exists x\,(x \in Z)$	by Lemma 3.4

Putting in the definition of Z, we have the formula in the conclusion of the lemma. That completes the proof of the lemma.

Theorem 13.4. *Let X be a finite set, and let $f : X \to X$ be a one-to-one function. Then f is onto.*

Proof. By induction on finite sets, we prove that if $f : X \to X$ is one-to-one, then f is onto. By Lemma 3.3, X has decidable equality.

Base case: The only function defined on the empty set is the empty function, which is both one-to-one and onto.

Induction step: Let $X = B \cup \{a\}$, where $a \notin B$, and B is finite. Suppose $f : X \to X$ is one-to-one. We have to prove

$$\forall y \in X \, \exists x \in X \, (\langle x, y\rangle \in f) \tag{83}$$

By Lemma 13.3, $a \in range(f) \ \lor \ a \notin range(f)$. Explicitly,

$$\exists x \in X \, (\langle x, a\rangle \in f) \ \lor \ \neg \exists x \in X \, (\langle x, a\rangle \in f).$$

We argue by cases accordingly.

Case 1, $\exists x \in X \, (\langle x, a\rangle \in f)$. Fix c such that $c \in X$ and $\langle c, a\rangle \in f$. Since X has decidable equality, we have $c = a \ \lor \ c \neq a$. We argue by cases.

Case 1a, $c = a$. Then $f : B \to B$. Let g be f restricted to B. Then g is one-to-one, since f is one-to-one. By the induction hypothesis, $g : B \to B$ is onto. Now let $y \in X$. Then $y = a \lor y \in B$. If $y = a$, then $\langle a, a\rangle \in f$. If $y \in B$, then since g is onto, there exists $x \in B$ with $\langle x, y\rangle \in B$. Then $\langle x, y\rangle \in f$. That completes Case 1a.

Case 1b, $c \neq a$. Since $f : X \to X$, there exists $b \in X$ such that $\langle a, b\rangle \in f$. Then $a \neq b$, since $\langle c, a\rangle \in f$ and $\langle a, b\rangle \in f$, so if $a = b$ then $\langle a, a\rangle \in f$; then since f is one-to-one we have $a = c$, contradiction. Define

$$g := (f - \{\langle c, a\rangle\} - \langle a, b\rangle) \cup \{\langle c, b\rangle\}.$$

We have $Rel(g)$, since by hypothesis $Rel(f)$. I say $dom(g) = B$. By extensionality, it suffices to show

$$\exists y \, (\langle t, y\rangle \in g) \leftrightarrow t \in B \tag{84}$$

Left to right: Assume $\langle t, y\rangle \in g$. Then

$$(\langle t, y\rangle \in f \ \land \ \langle t, y\rangle \neq \langle c, a\rangle \ \land \ \langle t, y\rangle \neq \langle a, b\rangle) \ \lor \ (t = c \ \land \ y = b).$$

If the second disjunct holds, then $t = c$, and $c \in X$ but $c \neq a$, so $c \in B$; so $t \in B$. Therefore we may assume the first disjunct holds:

$$(\langle t, y\rangle \in f \ \land \ \langle t, y\rangle \neq \langle c, a\rangle \ \land \ \langle t, y\rangle \neq \langle a, b\rangle).$$

Then $t \in X$ since $dom(f) = X$. Since $\langle t, y\rangle \neq \langle a, b\rangle$, we have $y \neq b$. Since $\langle a, b\rangle \in f$ and $\langle t, y\rangle \in f$ it follows that $t \neq a$. Since $X = B \cup \{a\}$, we have $t \in B$. That completes the left-to-right direction of (84).

Right to left. Suppose $t \in B$. Since $dom f = X$ and $B \subseteq X$, there exists z such that $\langle t, z\rangle \in f$. Unless $t = c$ or $t = a$, we have $\langle t, z\rangle \in g$. If $t = c$ we can take $y = b$. Since $t \in B$ we do not have $t = a$. That completes the proof of (84). That completes the proof that $dom(g) = B$.

