Volume 72 (2026), pp. 247–320
Received: *26 June 2025*
Revised: *6 December 2025*
Accepted: *20 January 2026*
DOI: 10.60866/CAM.290

ZML
Zeitschrift für Mathematische Logik
und Grundlagen der Mathematik

Finite sets, mappings, cardinals, and arithmetic in intuitionistic New Foundations

Michael Beeson

Department of Mathematics and Statistics, San José State University, 1 Washington Square, San Jose, CA 95112, California, United States of America

Department of Mathematics, University of California, Santa Cruz, 7487 Red Hill Road, Santa Cruz, CA 95064, California, United States of America

Abstract. NF set theory using intuitionistic logic is called iNF. We develop the theories of finite sets and their power sets and mappings, 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 basis for further investigations of iNF, including the development of Bishop-style constructive mathematics in iNF.

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 extensionality and stratified comprehension. The definition of these axioms will be reviewed below; full details can be found in [18]. Intuitionistic NF, or iNF, is the theory with the same language and axioms as NF, but with intuitionistic logic instead of classical.[1] Here we intend to provide a coherent infrastructure of definitions, theorems, and Lean-checked proofs on which further investigations can be based.[2]

The "axiom" of infinity is a theorem of NF, proved by Rosser [16; 18] and Specker [19]. 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 article on NF says [8]:

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

In attempting to determine whether the quoted statement is true, I found that I first needed to develop enough

Correspondence email: profbeeson@gmail.com

[1] iNF is briefly mentioned in Forster's thesis [9]; next mentioned in [5; 6; 7], where the focus is on intuitionistic type theories. The initial development of iNF may be in [11], which first called attention to the problem of interpreting HA in iNF.

[2] The development of NF and its variants has been surveyed by Forster [10], and a comprehensive online bibliography of research on set theories with a universal set is maintained by Holmes [13].

basic mathematics in $i\mathsf{NF}$ to tackle Specker's proof.[3] That mathematical infrastructure is presented in this paper. The purpose of this development is to provide a basis on which one can:

(1) investigate $i\mathsf{NF}$ further;
(2) develop Bishop-style constructive mathematics in $i\mathsf{NF}$ (after proving or assuming infinity).

The following questions about $i\mathsf{NF}$ remain open:[4]

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

Regarding whether $\mathbb{F}$ is finite: For all we know, there might be a largest finite cardinal $\mathbf{m}$, 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, since $\mathbb{V}$ is not finite. But intuitionistically, it is an open question.

Each of the lemmas and theorems in this paper is provable in $i\mathsf{NF}$. An important reference for NF is Rosser's book [17; 18].[5] 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. Since all of Rosser's results are obtained using classical logic, we cannot rely on Rosser.

It should be noted that the consistency of classical NF has been proved [14], and the proof has been checked in Lean. This result implies, of course, that the subtheory $i\mathsf{NF}$ considered here is also consistent; but it is otherwise not directly relevant.

Notational issues. There is no traditional, universally accepted notation for some of the notions central to NF. Rosser [18] and Specker [19] are two of the original sources. Both of these were written prior to the advent of TeX and LaTeX, and for the most part were limited to characters found on a typewriter keyboard. Forster [10] used different notation, making use of TeX. Now, however, keyboard characters are back in style, because they are easier to use in computer proof-checking. Lean, for example, goes to great lengths to support complicated typography — but one cannot search for those symbols, which is quite annoying.

I therefore used Specker's notation when using Lean and in pre-publication versions of this paper; but the referee asked me to change it, so I did. The following table compares the notational styles of Specker and this paper. It may prove useful if anyone wants to compare this paper to Specker or Rosser, or to the Lean proofs, or to readers who know one style or the other already.

Table 1: Notation.

Specker	This paper
USC(x)	$\mathcal{P}_1(x)$
SSC(x)	$\mathcal{P}_s(x)$
SC(x)	$\mathcal{P}(x)$
Nc(x)	$\lvert x\rvert$
Λ	$\varnothing$

3 Eventually I came to the conclusion that the quoted statement is true; that is beyond the scope of this paper, but see a short discussion near the end.

4 The terms used in these questions can be looked up in the index of [2].

5 The two editions are identical except for the appendices added to the second edition, one of which contains Rosser's proof of infinity.

Use of computer proof-checking. All the proofs in this paper have been checked in the proof assistant Lean. Could there still be errors? The possible sources of error are:

(1) Use of an unstratified definition;
(2) Lean proof and paper proof might not exactly correspond;
(3) Lean might have smuggled in classical logic, i.e., used it without telling me;
(4) Perhaps the order of theorems in the paper is not strictly the logical order.

Regarding the smuggling: Lean's underlying theory is intuitionistic, but the library is classical, and even though I did not use the library, and even though Lean experts helped me, the possibility theoretically exists. Regarding the correspondence: if there are such problems, they are just typos. Regarding stratification: I allowed the full comprehension axiom, but used only stratified instances. I used a computer script *ex post facto* to check stratification.[6] Regarding the order of theorems: At least no lemma or theorem is cited before it is proved. Of course in Lean, the logical order is enforced, but that is often not the best order for presentation.

The reader who is worried about errors in Lean has the option to forget it was ever mentioned, and just read the proofs, which are here presented in complete human-readable detail.

2 Axioms of NF, ordered pairs, and functions

The axioms of NF are extensionality and stratified comprehension. The axiom of extensionality says that two sets with the same elements are equal. The axiom schema of stratified comprehension says that $\{x : \varphi(x)\}$ 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

(1) in every subformula $x \in y$, y gets an index one greater than x gets, and
(2) 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. The empty set can be defined as $\varnothing = \{x : x \neq x\}$.

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 two more than the indices of the paired elements.[7] 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 $x \cup y$ and intersection $x \cap y$, union, intersection,

[6] Originally I intended to use a finite axiomatization. But it is often quite complicated to derive simple definitions from a finite axiomatization; and then one still has to worry if the finite axiomatization is really correct.

[7] The axiom of infinity is needed to construct an ordered pair that does not raise the type level. See [18, p. 280].

set difference $x - y$, and generally we can add a function symbol c_φ for any stratified formula φ, so that $x \in c_\varphi(y) \leftrightarrow \varphi(x, y)$. For a detailed discussion of the logical underpinnings of this step, see [12]. 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 $\varphi(u, x)$ is $u = x$. □

Lemma 2.4. For all $a, b, x\, (x \in a - b \leftrightarrow x \in a \wedge x \notin b)$.

Proof. This can be taken as the defining axiom for $a - b$; or it may be derived in a finite axiomatization from other axioms. □

Lemma 2.5. For all $x, y\, (\{x\} = \{y\} \leftrightarrow x = y)$.

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

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

□

2.1 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 $\varphi(x)$ 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 $z \in y$, y is assigned an index one larger than the index assigned to z. Note that the assignment is to variables, rather than occurrences of variable, so every occurrence of z 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 two 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 [12] meets the need: it will unwind the function symbols in favor of their definitions, preserving stratification.[8] 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

8 The referee pointed out [1], which is recent enough that it cites a preprint version of this paper. Theorem 3.11 of that paper is the key step in proving that stratified comprehension in the extended language is conservative over NF.

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 were at some point 154 instances of comprehension in that list (which includes more than just the instances used in this paper). The Lean proof assistant does not check 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.

2.2 Functions and functional notation

Definition 2.6. The expression $f\colon X \to Y$ (*f maps X to Y*) means "for every $x \in X$ there exists a unique $y \in Y$ such that $\langle x, y\rangle \in f$". The expression *"$f$ 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.[9] Here is how to do that. We introduce a function symbol "Ap" (with the idea that we will abbreviate $\mathrm{Ap}(f, x)$ to $f(x)$ informally).

Definition 2.7. $\mathrm{Ap}(f, x) = \{u : \exists y\,(\langle x, y\rangle \in f \wedge u \in y\}$.

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 $\mathrm{Ap}(f, x)$ by $f(x)$ anyway, so Ap will be invisible in the informal development. This procedure is justified by the following lemma:

Lemma 2.8. If f is a function and $\langle x, y\rangle \in f$, then $y = \mathrm{Ap}(f, x)$.

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

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

Right to left. Suppose $t \in \mathrm{Ap}(f, x)$. 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. □

2.3 One-to-one, onto, and similarities

The function $f\colon X \to Y$ 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 $f\colon X \to Y$ 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 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.

[9] 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.

Lemma 2.9. 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 $f\colon X \to Y$ is one-to-one, then $f^{-1}\colon Y \to X$ and f^{-1} is one-to-one and onto.

Proof. Let $f\colon X \to Y$ 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, $f^{-1}\colon y \to x$. Since $f\colon X \to Y$, for each $x \in X$ there is a unique $y \in Y$ such that $\langle x, y\rangle \in f$.

I say $f^{-1}\colon Y \to X$. 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 $f^{-1}\colon Y \to X$, as claimed.

I say f^{-1} is one-to-one from Y to X. Let $x \in X$; since $f\colon X \to Y$ 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 $f\colon X \to Y$, 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. □

Definition 2.10. The relation $x \sim y$ (x *is similar to* y) is defined by $\exists f\,(f\colon x \to y \wedge f$ 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 2.11. The relation $x \sim y$ is an equivalence relation.

Proof. Ad reflexivity: We have $x \sim x$ 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 $f\colon x \to y$. By Lemma 2.9, there exists a function $f^{-1}\colon y \to x$ 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 $f\colon x \to y$ is one-to-one and onto, and $g\colon y \to z$ is one-to-one and onto. Then $f \circ g\colon x \to z$ is one-to-one and onto. Therefore $x \sim z$. That completes the proof of transitivity. □

Lemma 2.12. For all $x\,(x \sim \varnothing \leftrightarrow x = \varnothing)$.

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

Right to left. Suppose $x = \varnothing$. We have to show $\varnothing \sim \varnothing$. But $\varnothing\colon \varnothing \to \varnothing$ is a similarity. □

Lemma 2.13. $a \subseteq b \wedge b \subseteq a \leftrightarrow a = b$.

Proof. By the definition of $\subseteq$ and the axiom of extensionality. □

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 $\varnothing$ 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. This definition was introduced in [6] as "N-finite".[10]

---

[10] He also defined other notions of "finite"; for example K-finite drops the requirement $z \notin u$ from the definition. That notion, and the other notion considered *op. cit.*, do not satisfy the property that the cardinality of a finite set is a finite cardinal, i.e., an integer. For example, $\{c\}$ will be K-finite, even if we do not know whether or not c is inhabited, so we cannot assign $\{c\}$ a finite cardinal.

Definition 3.2. The set X *has decidable equality* if $\forall x, y \in X (x = y \vee x \neq y)$. The class $\mathsf{DECIDABLE}$ is the class of all sets having decidable equality.

The formula defining decidable equality is stratified, so the class $\mathsf{DECIDABLE}$ can be proved to exist.

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

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. □

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

Proof. Define $Z = \{X \in \mathsf{FINITE} : X = \varnothing \vee \exists u\, (u \in X)\}$. We will show Z satisfies the closure conditions in the definition of FINITE. Evidently $\varnothing \in Z$. 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 $Y \in Z$. □

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. □

Lemma 3.6. $\varnothing \in \mathsf{FINITE}$.

Proof. $\varnothing$ belongs to every set W containing $\varnothing$ and containing $u \cup \{e\}$ whenever $u \in W$ and $e \notin W$. Since FINITE is the intersection of such sets W, $\varnothing \in \mathsf{FINITE}$. □

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

Proof. Let $x \in \mathsf{FINITE}$. Then x belongs to every set W containing $\varnothing$ 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, $x \cup \{c\} \in \mathsf{FINITE}$. □

Lemma 3.8. If $z \in \mathsf{FINITE}$, then $z = \varnothing$ 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 $z = \varnothing$) and the induction step are immediate. □

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

Proof. We have

$$\begin{aligned}
\varnothing &\in \mathsf{FINITE} && \text{by Lemma 3.6,}\\
x &\notin \varnothing && \text{by the definition of } \varnothing,\\
\varnothing \cup \{x\} &\in \mathsf{FINITE} && \text{by Lemma 3.7,}\\
\{x\} &= \varnothing \cup \{x\} && \text{by the definitions of } \cup \text{ and } \varnothing,\\
\{x\} &\in \mathsf{FINITE} && \text{by the preceding two lines.}
\end{aligned}$$

□

Definition 3.10. $\mathcal{P}_1(x) := \{\{y\} : y \in x\}$.

Lemma 3.11. $\mathcal{P}_1(x)$ is finite if and only if x is finite.

Proof. Left to right. We have to prove $\forall y \in \mathsf{FINITE}\, \forall x\, (y = \mathcal{P}_1(x) \to x \in \mathsf{FINITE})$. 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 $y = \varnothing = \mathcal{P}_1(x)$, we have $x = \varnothing$, so $x \in \mathsf{FINITE}$.

Induction step. Suppose $y \in \mathsf{FINITE}$ has the form $y = z \cup \{w\} = \mathcal{P}_1(x)$ and $w \notin z$, and $z \in \mathsf{FINITE}$. Then $w = \{c\}$ for some $c \in x$. The induction hypothesis is

$$\forall w\, (z = \mathcal{P}_1(w) \to w \in \mathsf{FINITE}). \tag{1}$$

Then

$$\begin{aligned} z &= y - \{w\} && \text{since } y = z \cup \{w\}, \\ &= \mathcal{P}_1(x) - \{\{c\}\} && \text{since } y = \mathcal{P}_1(x) \text{ and } w = \{c\}, \\ &= \mathcal{P}_1(x - \{c\}). \end{aligned}$$

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

$$\begin{aligned} q \in y \to q = \{c\} \vee q \neq \{c\} &\qquad \text{by Lemma 3.3,} \\ u \in x \to \{u\} = \{c\} \vee \{u\} \neq \{c\} &\qquad \text{since } y = \mathcal{P}_1(x), \\ u \in x \to u = c \vee u \neq c. & \end{aligned}$$

It follows that

$$(x - \{c\}) \cup \{c\} = x. \tag{2}$$

By the induction hypothesis (1), with $x - \{c\}$ substituted for w, we have

$$\begin{aligned} x - \{c\} \in \mathsf{FINITE}, & \\ (x - \{c\}) \cup \{c\} \in \mathsf{FINITE} &\qquad \text{by definition of } \mathsf{FINITE}, \\ x \in \mathsf{FINITE} &\qquad \text{by (2).} \end{aligned}$$

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

Right to left. We have to prove

$$x \in \mathsf{FINITE} \to \mathcal{P}_1(x) \in \mathsf{FINITE}. \tag{3}$$

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

Base case. $\mathcal{P}_1(\varnothing) = \varnothing \in \mathsf{FINITE}$.

Induction step. We have for any x and $c \notin x$, $\mathcal{P}_1(x \cup \{c\}) = \mathcal{P}_1(x) \cup \{\{c\}\}$. Let $c \notin x$ and $x \in \mathsf{FINITE}$. By the induction hypothesis (3), $\mathcal{P}_1(x)$ is finite, and since $c \notin x$, we have $\{c\} \notin \mathcal{P}_1(x)$. Then $\mathcal{P}_1(x) \cup \{\{c\}\}$ is finite. Then $\mathcal{P}_1(x \cup \{c\})$ is finite. That completes the induction step. □

Lemma 3.12. The union of two disjoint finite sets is finite.

Proof. We prove by induction on finite sets X that $\forall Y \in \mathsf{FINITE}\, (X \cap Y = \varnothing \to X \cup Y \in \mathsf{FINITE})$.

Base case. $\varnothing \cup Y = Y$ is finite.

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

$$\begin{aligned} X \cup Y &= (Z \cup Y) \cup \{b\} \\ &= Z \cup (Y \cup \{b\}). \end{aligned} \tag{4}$$

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

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

Then by the induction hypothesis, $Z \cup (Y \cup \{b\})$ is finite. Then by (4), $X \cup Y$ is finite. That completes the induction step. □

Lemma 3.13. 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 2.9, $f^{-1} : y \to x$ is a one-to-one function. Then we have for $u, v \in y$,

$$u = v \leftrightarrow f^1(u) = f^{-1}(v). \tag{5}$$

Since x has decidable equality, we have $f^1(u) = f^{-1}(v) \vee f^1(u) \neq f^{-1}(v)$. By (5), $u = v \vee u \neq v$. Therefore y has decidable equality. ☐

Lemma 3.14. 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 of Lemma 3.14. 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. ☐

Lemma 3.15. 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: $x = \varnothing$. Suppose $y \sim \varnothing$. Then $y = \varnothing$, 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 3.13, 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 3.14, $g : z \to y - \{q\}$ 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. ☐

Definition 3.16. The *power set* of a set X is defined as the set of subclasses of X: $\mathcal{P}(X) = \{Y : Y \subset X\}$.

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

Definition 3.17. We define the set of *separable subclasses* of X by $\mathcal{P}_s(X) := \{u : u \subseteq X \wedge X = u \cup (X - u)\}$.