Now I say that $g : B \to B$. Suppose $x \in B$. We must show there exists y with $\langle x, y\rangle \in g$. Since $f : X \to X$, there exists $y \in X$ such that $\langle x, y\rangle \in f$. Then $x = c \ \lor \ x \neq c$. If $x \neq c$ then $\langle x, y\rangle \in g$. If $x = c$ then $\langle x, b\rangle \in g$. That completes the proof that $\exists y \, (\langle x, y\rangle \in g)$. We must also show that if $\langle x, y\rangle \in g$ and $\langle x, z\rangle \in g$ then $y = z$. If $x \neq c$ then $\langle x, y\rangle \in f$ and $\langle x, z\rangle \in f$, so $y = z$. If $x = c$ then $y = b$ and $z = b$, so $y = z$. That completes the proof that $g : B \to B$.

Now I say that g is one-to-one. Suppose $g(u) = g(v)$. If $u \neq c$ and $v \neq c$, then $g(u) = f(u)$ and $g(v) = f(v)$, so $u = v$ since f is one-to-one. If $u = c$ and $v \neq c$ then $g(u) = b$. Since $v \neq c$, $g(v) = f(v) = b$. Since f is one-to-one, $v = a$. But $v \notin B$, so $\langle v, b\rangle \notin g$, since $dom(g) = B$. Similarly if $v = c$ and $u \neq c$. That completes the proof that g is one-to-one.

By the induction hypothesis, g is onto. Now I say that f is onto. Let $y \in X$. Then if $y = a$, we have $\langle c, y\rangle \in f$. If $y = b$ we have $\langle a, y\rangle \in f$. If $y \neq a$ and $y \neq b$, then $y = g(x) = f(x)$ for some x. Since X has decidable equality, these cases are exhaustive. That completes Case 1b.

Case 2, $\neg\exists x \in X\,(\langle x, a\rangle \in f)$. Let g be f restricted to B. Then $Rel(g)$, and $dom(g) = B$, and g is one-to-one, and $g : B \to B$. Then by the induction hypothesis, g is onto. Since $f : X \to X$, there exists some $b \in X$ such that $\langle a, b\rangle \in f$. By hypothesis $b \neq a$. Then $b \in B$. Since g is onto, there exists $x \in B$ such that $\langle x, b\rangle \in g$. Then $\langle x, b\rangle \in f$. Since f is one-to-one, we have $x = a$. But $x \in B$, while $a \notin B$. That contradiction completes Case 2. That completes the proof of the theorem.

Lemma 13.5. *Let* $B \in \mathsf{FINITE}$ *and* $a \notin B$. *Then* $Nc(B \cup \{a\}) = (Nc(B))^+$.

Proof. We have

$B \in Nc(B)$	by Lemma 4.11
$B \cup \{a\} \in Nc(B \cup \{a\})$	by Lemma 4.11
$B \cup \{a\} \in (NcB)^+$	by definition of successor
$B \cup \{a\} \in \mathsf{FINITE}$	by Lemma 3.7
$Nc(B \cup \{a\} \in \mathbb{F}$	by Lemma 4.21
$Nc(B) \in \mathbb{F}$	by Lemma 4.21
$(Nc(B))^+ \in \mathbb{F}$	by Lemma 4.19
$B \cup \{a\} \in Nc(B \cup \{a\}) \cap (Nc(B))^+$	by the definition of intersection
$Nc(B \cup \{a\} = (Nc(B))^+$	by Lemma 5.7

That completes the proof of the lemma.

Lemma 13.6. *Let* $m, n \in \mathbb{F}$ *and* $m + n \leq m^+$ *and* $m + n \in \mathbb{F}$ *and* $n \neq \mathsf{zero}$. *Then* $n = \mathsf{one}$.

Proof.