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 $\mathcal{P}_s(X) = \mathcal{P}(X)$, but that is not something we can assert constructively. The formula in the definition is stratified, so the definition can be given in $i\mathsf{NF}$. When working with finite sets, $\mathcal{P}_s(X)$ is a good constructive substitute for $\mathcal{P}(X)$. We illustrate this by proving some facts about $\mathcal{P}(X)$, before returning to the question of the proper constructive substitute for $\mathcal{P}(X)$ when X is not necessarily finite.

Lemma 3.18. Let x be a finite set. Then $\mathcal{P}_s(x)$ is also a finite set.

Remark. We cannot prove this with $\mathcal{P}(x)$ in place of $\mathcal{P}_s(x)$.

Proof of Lemma 3.18. The formula to be proved is $x \in \mathsf{FINITE} \to \mathcal{P}_s(x) \in \mathsf{FINITE}$. 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. $\mathcal{P}_s(\varnothing) = \{\varnothing\}$ 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, $\mathcal{P}_s(x) \in \mathsf{FINITE}$. I say that the map $u \mapsto u \cup \{c\}$ is definable in $i\mathsf{NF}$:

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

The formula can be stratified by giving c index 0, u and y index 1, $\mathcal{P}_s(x)$ index 2; then $\langle u, y\rangle$ has index 3 and we can give f index 4. Hence f is definable in $i\mathsf{NF}$ as claimed. Note that 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 $A := \mathrm{range}(f)$. Then

$$A = \{u \cup \{c\} : u \in \mathcal{P}_s(x)\}. \tag{6}$$

Then $\mathcal{P}_s(x) \sim A$, because $f : \mathcal{P}_s(x) \to A$ is one-to-one and onto. Since $\mathcal{P}_s(x)$ is finite (by the induction hypothesis), by Lemma 3.3, $\mathcal{P}_s(x)$ has decidable equality. Then A has decidable equality, by Lemma 3.13. Since A has decidable equality, and is similar to the finite set $\mathcal{P}_s(x)$, A is finite, by Lemma 3.15.

I say that

$$\mathcal{P}_s(x \cup \{c\}) = A \cup \mathcal{P}_s(x). \tag{7}$$

By extensionality, it suffices to show that the two sides of (7) have the same members.

Left to right. Let $v \in \mathcal{P}_s(x \cup \{c\})$. Then v is a separable subset of $x \cup \{c\}$. Then $c \in v \vee c \notin v$. If $c \notin v$ then $v \in \mathcal{P}_s(x)$. If $c \in v$,

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

We have $v - \{c\} \in \mathcal{P}_s(x)$, since $v \subset x \cup \{c\}$ and v has decidable equality. Then $f(v - \{c\}) \in \mathrm{range}(f) = A$. But $f(v - \{c\}) = (v - \{c\}) \cup \{c\} = v$. Therefore $v \in A$. Therefore $v \in A \cup \mathcal{P}_s(x)$, as desired. That completes the proof of the left-to-right direction of (7).

Right to left. Let $v \in A \cup \mathcal{P}_s(x)$. Then $v \in A \vee v \in \mathcal{P}_s(x)$.

Case 1: $v \in A$. Then by (6), v has the form $v = u \cup \{c\}$ for some $u \in \mathcal{P}_s(x)$. Then $u \cup \{c\} \in \mathcal{P}_s(x \cup \{c\})$, as required.

Case 2: $v \in \mathcal{P}_s(x)$. First we note that if $c \notin x$ then $\mathcal{P}_s(x) \subseteq \mathcal{P}_s(x \cup \{c\})$. Therefore, since $v \in \mathcal{P}_s(x)$, we have $v \in \mathcal{P}_s(x \cup \{c\})$. That completes the proof of (7).

Note that A and $\mathcal{P}_s(x)$ are disjoint, since every member of A contains c, and no member of $\mathcal{P}_s(x)$ contains c, since $c \notin x$. Then by Lemma 3.12 and (7), $\mathcal{P}_s(x \cup \{c\}) \in \mathsf{FINITE}$, as desired. □

Lemma 3.19. 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

$$b \in \mathsf{FINITE} \to b \subseteq a \to a = (a - b) \cup b. \tag{8}$$

The formula is stratified, so induction is legal.

Base case: $b = \varnothing$. Then $b \subseteq a$, so we have to prove $a = (a - \varnothing) \cup \varnothing$, 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 $a = (a - (b \cup \{c\})) \cup (b \cup \{c\})$. By extensionality, it suffices to show that

$$x \in a \leftrightarrow x \in (a - (b \cup \{c\}) \cup (b \cup \{c\}). \tag{9}$$

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

Ad left-to-right of (9)*:* Let $x \in a$. Then by decidable equality on a, we have

$$x = c \vee x \neq c. \tag{10}$$

By the induction hypothesis (8), we have

$$x \in b \vee x \notin b. \tag{11}$$

By (10) and (11) we have $x \in b \cup \{c\} \vee x \notin b \cup \{c\}$. Therefore $x \in (a - (b \cup \{c\}) \cup (b \cup \{c\})$. That completes the left-to-right implication in (9).

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. □

Lemma 3.20. 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, $\forall z \in X\,(z \in U \vee z \notin U)$. 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,

$$\forall z \in Y\,(z \in V \vee z \notin V). \tag{12}$$

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 (12). 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. □

Lemma 3.21. 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,

$$a \in \mathsf{FINITE} \wedge c \in a \to a - \{c\} \in \mathsf{FINITE}. \tag{13}$$

By Lemma 3.3, a has decidable equality. Hence $a - \{c\}$ is a separable subset of a. Then by Lemma 3.20, it is finite. That completes the proof of (13).

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. $\varnothing - b = \varnothing$ 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 3.19. 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 (13). 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, and that completes the proof of the induction step. □

Lemma 3.22 (Bounded quantification)**.** Let X be any set with decidable equality, and B a finite subset of X. Let Y be any set, with R a separable subset of $X \times Y$. Let P be defined by $z \in P \leftrightarrow z \in X \wedge \exists u \in B\, \langle u, z\rangle \in R$. Then P is a separable subset of X. With complete precision:

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

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

Proof of Lemma 3.22. 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: $B = \varnothing$. Then $X \times Y = \varnothing$, so $R = \varnothing$. 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

$$\forall z \in X\, (\exists u \in B\, \langle u, z\rangle \in R \leftrightarrow (\exists u \in A\, \langle u, z\rangle \in R) \vee \langle c, z\rangle \in R). \tag{14}$$

We have to prove $(\exists u \in B\, \langle u, z\rangle \in R) \vee \neg (\exists u \in B\, \langle u, z\rangle \in R)$. By (14), that is equivalent to

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

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. □

Lemma 3.23 (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 $f\colon U \to Y$ 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 $f\colon U \to Y$ 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 $f(u) = c$ and $f(v) = v$. Since $f(u) = f(v)$ we have $v = c$. But $v \in U$ and $c \notin U$, contradiction. □

Definition 3.24 (Dedekind)**.** The class X is *infinite* if $X \sim Y$ for some $Y \subseteq X$ with $Y \neq X$.[11]

Theorem 3.25. 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 of Theorem 3.25. 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 $i\mathsf{NF}$. Therefore induction is legal.

Base case: $X = \varnothing$. The only subset of $\varnothing$ is $\varnothing$, 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,
$f\colon X \to Y$	with f one-to-one and onto, by definition of $X \sim Y$,
$Y \in \mathsf{FINITE}$	by Lemma 3.15,
$Y \in \mathsf{DECIDABLE}$	by Lemma 3.3.

Let $c = f(b)$ and $U = Y - \{c\}$. Let g be f restricted to A. Then $g\colon A \to U$ 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 3.19, 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, and $p \neq b$ 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 $g\colon A \to Y - \{b\}$ 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 $Y - \{b\}$. By the induction hypothesis, $A = Y - \{b\}$. Therefore $Y = A \cup \{b\} = X$. That completes Case 2.

[11] Alternate definitions one might consider: X is infinite if there is a similarity from X to a subset of X that omits a value; X is infinite if $X - A$ is inhabited, for every finite set A. Whether Dedekind infinite implies these properties is not known.

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 $f\colon A \to Y - \{c\} \subseteq A$. Then by the induction hypothesis, $Y - \{c\} = A$. 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. □

Lemma 3.26. A finite union of finite disjoint sets is finite. That is,

$$x \in \mathsf{FINITE} \land \forall u\,(u \in x \to u \in \mathsf{FINITE}) \land \forall u, v \in x\,(u \neq v \to u \cap v = \varnothing) \\ \to \bigcup x \in \mathsf{FINITE}.$$

Proof. By induction on the finite set x.

Base case: $x = \varnothing$. Then $\bigcup x = \varnothing$, which is finite.

Induction step. Suppose $x = y \cup \{c\}$ 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 disjoint. Then by the induction hypothesis, $\bigcup y$ is finite. A short argument from the definitions of union and binary union proves $\bigcup(y \cup \{c\}) = (\bigcup y) \cup c$. Since $x = y \cup \{c\}$, we have

$$\bigcup x = (\bigcup y) \cup c. \tag{15}$$

Now c is finite, since every member of x is finite and $c \in x$. We have $\bigcup y \cap c = \varnothing$, 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 3.12. Then $\bigcup x$ is finite, by (15). That completes the induction step. □

Lemma 3.27. Suppose $c \notin x$. Then $\mathcal{P}_s(x) \subseteq \mathcal{P}_s(x \cup \{c\})$.

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

Lemma 3.28. 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 $(u \in X \lor u \notin X) \land (u \in Y \lor u \notin Y)$. I say that $X \cap Y$ is a separable subset of A. To prove that, we must prove

$$u \in X \cap Y \lor u \notin X \cap Y. \tag{16}$$

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, (16) is immediate. Hence $X \cap Y$ is a separable subset of A, as claimed. Similarly, $X \cup Y$ is a separable subset of A. □

Lemma 3.29 (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 of Lemma 3.29. 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: $B = \varnothing$. The conclusion $\forall x \in \varnothing\, x \in P$ holds since $x \in \varnothing$ 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

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

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

$$\forall x \in B\,(\neg\neg\, x \in Q). \tag{17}$$

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 (17) we have

$$\neg\neg\,\forall x \in B\,(x \in Q) \qquad \text{by the induction hypothesis,}$$
$$\neg\neg\,\forall x \in B\,(x \in P \land c \in P) \qquad \text{by the definition of } Q. \tag{18}$$

Now we would like to infer

$$\neg\neg\,((\forall x \in B\,(x \in P)) \land c \in P), \tag{19}$$

which seems plausible as x does not occur in $c \in P$. In fact we have the equivalence of (18) and (19), since B is inhabited. (That was why we had to break the proof into cases according as B is empty or inhabited.) Then indeed (19) follows. By the definitions of union and unit class we have

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

Applying that equivalence to (19), we have the desired conclusion, $\neg\neg\,\forall x \in (B \cup \{c\})\,(x \in P)$. That completes the induction step. □

Lemma 3.30. 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 $\{x \in \{\varnothing\} : P\}$. That set is finite if and only if $P \lor \neg P$, by Lemma 3.4.

Proof of Lemma 3.30. Let X be a finite set, and $A \subseteq X$. By Lemma 3.20, 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

$$\neg\neg\, X = A \cup (X - A). \tag{20}$$

We have

$$\begin{aligned} \forall t \in X\, \neg\neg\,(t \in A \vee t \notin A) &\quad \text{by logic,} \\ \neg\neg\,\forall t \in X\, t \in A \vee t \notin A) &\quad \text{by Lemma 3.29,} \\ \neg\neg\, X = A \cup (X - A) &\quad \text{by the definitions of union and difference.} \end{aligned}$$

That is (20). □

Lemma 3.31. Let $x \in \mathsf{FINITE}$ and $y \in \mathsf{FINITE}$. Then $\neg\neg\,(x \cup y \in \mathsf{FINITE})$.

Remark. Lemma 3.12 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 of Lemma 3.31. The formula is stratified, so we can prove it by induction on finite sets y, for a fixed finite set x.

Base case: $y = \varnothing$. We have $x \cup \varnothing = x$, 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

$$c \notin x \to x \cup (y \cup \{c\}) \in \mathsf{FINITE}. \tag{21}$$

To prove that:

$$\begin{aligned} x \cup (y \cup \{c\}) = (x \cup y) \cup \{c\} &\quad \text{by definition of union,} \\ c \notin x \cup y &\quad \text{since } c \notin x, \\ x \cup (y \cup \{c\}) \in \mathsf{FINITE}. & \end{aligned}$$

That completes the proof of (21).

We also have

$$c \in x \to x \cup (y \cup \{c\}) \in \mathsf{FINITE}, \tag{22}$$

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 (21) and (22), we have $\neg\neg\,(x \cup y) \cup \{c\} \in \mathsf{FINITE}$. That completes the induction step. □

Lemma 3.32. Let X be a finite set and $c \in X$. Then $X - \{c\}$ is finite.

Proof. We have

$$\begin{aligned} X \text{ has decidable equality} &\quad \text{by Lemma 3.3,} \\ X - \{c\} \text{ is a separable subset of } X &\quad \text{by the definition of separable,} \\ X - \{c\} \in \mathsf{FINITE} &\quad \text{by Lemma 3.20.} \end{aligned}$$

□

Before leaving this section, we shall state a technical lemma about similarities, arising from the details of the definitions of "maps" and "similarity". The issue is that $f\colon X \to Y$ does not require that the domain of f be exactly X; it is allowed to be larger. That is generally a good thing, as once we have defined X and proved it maps X to Y, it automatically maps subsets of X to Y. But to be a similarity from X to Y, the domain of f must be exactly X and the range exactly Y. The following lemma is the price we must pay for allowing the domain of f to be larger in "maps". Stating it here allows us to cite it, without revisiting this issue in future work.

Lemma 3.33. Suppose $f\colon A \to B$ and f is one-to-one and onto B. Let R be the range of f. Suppose $R \subseteq B$ and the domain of f is A. Then f is a similarity from A to R.

Proof. We omit the proof, which takes 111 lines of Lean, because it is just a straightforward unwinding of the definitions involved. □

4 Frege cardinals

The formula in the following definition is stratifiable, so the definition can be given in $i\mathsf{NF}$. 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 $i\mathsf{NF}$.

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

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

Definition 4.2. $\mathsf{zero} = \{\varnothing\}$.

Definition 4.3. The set $\mathbb{F}$ of finite Frege cardinals is the least set containing $\mathsf{zero} = \{\varnothing\}$ 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 $i\mathsf{NF}$. According to that definition, if there were a largest finite cardinal κ, then κ^+ would be the empty set, not zero, which is $\{\varnothing\}$. So in that case, the successor of the largest finite cardinal κ would not belong to $\mathbb{F}$, which does not contain $\varnothing$. Instead, in that case the result would be that successor does not map $\mathbb{F} \to \mathbb{F}$. Of course $\varnothing^+ = \varnothing$, 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, $\mathsf{zero} = \{\varnothing\}$ is in Z, since $\varnothing$ 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 $\mathbb{F} \subseteq Z$. □

Lemma 4.5 (Stratified induction)**.** Let φ be a stratified formula (or weakly stratified with respect to x), so $\{x : \varphi(x)\}$ exists. Then $(\varphi(\mathsf{zero}) \wedge \forall x\,(\varphi(x) \wedge \exists u\,(u \in x^+) \to \varphi(x^+))) \to \forall x\,\varphi(x)$.

Proof. Since $Z := \{x : \varphi(x)\}$ is definable and satisfies the closure conditions that define $\mathbb{F}$, we have $\mathbb{F} \subseteq Z$. □

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

We follow Rosser [17, 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 $\mathsf{NC} = \{\kappa : \forall u \in \kappa \forall v\, (v \in \kappa \leftrightarrow u \sim v)\}$.

Remark. It would not do to use $\exists u$ instead of $\forall u$, since then $\varnothing$ would not be a cardinal, but allow for that possibility. We note that Rosser's definition requires cardinals to be inhabited. In the work presented here, it makes no difference, as we work only with finite cardinals.

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. $\mathsf{zero} = \{\varnothing\}$ is inhabited.

Induction step. Suppose κ^+ is inhabited. Then κ^+ is inhabited. (We do not even need to use the induction hypothesis — see the remark after Lemma 4.5.).) □

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

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

Proof of Lemma 4.8. 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 $i\mathsf{NF}$. Therefore the definition of Z is legal.

We will show Z contains zero and is closed under Frege successor. The only member of zero is the empty set, and the only set in one-to-one correspondence with the empty set is $\varnothing$ itself, therefore Z contains zero.

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 $\mathbb{F} \subseteq Z$. □

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 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. □

Definition 4.10. Following Rosser, we define the cardinal of x to be $|x| = \{u : u \sim x\}$.

Remark. Then the inhabited cardinals, that is, the inhabited members of NC, are exactly the sets of the form $|x|$ for some x.

Lemma 4.11. For all x, $x \in |x|$.

Proof. By Lemma 2.11, we have $x \sim x$. Then $x \in |x|$ by Definition 4.10. □

Lemma 4.12. $|x| = |y|$ if and only if $x \sim y$.