$n = r^+$	for some $r \in \mathbb{F}$, by Lemma 4.17
$m + r^+ \leq m^+$	since $m + n \leq m^+$ and $n = r^+$
$a \in m + n \;\wedge\; b \in m^+$	for some a and b, by definition of addition
$m^+ \in \mathbb{F}$	by Lemma 4.19
$m + r^+ + k = m^+$	for some $k \in \mathbb{F}$, by Lemma 8.22
$(m + r + k)^+ = m^+$	by Lemma 8.2
$m + r \in \mathbb{F}$	by Lemma 8.8
$m + r + k^+ = m^+$	by Lemma 8.2
$m + r + k^+ \in \mathbb{F}$	since $m + r + k^+ = m^+ \in \mathbb{F}$
$m + r + k \in \mathbb{F}$	by Lemma 8.9
$m + r + k = m$	by Lemma 5.12
$r + k + m = \mathsf{zero} + m$	by Lemma 8.2

$m + r \in \mathbb{F} \ \wedge \ r + k \in \mathbb{F}$	by Lemm 8.7
$r + k + m \in \mathbb{F}$	by commutativity and associativity, since $m + r + k \in \mathbb{F}$
$r + k = \mathsf{zero}$	by Lemma 8.16
$(m + r)^+ \le m^+$	by Lemma 8.2
$m + r^+ \in \mathbb{F}$	since $m + n \in \mathbb{F}$
$m + r \in \mathbb{F}$	by Lemma 8.9
$m + r = m$	by Lemma 5.12
$m + r = m + \mathsf{zero}$	by Lemma 8.2
$r = \mathsf{zero}$	by Lemma 8.16
$n = r^+ = \mathsf{zero}^+ = \mathsf{one}$	since $\mathsf{one} = \mathsf{zero}^+$
$r = \mathsf{zero}$	by Lemma 11.25
$r^+ = \mathsf{one}$	by the definition of one
$n = \mathsf{one}$	since $n = r^+$

That completes the proof of the lemma.

Lemma 13.7. *Let $X \in \mathsf{FINITE}$ and let Z be a separable subset of X. Then*

$$Nc(Z) \le Nc(X).$$

Proof. We have

$Nc(X) \in \mathbb{F}$	by Lemma 4.21
$Z \in \mathsf{FINITE}$	by Lemma 3.19
$Nc(Z) \in \mathbb{F}$	by Lemma 4.21
$X \in Nc(X)$	by Lemma 4.11
$Z \in Nc(Z)$	by Lemma 4.11
$Nc(Z) \le Nc(X)$	by the definition of $\le$

That completes the proof of the lemma.

Theorem 13.8. *Let X be a finite set, and let $f : X \to X$ be onto, with $dom(f) \subseteq X$. Then f is one-to-one.*

Proof. We prove the more general fact that if X and Y are finite sets with $Nc(X) \le Nc(Y)$, and $f : X \to Y$ is onto, then f is one-to-one. (The theorem follows by taking $Y = X$). More explicitly, we will prove by induction on finite sets Y that

$$\begin{aligned}
&\forall Y \in \mathsf{FINITE}\, \forall X \in \mathsf{FINITE}\, (Nc(X) \le Nc(Y) \to \forall f\, (f \in \mathsf{FUNC}\\
&\to Rel(f) \to dom(f) \subseteq X\\
&\to \forall x \in X\, \exists y \in Y\, (\langle x, y\rangle \in f)\\
&\to \forall y \in Y\, \exists x \in X\, (\langle x, y\rangle \in f)\\
&\to \forall y \in Y\, \forall x, z \in X\, (\langle x, y\rangle \in f \to \langle z, y\rangle \in f \to x = z)))
\end{aligned}$$

The formula is stratified, giving x, y, z index 0, f index 3, X and Y index 1, and $Nc(X)$ and $Nc(Y)$ index 2. FUNC and FINITE are parameters; $Rel(f)$ is stratified giving f index 3; $dom(f) \subseteq X$ can be expressed as $\forall x, y\, (\langle x, y\rangle \in f \to x \in X)$, which is stratified. Therefore we may proceed by induction on finite sets Y.

Base case, $Y = \Lambda$. Then (in the last line) $y \in Y$ is impossible, so the last line holds if the previous lines are assumed. That completes the base case.