Proof. By Lemma 2.11, which says that the relation $\sim$ is an equivalence relation. □

Lemma 4.13. $c \notin x \to |x \cup \{c\}| = |x|^+$.

Proof. By extensionality, it suffices to show that the two sides have the same members. That is, we must show, under the assumption $c \notin x$, that $u \sim x \cup \{c\} \leftrightarrow \exists b, v\, (b \notin v \land v \sim x \land u = v \cup \{b\})$.

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.

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, $z \in u \to z \in u \to z \neq b \lor z = b$. 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 $y \in x \cup \{c\}$, $y = c \lor y \neq c$. Therefore $z = b \lor z \neq b$, as desired. Note that it is not necessary that z have decidable equality. That completes the left-to-right direction. □

Lemma 4.14. $|\varnothing| = \mathsf{zero}$.

Proof. By Definition 4.2, $\mathsf{zero} = \{\varnothing\}$. By definition, $|\varnothing|$ contains exactly the sets similar to $\varnothing$. By Lemma 2.12, $\varnothing$ is the only set similar to $\varnothing$. Therefore $|\varnothing| = \{\varnothing\}$. Then $|\varnothing| = \mathsf{zero}$ since both are equal to $\{\varnothing\}$. □

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 $\mathsf{zero} = \{\varnothing\}$ on any set.

Proof of Lemma 4.15. 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. □

Lemma 4.16. Frege successor does not take the value 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 $\varnothing$, rather than zero, which is $\{\varnothing\}$, so even in that case zero does not occur as a successor.

Proof of Lemma 4.16. If $\kappa^+ = \{\varnothing\}$, then κ^+ is inhabited, but contains no inhabited set, contradicting Lemma 4.15. □

Lemma 4.17. Every finite cardinal is either equal to zero or is the successor of an element of $\mathbb{F}$.

Proof. The set $Z = \{\kappa \in \mathbb{F} : \kappa = \mathsf{zero} \vee \exists \mu\, (\mu \in \mathbb{F} \wedge \kappa = \mu^+)\}$ is definable in $i\mathsf{NF}$, since its defining formula is stratified. The set Z contains zero and is closed under successor. Therefore, by definition of $\mathbb{F}$, $\mathbb{F} \subseteq Z$. □

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, $\mathsf{zero} \in \mathbb{F}$. □

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. □

Lemma 4.20. The cardinal of a finite set is a finite cardinal. That is, $\forall x \in \mathsf{FINITE}\, (|x| \in \mathbb{F})$.

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

Base case. By Lemma 4.14, $|\varnothing| = \mathsf{zero}$. By Lemma 4.19, $\mathsf{zero} \in \mathbb{F}$.

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

Lemma 4.21. 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, $\mathsf{zero} = \{\varnothing\}$ by definition, so zero is inhabited. For the induction step, we always suppose m^+ is inhabited, so there is nothing more to prove. □

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 4.22. A set similar to a finite set is finite.

Proof. Let a be finite and $a \sim b$. Let $\kappa = |a|$. Then

$$
\begin{aligned}
\kappa &\in \mathbb{F} && \text{by Lemma 4.20,}\\
a &\sim a && \text{by Lemma 2.11,}\\
a &\in \kappa && \text{by definition of } |a|,\\
b &\in \kappa && \text{by Lemma 4.8,}\\
b &\in \mathsf{FINITE} && \text{by Lemma 4.4.}
\end{aligned}
$$
□

Lemma 4.23.

(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 $\mu \subseteq \kappa$. □

Lemma 4.24. Let x and y be finite sets. Then $x \sim y \to |x| = |y|$.

Proof. Assume $x \in \mathsf{FINITE}$ and $y \in \mathsf{FINITE}$ and $x \sim y$. Then

$$
\begin{aligned}
x &\in |x| && \text{by Lemma 4.11,}\\
y &\in |y| && \text{by Lemma 4.11,}\\
|x| &\in \mathbb{F} && \text{by Lemma 4.20,}\\
|y| &\in \mathbb{F} && \text{by Lemma 4.20,}\\
y &\in |x| && \text{by Lemma 4.8,}\\
|x| &= |y| && \text{by Lemma 4.23.}
\end{aligned}
$$

□

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)**.**

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

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:

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

Definition 5.3. The *image of a under f*, written $f\,``\,a$, is defined by $f\,``\,a := \mathrm{range}(f \cap (a \times \mathbb{V}))$.

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 $f\colon b \to c$ 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

$$e \cup (c - e) \subseteq c, \tag{23}$$

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

$$c \subseteq e \cup (c - e), \tag{24}$$

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 (23) and (24), we have $c = e \cup (c - e)$ as desired. □

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

$$c = e \cup (c - e). \tag{25}$$

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

$$\begin{aligned} e \cup (d - e) &= e \cup ((c \cup (d - c)) - e) && \text{since } d = c \cup (d - c), \\ &= e \cup (c - e) \cup ((d - c) - e) && \text{since } (p \cup q) - r = (p - r) \cup (q - r), \\ &= c \cup ((d - c) - e) && \text{by (25)}, \\ &= c \cup (d - c) && \text{since } e \subseteq c, \\ &= d && \text{since } d = c \cup (d - c). \end{aligned}$$

as desired. Then $\kappa \le \mu$ as desired. □

Lemma 5.7. 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 4.23, 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 3.25 implies that y is not finite, which is a contradiction. □

Lemma 5.8. 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

$$y = x \cup (y - x). \tag{26}$$

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 $f\colon y \to b$ 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 (26), 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 $\exists a \in \kappa\,(a \subseteq b \wedge b = a \cup (b - a))$. □

Lemma 5.9. 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 of Lemma 5.9. 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

$$(z \cup \{a\}) - \{c\} = (z - \{c\}) \cup \{a\}. \tag{27}$$

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

$$\begin{aligned} z &\sim (z - \{c\}) \cup \{a\} && \text{by Lemma 3.23,} \\ &= (z \cup \{a\}) - \{c\} && \text{by (27).} \end{aligned}$$

Then by Lemma 4.8 and the fact that $z \in \kappa$, we have $(z \cup \{a\}) - \{c\} \in \kappa$. Since $z \cup \{a\} = x$, that implies $x - \{c\} \in \kappa$, which is the conclusion of the lemma. □

Lemma 5.10. 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 5.8, 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

$$y \cup \{c\} = (x \cup \{c\}) \cup (y \cup \{c\} - (x \cup \{c\})). \tag{28}$$

Left-to-right of (28)*:* 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 (28). 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 (28). If $u \notin x$ then $u \in y \cup \{c\} - (x \cup \{c\})$, and hence u belongs to the right side of (28). That completes the proof of the left-to-right direction of (28).

Right-to-left of (28)*:* 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 (28) is a subset of the left side. That completes the proof of (28).

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 5.9, $x - \{c\} \in \kappa$ 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

$$u \in y \to u = c \vee u \ne c. \tag{29}$$

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

$$u \in y \to u \in x \vee u \notin x. \tag{30}$$

Then by (29) and (30), we have

$$u \in y \to u \in (x - \{c\}) \vee u \notin (x - \{c\}). \tag{31}$$

It follows from (31) that $y - \{c\} = ((y - \{c\}) - (x - \{c\})) \cup (x - \{c\})$. Therefore $\kappa \le \mu$. □

Lemma 5.11. For λ and μ in $\mathbb{F}$, if λ^+ 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 4.23, 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 5.9, $x \cup \{a\} - \{a\} \in \mu$. 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. □

Lemma 5.12. Let x be a separable subset of y, that is, $x \subseteq y$ and $y = x \cup (y - x)$. Then $y - x = \varnothing \leftrightarrow y = x$.

Proof. Suppose $x \subseteq y$ and $y = x \cup (y - x)$.

Left to right. Suppose $y - x = \varnothing$; 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 $y - x = x - x = \varnothing$. □

Lemma 5.13. For finite cardinals κ and μ, if κ^+ and μ^+ are inhabited we have $\kappa < \mu \leftrightarrow \kappa^+ < \mu^+$.

Proof. Left to right. Suppose $\kappa < \mu$. By definition that means $\kappa \le \mu$ and $\kappa \neq \mu$. By Lemma 5.10, $\kappa^+ \le \mu^+$. We have to show $\kappa^+ \neq \mu^+$. 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 5.8, there exists a separable subset x of y with $x \in \kappa$. By Lemma 4.4, x is finite. By Lemma 3.21, $y - x$ is finite. Since $\kappa \neq \mu$, we have $x \neq y$, by Lemma 4.23. Then, since x is a separable subset of y, $y - x$ is not empty, by Lemma 5.12. 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 5.9 we have $y \in \kappa$. But from the start we had $y \in \mu$. Then by Lemma 4.23, 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 $\kappa^+ \neq \mu^+$. By Lemma 5.10, $\kappa \le \mu$, and since successor is a function, $\kappa \neq \mu$. □

Definition 5.14. We define names for the first few integers (repeating the definition of zero, which has already been given).

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

Lemma 5.15. $\mathsf{one} \in \mathbb{F}$.

Proof. We have

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

□

Lemma 5.16. $\forall \kappa \in \mathbb{F}\, (\kappa = \mathsf{zero} \vee \kappa \neq \mathsf{zero})$.

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, $\kappa \in \mathbb{F} \to \kappa = \mathsf{zero} \vee \kappa \neq \mathsf{zero}$. □

Theorem 5.17. 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 $\varnothing$, so $x = y = \varnothing$. Then $\varnothing \in \mu$ and $\varnothing \in \mathsf{zero}$, so by Lemma 4.23, $\mu = \mathsf{zero}$. 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 5.16, $\mu = \mathsf{zero} \vee \mu \neq \mathsf{zero}$; and if $\mu \neq \mathsf{zero}$ then $\mathsf{zero} < \mu$, since $\varnothing$ is a separable subset of any $x \in \mu$.

Induction step. Suppose κ^+ is inhabited. We have to prove $\kappa^+ < \mu \vee \kappa^+ = \mu \vee \mu < \kappa^+$. By Lemma 5.16, 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

$$\kappa^+ < \lambda^+ \vee \kappa^+ = \mu^+ \vee \mu^+ < \lambda^+. \tag{32}$$

By the induction hypothesis we have $\kappa < \lambda \vee \kappa = \mu \vee \mu < \lambda$ and exactly one of the three holds. By Lemma 5.13 and Lemma 5.11, each disjunct is equivalent to one of the disjuncts of (32). That completes the induction step. □

Corollary 5.18. $\mathbb{F}$ 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 5.17, we have $\kappa < \mu$ or $\kappa = \mu$ or $\mu < \kappa$, and exactly one of the disjuncts holds. Therefore $\kappa \neq \mu$ is equivalent to $\kappa < \mu \vee \mu < \kappa$. □

Lemma 5.19. For all $\kappa \in \mathbb{F}$, we have $\kappa \leq \kappa$.

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 $\kappa \leq \kappa$ by the definition of $\leq$. □

Lemma 5.20. For $\kappa, \mu \in \mathbb{F}$ we have $\kappa \leq \mu \leftrightarrow \kappa < \mu \vee \kappa = \mu$.

Proof. Suppose $\kappa, \mu \in \mathbb{F}$. By Theorem 5.17 we have $\kappa < \mu \vee \kappa = \mu \vee \mu < \kappa$, and exactly one of the three disjuncts holds.

Left to right. Suppose $\kappa \leq \mu$. 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 3.21, $b - a$ is finite. By Lemma 3.4, $b - a$ is empty or inhabited.

Case 1: $b - a = \varnothing$. I say $b = a$. By extensionality, it suffices to prove

$$t \in b \leftrightarrow t \in a. \tag{33}$$

Left-to-right of (33)*:* 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 $b - a = \varnothing$. Therefore $t \in a$.

Right-to-left of (33)*:* 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 Lemma 4.23, $\kappa = \mu$. That completes Case 1.

Case 2: $b - a$ is inhabited. Then a is a proper subset of b. By Lemma 5.7, $\kappa < \mu$. 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 5.19. □

Lemma 5.21. For $\kappa, \mu \in \mathbb{F}$ we have $\kappa \le \mu \wedge \mu \le \kappa \to \kappa = \mu$.

Proof. By Lemma 5.20, it suffices to prove

$$(\kappa < \mu \vee \kappa = \mu) \wedge (\mu < \kappa \vee \mu = \kappa) \to \kappa = \mu. \tag{34}$$

By Theorem 5.17, $\kappa < \mu \vee \kappa = \mu \vee \mu < \kappa$ and exactly one of the three disjuncts holds. Now (34) follows by propositional logic. □

We next prove two variations on trichotomy that are frequently useful.

Lemma 5.22. Suppose $\kappa < \mu \le \lambda$, where $\kappa, \mu, \lambda \in \mathbb{F}$. Then $\kappa < \lambda$.

Proof. By Lemma 5.6, we have $\kappa \le \lambda$. We must show $\kappa \ne \lambda$. Suppose $\kappa = \lambda$. Since $\kappa < \mu$ we have $\lambda < \mu$. Hence $\lambda \le \mu$. By hypothesis $\mu \le \lambda$. By Lemma 5.21, $\mu = \lambda$, contradicting $\mu < \lambda$. □

Lemma 5.23. Let $\kappa, \mu \in \mathbb{F}$. Then $\kappa < \mu \vee \mu \le \kappa$.

Proof. By Theorem 5.17, $\kappa < \mu \vee \kappa = \mu \vee \mu < \kappa$.

Case 1: $\kappa < \mu$. Then we are done.

Case 2: $\kappa = \mu$. Then $\kappa \le \mu$ by Lemma 5.19.

Case 3: $\mu < \kappa$. Then $\mu \le \kappa$ by the definition of $<$. □

Lemma 5.24. Let $\kappa, \mu \in \mathbb{F}$. Then $\kappa \le \mu \vee \mu < \kappa$.

Proof. By Theorem 5.17, $\kappa < \mu \vee \kappa = \mu \vee \mu < \kappa$.

Case 1: $\kappa < \mu$. Then $\kappa \le \mu$ by the definition of $<$.

Case 2: $\kappa = \mu$. Then $\kappa \le \mu$ by Lemma 5.19.

Case 3: $\mu < \kappa$. Then we are done. □

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

Proof. By Lemma 5.6, we have $\kappa \le \mu$. Since $\kappa < \mu$ is defined as $\kappa \le \mu$ and $\kappa \ne \mu$, it only remains to show $\kappa \ne \mu$. Suppose $\kappa = \mu$. Then $\kappa \le \lambda$ and $\lambda \le \kappa$. By Theorem 5.17, we have $\kappa = \lambda$, contradiction. □

Lemma 5.26. Let $\kappa, \lambda, \mu \in \mathbb{F}$ and suppose $\kappa < \lambda < \mu$. Then $\kappa < \mu$.

Proof. Since $\kappa < \lambda$ we have $\kappa \le \lambda$, by the definition of $<$. Then by Lemma 5.22, $\kappa < \mu$. □

Lemma 5.27. 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 5.7, 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 $\kappa < \kappa^+$. □

Lemma 5.28. For all $m \in \mathbb{F}$, we do not have $m^+ \le m$.

Proof. Suppose $m \in \mathbb{F}$ and $m^+ \le m$. By the definition of $\le$, m^+ is inhabited. Then by Lemma 5.27, we have $m < m^+$, which contradicts Theorem 5.17, since $m^+ \le m$. □

Lemma 5.29. For $x \in \mathbb{F}$, $x \not< x$.

Proof. Immediate from Theorem 5.17, since $x = x$. □

Lemma 5.30. For $x \in \mathbb{F}$ we have $x \not< \mathsf{zero}$.

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

$$
\begin{array}{rl}
x \le \mathsf{zero} & \text{by definition of } <, \\
a \in x \wedge a \subset b \wedge b \in \mathsf{zero} & \text{for some } a, b, \text{ by definition of } \le, \\
b \in \{\varnothing\} & \text{since } \mathsf{zero} = \{\varnothing\}, \\
b = \varnothing & \text{by Lemma 2.3}, \\
a = \varnothing & \text{since } a \subset b, \\
\varnothing \in x \cap \mathsf{zero} & \text{by definition of intersection}, \\
x = \mathsf{zero} & \text{by Lemma 4.23}, \\
\mathsf{zero} < \mathsf{zero} & \text{since } x < \mathsf{zero}, \\
\neg\, \mathsf{zero} < \mathsf{zero} & \text{by Lemma 5.29}.
\end{array}
$$

That is the desired contradiction. □

Lemma 5.31. 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

$$
\begin{array}{rl}
b \in \mathsf{FINITE} \wedge a \in \mathsf{FINITE} & \text{by Lemma 4.4}, \\
b - a \in \mathsf{FINITE} & \text{by Lemma 3.21}, \\
b - a = \varnothing \vee \exists u\, (u \in b - a) & \text{by Lemma 3.4}.
\end{array}
$$

We argue by cases.

Case 1: $b - a = \varnothing$. Then $b = a$, so $a \in \kappa \cap \mu$, so by Lemma 4.23, $\kappa = \mu$, contradicting $\kappa < \mu$.