Induction step, $Y = B \cup \{a\}$ with $a \notin B$ and $B \in \mathsf{FINITE}$. Suppose $X \in \mathsf{FINITE}$, and $f : X \to Y$ is onto, and $f \in \mathsf{FUNC}$ and $Rel(f)$ and $dom(f) \subseteq X$. We must prove $f : X \to Y$ is one-to-one. Define

$$Z := \{x \in X : \langle x, a\rangle \in f\}. \tag{85}$$

The formula is stratified, giving x and a index 0 and f index 3, so the definition is legal. Since f is onto, Z is inhabited. I say that Z is a separable subset of X. That is,

$$\forall x \in X\, (\langle x, a\rangle \in f \;\vee\; \langle x, a\rangle \notin f). \tag{86}$$

To prove that, let $x \in X$. Since $f : X \to Y$, there exists $y \in Y$ with $\langle x, y\rangle \in f$. Since $f \in \mathsf{FUNC}$, we have $\langle x, a\rangle \in f \leftrightarrow y = a$. Since Y is finite, we have $y = a \vee y \neq a$ by Lemma 3.3. That completes the proof of (86). Then by Lemma 3.19, $Z \in \mathsf{FINITE}$ and $X - Z \in \mathsf{FINITE}$.

Let g be f restricted to $X - Z$. Then $g : X - Z \to B$ and g is onto B. I say that

$$Nc(X - Z) \neq Nc(X) \tag{87}$$

To prove that, assume $Nc(X - Z) = Nc(X)$. Then

$Nc(X - Z) \in \mathbb{F}$	by Lemma 4.21
$Nc(X) \in \mathbb{F}$	by Lemma 4.21
$X \sim X - Z$	by Lemma 4.9
$u \in Z$	for some $u \in X$, since f is onto Y
$X - Z \subseteq X$	by the definition of Z
$X \neq X - Z$	since $u \notin X - Z$ but $u \in X$

Therefore X is similar to a proper subset of X. Then by Definition 3.23, X is infinite. Then by Theorem 3.24, X is not finite. But that contradicts the hypothesis. That completes the proof of (87).

Now I say that $Nc(X - Z) \leq Nc(B)$. To prove that:

$Nc(X - Z) \leq Nc(X)$	by Lemma 13.7
$Nc(X - Z) < Nc(X)$	by (87 and the definition of $<$
$Nc(X) \leq Nc(B \cup \{a\})$	by hypothesis
$Nc(B \cup \{a\}) = (Nc(B))^+$	since $a \notin B$
$Nc(X - Z) < Nc(B)^+$	by the previous two lines
$Nc(X - Z) \leq Nc(B)$	by Lemma 13.6

Therefore we can apply the induction hypothesis to g. Hence $g : X - Z \to B$ is one-to-one. Therefore g is a similarity. Then

$$\begin{aligned}
Nc(X - Z) &= Nc(B) && \text{by Lemma 4.9 and ten omitted steps}\\
Nc(X) &= Nc(X - Z) + Nc(Z) && \text{by Lemma 8.15}\\
Nc(X) &= Nc(B) + Nc(Z) && \text{by the previous two lines}\\
Nc(X) &\le Nc(Y) && \text{by hypothesis}\\
Nc(B) + Nc(Z) &\le Nc(Y) && \text{by the previous two lines}\\
Nc(Y) &= Nc(B)^+ && \text{since } Y = B \cup \{a\} \text{ and } a \notin B\\
Nc(B) + Nc(Z) &\le Nc(B)^+ && \text{by the previous two lines}\\
Nc(Z) &= \mathsf{one} && \text{by Lemma 13.6}
\end{aligned}$$

By Lemma 6.5, Z is a unit class $\{c\}$ for some c. By (85),

$$\forall x\,(\langle x, a\rangle \in f \leftrightarrow x = c).$$

I say that f is one-to-one. To prove that, let $u, v \in X$ and $\langle u, y\rangle \in f$ and $\langle v, y\rangle \in f$. We must prove $u = v$. Since Y has decidable equality, we have $y = a \ \vee\ y \neq a$. We argue by cases accordingly.

Case 1, $y = a$. Then $u \in Z$ and $v \in Z$. Then $u = c$ and $v = c$, so $u = v$. That completes Case 1.