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

$$
\begin{array}{rl}
a \cup \{c\} \in \kappa^+ & \text{by the definition of successor}, \\
a \cup \{c\} \subseteq b & \text{since } c \in b, \\
b = (a \cup \{c\}) \cup (b - (a \cup \{c\})) & \text{by Corollary 5.18}, \\
\kappa^+ \le \mu & \text{by the definition of } \le.
\end{array}
$$

□

Lemma 5.32. 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 $u \in \mathcal{P}_s(v)$. Then

$$
\begin{array}{rl}
v \in \mathsf{FINITE} & \text{by Lemma 4.4}, \\
u \in \mathsf{FINITE} & \text{by Lemma 3.20}, \\
v - u \in \mathsf{FINITE} & \text{by Lemma 3.21}, \\
v - u \ne \varnothing & \text{by Lemma 4.23, since } a \ne b,
\end{array}
$$

$$\begin{array}{ll} \exists c\,(c \in v - u) & \text{by Lemma 3.4,} \\ c \in v - u & \text{fixing } c, \\ u \cup \{c\} \in a^+ & \text{by definition of successor,} \\ a^+ \in \mathbb{F} & \text{by Lemma 4.19.} \end{array}$$ □

Lemma 5.33. 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 of Lemma 5.33. Suppose $\kappa \le \mu^+$. Then by Lemma 5.20, $\kappa < \mu^+ \vee \kappa = \mu^+$. If $\kappa = \mu^+$ we are done; so we may suppose $\kappa < \mu^+$. Then

$$\begin{array}{ll} \kappa^+ \le \mu^+ & \text{by Lemma 5.31,} \\ \exists u\,(u \in \mu^+) & \text{by the definition of } \le, \\ \exists u\,(u \in \kappa^+) & \text{by the definition of } \le, \\ \kappa \le \mu & \text{by Lemma 5.10.} \end{array}$$ □

Lemma 5.34. 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 $\kappa \ne \mu^+$. By Lemma 5.33, $\kappa \le \mu$. By Lemma 5.20, $\kappa < \mu \vee \kappa = \mu$ as desired.

Right to left. Assume $\mu^+ \in \mathbb{F}$. Then μ^+ is inhabited, by Corollary 4.7. If $\kappa = \mu$ then $\kappa < \mu^+$ by Lemma 5.27. If $\kappa < \mu$ then $\kappa < \mu^+$ by Lemma 5.26. □

Lemma 5.35. $\forall m \in \mathbb{F}\,(\neg\,(m < \mathsf{zero}))$.

Proof. By definition, $\mathsf{zero} = \{\varnothing\}$. Suppose $m \in \mathbb{F}$ and $m < \mathsf{zero}$. By definition of $<$, $m \le \mathsf{zero}$ and $m \ne \mathsf{zero}$. By definition of $\le$, there exist a and b with $a \in m$ and $b \in \mathsf{zero}$ and $a \in \mathcal{P}_s(b)$. Since $\mathsf{zero} = \{\varnothing\}$ we have $b = \varnothing$. The only separable subset of $\varnothing$ is $\varnothing$, so $a = \varnothing$. Then by Lemma 4.23, $m = \mathsf{zero}$. But that contradicts $m \ne \mathsf{zero}$. Therefore the assumptions $m \in \mathbb{F}$ and $m < \mathsf{zero}$ are untenable. □

Lemma 5.36. 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 of Lemma 5.36. The formula to be proved is $\forall x \in \mathsf{FINITE}\,(x \subseteq \mathbb{F} \to x \ne \varnothing \to \exists m \in x\, \forall t\,(t \in x \to t \le m))$. The formula is stratified, giving m and t index 0 and x index 1. Since $\mathbb{F}$ and FINITE are parameters, they do not require an index. Therefore we may proceed by induction on finite sets.

Base case. Immediate, since $\varnothing \ne \varnothing$.

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 $x = \varnothing$, 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 5.17, $c \le m$ 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 $\le$. □

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

Proof. Suppose $x = x^+$. Then

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

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 3.25, it is not finite. But it is finite. That contradiction shows $x \neq x^+$. □

Lemma 5.38. 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 5.37, we have $x \neq x^+$. Then by definition of $<$, we have $x < x^+$. □

6 Power sets and similarity

We will replace Rosser and Specker's use of the full power set $\mathcal{P}$ by the separable power set $\mathcal{P}_s$. In this section we prove some lemmas from Specker [19, § 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 [19, Lemma 2.6], which we take in two steps with the next two lemmas, and after that [19, Lemma 2.4 and Lemma 2.3].

Lemma 6.1. Let $y \in \mathcal{P}_s(\mathcal{P}_1(a))$. Then there exists $z \in \mathcal{P}_s(a)$ such that $y = \mathcal{P}_1(z)$.

Proof. Suppose $y \in \mathcal{P}_s(\mathcal{P}_1(a))$. Define

$$z := \{u : \{u\} \in y\}. \tag{35}$$

That definition is legal since the formula is stratified giving u index 0 and y index 2. Then $y = \mathcal{P}_1(z)$ since the members of y are the singletons of the members of z. I say that $z \subseteq a$: Suppose $u \in z$. Then

$$\begin{array}{rl} \{u\} \in y & \text{by (35),} \\ \{u\} \in \mathcal{P}_1(a) & \text{since } y \subseteq \mathcal{P}_1(a), \\ u \in a & \text{by definition of } \mathcal{P}_1(a). \end{array}$$

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 (35), $u \in z \vee u \notin z \leftrightarrow \{u\} \in y \vee \{u\} \notin y$, and that is true since y is a separable subset of $\mathcal{P}_1(a)$. □

Lemma 6.2 (Specker, [19, Lemma 2.6])**.** $|\mathcal{P}_s(\mathcal{P}_1(a))| = |\mathcal{P}_1(\mathcal{P}_s(a))|$.

Remarks. Of course Specker has $\mathcal{P}$ instead of $\mathcal{P}_s$. We follow the proof from [17, p. 368], that Specker cites, checking it constructively with $\mathcal{P}_s$ in place of $\mathcal{P}$. But fundamentally, this lemma is just about shuffling brackets. We have $\{\{p\},\{q\},\{r\}\} \in \mathcal{P}_s(\mathcal{P}_1(a))$ corresponding to $\{\{p,q,r\}\} \in \mathcal{P}_1(\mathcal{P}_s(a))$. It is a useful result but not a deep one.

Proof of Lemma 6.2. Let $W := \{u : \exists z\,(u = \langle \{z\}, \mathcal{P}_1(z)\rangle)\}$. The definition is stratified giving z index 1, so $\{z\}$ and $\mathcal{P}_1(z)$ both get index 2, and u gets index 4. It follows that W is a relation (contains only ordered pairs) and $\langle x, y\rangle \in W \leftrightarrow \exists z\,(x = \{z\} \wedge y = \mathcal{P}_1(z))$.

I say that W is (the graph of) a one-one-function mapping $\mathcal{P}_1(\mathcal{P}_s(a))$ onto $\mathcal{P}_s(\mathcal{P}_1(a))$. (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 $y = \mathcal{P}_1(z)$, 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 $y \in \mathcal{P}_s(\mathcal{P}_1(a))$. By Lemma 6.1, there exists $z \in \mathcal{P}_s(a)$ such that $y = \mathcal{P}_1(z)$. Then $\langle \{z\}, y\rangle \in W$. Hence y is in the range of W. Since y was an arbitrary member of $\mathcal{P}_s(\mathcal{P}_1(a))$, it follows that W is onto.

We have shown that W is a similarity from $\mathcal{P}_s(\mathcal{P}_1(a))$ to $\mathcal{P}_1(\mathcal{P}_s(a))$. Therefore those two sets have the same cardinal. □

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 $f\colon \{a\} \to \{b\}$ 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 $f\colon x \to \{a\}$ 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 $x = \{c\}$. □

Lemma 6.5. We have $u \in \mathsf{one} \leftrightarrow \exists a\,(u = \{a\})$.

Proof. By definition, $\mathsf{one} = \mathsf{zero}^+$ and $\mathsf{zero} = \{\varnothing\}$. For any a, we have $a \notin \varnothing$, so $\varnothing \cup \{a\} = \{a\} \in \mathsf{zero}^+ = \mathsf{one}$. Conversely, if $u \in \mathsf{one}$, then $u = \varnothing \cup \{a\}$ for some a, by definition of successor, so $u = \{a\}$. □

Lemma 6.6. Suppose a and b are finite sets. Then $a \in \mathcal{P}_s(b) \to \mathcal{P}_1(a) \in \mathcal{P}_s(\mathcal{P}_s(b))$.