Case 2, $y \neq a$. Then $u \notin Z$ and $v \notin Z$, so $\langle u, y\rangle \in g$ and $\langle v, y\rangle \in g$. Since g is one-to-one, we have $u = v$ as desired. That completes Case 2. That completes the induction step. That completes the proof of the lemma.

14. The initial segments of $\mathbb{F}$

Next we begin to investigate the possible cardinalities of finite sets. The set of integers less than a given integer is a canonical example of a finite set.

Definition 14.1. *For $k \in \mathbb{F}$, we define*

$$\mathbb{J}(k) = \{x \in \mathbb{F} : x < k\}$$

$$\bar{\mathbb{J}}(k) = \{x \in \mathbb{F} : x \le k\}.$$

The definition is stratified, so $\mathbb{J}(k)$ can be defined, but $\mathbb{J}(k)$ gets index 1 if x gets index 0, so $\mathbb{J}$ is not definable as a function on $\mathbb{F}$.

Lemma 14.2. *For each $m \in \mathbb{F}$, if $m^+ \in \mathbb{F}$ then*

$$\mathbb{J}(m^+) = \mathbb{J}(m) \cup \{m\}$$

$$\bar{\mathbb{J}}(m^+) = \bar{\mathbb{J}}(m) \cup \{m^+\}.$$

Proof. By the definitions of $\mathbb{J}$ and $\bar{\mathbb{J}}$, and the fact that for $x \in \mathbb{F}$ we have

$$x < m^+ \leftrightarrow x < m \ \vee\ x = m,$$

by Lemma 5.33. That completes the proof.

Lemma 14.3. *For $m \in \mathbb{F}$, $\mathbb{J}(m)$ and $\bar{\mathbb{J}}(m)$ are finite sets.*

Proof. By induction on m. The formulas to be proved, namely

$$\forall m\,(m \in \mathbb{F} \to \mathbb{J}(m) \in \mathsf{FINITE}$$

and similarly for $\bar{\mathbb{J}}$, are stratified, giving m index 0. $\mathbb{F}$ and FINITE are parameters and do not require an index.

Base case, $m = \mathsf{zero}$. Then $\mathbb{J}(\mathsf{zero}) = \Lambda$, by Lemma 5.34. By Lemma 3.6, $\Lambda \in \mathsf{FINITE}$. That completes the base case for $\mathbb{J}$. For $\bar{J}$, we have $x \le \mathsf{zero} \leftrightarrow x = \mathsf{zero}$, so $\bar{J}(\mathsf{zero}) = \{\mathsf{zero}\}$, which is finite by Lemma 3.7. That completes the base case.

Induction step. Suppose $m \in \mathbb{F}$ and m^+ is inhabited. By induction hypothesis, $\mathbb{J}(m)$ and $\bar{\mathbb{J}}(m)$ are finite. By Lemma 14.2, $\mathbb{J}(m^+) = \mathbb{J}(m) \cup \{m\}$, so by Lemma 3.7, $J(m^+) \in \mathsf{FINITE}$. Similarly for $\bar{\mathbb{J}}(m)$. That completes the induction step. That completes the proof of the lemma.

Lemma 14.4. *Suppose* $m \in \mathbb{F}$. *Then* $Nc(\mathbb{J}(m)) = \mathbb{T}^2 m$.

Proof. The formula of the lemma is stratified, giving m index 0, since then $\mathbb{T}^2 m$ gets index 2, while $\mathbb{J}(m)$ gets index 1 and $Nc(\mathbb{J}(m))$ gets index 2, so the two sides of the equation both get index 2. Therefore the lemma may be proved by induction.

Base case: $\mathbb{J}(\mathsf{zero}) = \Lambda$, by Lemma 5.29. We have $Nc(\Lambda) = \mathsf{zero}$, by Lemma 4.11 and the definition of zero. By Lemma 11.9, we have $\mathbb{T}^2\mathsf{zero} = \mathsf{zero}$. That completes the base case.

Induction step: We have

$$\begin{array}{rl}
\mathbb{J}(m^+) = \mathbb{J}(m) \cup \{m^+\} & \text{by Lemma 14.2} \\
Nc(\mathbb{J}(m)) = \mathbb{T}^2 m & \text{by the induction hypothesis} \\
\mathbb{J}(m) \in \mathbb{T}^2 m & \text{by Lemma 4.11} \\
\exists u\,(u \in m^+) & \text{assumed for proof by induction} \\
m^+ \in \mathbb{F} & \text{by Lemma 4.19} \\
m \notin \mathbb{J}(m) & \text{by definition of } \mathbb{J}(m) \\
\mathbb{J}(m) \cup \{m\} \in (\mathbb{T}^2 m)^+ & \text{by definition of successor} \\
(\mathbb{T}m)^+ = \mathbb{T}(m^+) & \text{by Lemma 11.8} \\
\mathbb{T}(m^+) \in \mathbb{F} & \text{by Lemma 11.6} \\
(\mathbb{T}m)^+ \in \mathbb{F} & \text{by the preceding two lines} \\
\exists u\,(u \in (\mathbb{T}m)^+) & \text{by Lemma 4.7} \\
(\mathbb{T}^2 m)^+ = \mathbb{T}^2(m^+) & \text{by Lemma 11.8} \\
\mathbb{J}(m^+) \in \mathbb{T}^2(m^+) & \text{by the preceding lines} \\
\mathbb{J}(m^+) \in Nc(\mathbb{J}(m^+)) & \text{by Lemma 4.11} \\
\mathbb{J}(m^+) \in \mathbb{T}^2(m^+) \cap Nc(\mathbb{J}(m^+)) & \text{by definition of intersection} \\
Nc(\mathbb{J}(m^+)) = \mathbb{T}^2(m^+) & \text{by Lemma 4.7}
\end{array}$$

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

15. Rosser's Counting Axiom

Rosser introduced the "counting axiom", which is

$$m \in \mathbb{F} \to \mathbb{J}(m) \in m.$$

(See [9], p. 485.) In view of Lemma 14.4, that is equivalent to

$$m \in \mathbb{F} \to \mathbb{T}m = m.$$

Since $2^{\mathbb{T}m}$ is always defined for $m \in \mathbb{F}$, the counting axiom implies that 2^m is always defined for $m \in \mathbb{F}$. In particular then the set of iterated powers of 2 starting from zero is an infinite set. That is the conclusion of Specker's proof (but without assuming the counting axiom). The point here is that the counting axiom eliminates the need to constructivize Specker's proof: if we assume it, there remain only surmountable difficulties to interpreting HA in INF. But the counting axiom is stronger than NF [6], so this observation does not help with the problem of finiteness in INF.

References

[1] Michael Beeson. *Foundations of Constructive Mathematics: Metamathematical Studies*. Number 6 in Ergebnisse der Mathematik und ihrer Grenzgebiete. Springer, Berlin Heidelberg New York Tokyo, 1985.

[2] 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.

[3] Thomas Forster. Quine's new foundations. In Edward N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, summer 2019 edition, 2019.

[4] Thomas E. Forster. A tutorial on constructive NF. In Marcel Crabbé and Thomas Forster, editors, *Proceedings of the 70th anniversary NF meeting in Cambridge*, volume 16 of *Cahiers du Centre de Logique*. Academia-L'Harmattan, 2009.

[5] C. Grabmayer, J. Leo, V. van Oostrom, and Albert Visser. On the termination of Russell's description elimination algorithm. *The Review of Symbolic Logic*, 4:367–393, 9 2011.

[6] Steven Orey. New foundations and the axiom of counting. *Duke Mathematical Journal*, 31(4):655–660, 1964.

[7] J. B. Rosser. The axiom of infinity in Quine's New Foundations. *Journal of Symbolic Logic*, 17:238–242, 1952.

[8] J. Barkley Rosser. *Logic for Mathematicians*. McGraw-Hill, New York, Toronto, London, first edition, 1953.

[9] J. Barkley Rosser. *Logic for Mathematicians*. Dover, Minneola, New York, second edition, 1978.

[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.