Proof. Suppose $a \in \mathcal{P}_s(b)$. Since b is finite, it has decidable equality, by Lemma 3.3. Therefore $\mathcal{P}_1(b) \subseteq \mathcal{P}_s(b)$. Since $\mathcal{P}_1(a) \subseteq \mathcal{P}_1(b)$, we have $\mathcal{P}_1(a) \subseteq \mathcal{P}_s(b)$. It remains to show that $\mathcal{P}_1(a)$ is a separable subset of $\mathcal{P}_s(b)$; that is, $\mathcal{P}_s(b) = \mathcal{P}_1(a) \cup (\mathcal{P}_s(b) - \mathcal{P}_1(a))$. By extensionality and the definitions of subset and union, it suffices to show $t \in \mathcal{P}_s(b) \leftrightarrow t \in \mathcal{P}_1(a) \vee (t \in \mathcal{P}_s(b) \wedge t \notin \mathcal{P}_1(a))$.

Right to left. It suffices to show $t \in \mathcal{P}_1(a) \to t \in \mathcal{P}_s(b)$. Let $t \in \mathcal{P}_1(a)$. 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 $t \in \mathcal{P}_s(b)$. Then $t \in \mathsf{FINITE}$, by Lemma 3.20. Then $|t| \in \mathbb{F}$, by Lemma 4.20. Then by Corollary 5.18, $|t| = \mathsf{one} \vee |t| \neq \mathsf{one}$.

Case 1: $|t| = \mathsf{one}$. By Lemma 6.5, t is a unit class. Since $a \in \mathcal{P}_s(b)$, we have $x \in b \to x \in a \vee x \notin a$. Since $t \in \mathcal{P}_1(a)$ if and only if for some x we have $t = \{x\} \wedge x \in a$, we have $t \in \mathcal{P}_s(b) \to t \in \mathcal{P}_1(a) \vee t \notin \mathcal{P}_1(a)$. That completes Case 1.

Case 2: $|t| \neq \mathsf{one}$. Then $|t|$ is not a unit class, by Lemma 6.5 and Lemma 4.23, so the second disjunct on the right holds. □

Lemma 6.7 (Specker, [19, Lemma 2.4])**.** For any sets a and b, $a \sim b \leftrightarrow \mathcal{P}_1(a) \sim \mathcal{P}_1(b)$.

Proof. Left to right. Suppose $f\colon a \to b$ 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 $g\colon \mathcal{P}_1(a) \to \mathcal{P}_1(b)$ is a similarity. We omit the straightforward proof.

Right to left. Let $g\colon \mathcal{P}_1(a) \to \mathcal{P}_1(b)$ 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 $f\colon a \to b$ is a similarity. We omit the proof. □

Lemma 6.8 (Specker, [19, Lemma 2.3])**.** For any sets a and b $a \sim b \to \mathcal{P}_s(a) \sim \mathcal{P}_s(b)$.

Proof. Let $f\colon a \to b$ be a similarity. Define $g := \{\langle u, f\text{“}\,u\rangle : u \in \mathcal{P}_s(a)\}$, where $f\text{“}\,u$ is the image of u under f, i.e., the range of the restriction of f to u. Then $g\colon \mathcal{P}_s(a) \to \mathcal{P}_s(b)$. 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 $y \in \mathcal{P}_s(b)$. 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 $g(x) = y$. (We can also define x using the operations of domain and inverse relation, which in turn can be defined by stratified comprehension.) □

Lemma 6.9. If a has decidable equality, then $\mathcal{P}_1(a) \subseteq \mathcal{P}_s(a)$.

Proof. Let $x \in \mathcal{P}_1(a)$. 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. □

Lemma 6.10. For all a, b, $a \subseteq b \leftrightarrow \mathcal{P}_1(a) \subseteq \mathcal{P}_1(b)$.

Proof. Left to right. Suppose $a \subseteq b$ and $t \in \mathcal{P}_1(a)$. We must show $t \in \mathcal{P}_1(b)$. Then $t = \{x\}$ for some $x \in a$. Since $a \subseteq b$ we have $x \in b$. Then $t \in \mathcal{P}_1(b)$. That completes the left-to-right direction.

Right to left. Suppose $\mathcal{P}_1(a) \subseteq \mathcal{P}_1(b)$ and $t \in a$. We must prove $t \in b$. Since $t \in a$ we have $\{t\} \in \mathcal{P}_1(a)$. Then $\{t\} \in \mathcal{P}_1(b)$. Then $\{t\} = \{q\}$ for some $q \in b$. Then $t = q$. Then $t \in b$ as desired. □

Lemma 6.11. For all a, b, $a \in \mathcal{P}_s(b) \leftrightarrow UCS(a) \in \mathcal{P}_s(\mathcal{P}_1(b))$.

Proof. Left to right. Suppose $a \in \mathcal{P}_s(b)$. Then $a \subset b$ and $b = a \cup (b - a)$. By Lemma 6.10,

$$\mathcal{P}_1(a) \subseteq \mathcal{P}_1(b). \tag{36}$$

It remains to show that $UCS(a)$ is a stable subset of $\mathcal{P}_1(b)$; that is, $\mathcal{P}_1(b) = \mathcal{P}_1(a) \cup (\mathcal{P}_1(b) - \mathcal{P}_1(a))$. By extensionality and the definitions of union and set difference, that is equivalent to

$$t \in \mathcal{P}_1(b) \leftrightarrow t \in \mathcal{P}_1(a) \vee (t \in \mathcal{P}_1(b) \wedge t \notin \mathcal{P}_1(a)). \tag{37}$$

Then we need only consider unit classes $t = \{x\}$, and using the fact that $\{x\} \in \mathcal{P}_1(b) \leftrightarrow t \in b$, and $\{x\} \in \mathcal{P}_1(a) \leftrightarrow t \in a$, (37) follows from (36). □

Lemma 6.12. For all a, b, we have $a \in \mathcal{P}_s(b) \leftrightarrow \mathcal{P}_s(a) \subseteq \mathcal{P}_s(b)$.

Proof. Left to right. Suppose $a \in \mathcal{P}_s(b)$. Then $a \subseteq b$ and

$$b = a \cup (b - a). \tag{38}$$

Now let $x \in \mathcal{P}_s(a)$. We must show $x \in \mathcal{P}_s(b)$. Since $x \in \mathcal{P}_s(a)$, we have $x \subseteq a$. Since $a \subseteq b$ we have $x \subseteq b$. We have

$$\begin{aligned} x &\in \mathcal{P}_s(a), \\ a &= x \cup (a - x) && \text{by definition of } \mathcal{P}_s(a), \\ b &= (x \cup (a - x)) \cup (b - (x \cup (a - x))) && \text{by (38)}, \\ b &= x \cup (b - x), \\ x &\in \mathcal{P}_s(b) && \text{by definition of } \mathcal{P}_s(b). \end{aligned}$$

That completes the left-to-right direction.

Right to left. Suppose $\mathcal{P}_s(a) \subseteq \mathcal{P}_s(b)$. We have to show $a \in \mathcal{P}_s(b)$; but that follows from $a \in \mathcal{P}_s(a)$ and the definition of subset. That completes the right to left direction. □

Lemma 6.13. Let b be a finite set. Then the subset relation on $\mathcal{P}_s(b)$ is decidable. That is,

$$\forall x, y \in \mathcal{P}_s(b)\,(x \subseteq y \vee x \not\subseteq y).$$

Proof. Assume $b \in \mathsf{FINITE}$. By Lemma 3.18, $\mathcal{P}_s(b) \in \mathsf{FINITE}$. Then by Lemma 3.3,

$$\mathcal{P}_s(b) \in \mathsf{DECIDABLE}. \tag{39}$$

We will prove by induction on finite sets y that $y \in \mathcal{P}_s(b) \to \forall x \in \mathcal{P}_s(b)\,(x \subseteq y \vee x \not\subseteq y)$. It is legal to proceed by induction, since the formula is stratified.

Base case: $y = \varnothing$. We will prove $\forall x \in \mathcal{P}_s(b)\,(x \subseteq \varnothing \vee x \not\subseteq \varnothing)$. Assume $x \in \mathcal{P}_s(b)$. We have $x \subseteq \varnothing$ if and only if $x = \varnothing$, so it suffices to prove $x = \varnothing \vee x \neq \varnothing$, but that follows from (39). That completes the base case.

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

$$z \in \mathcal{P}_s(b) \to \forall x \in \mathcal{P}_s(b)\,(x \subseteq z \vee x \not\subseteq z). \tag{40}$$

We have to prove

$$y \in \mathcal{P}_s(b) \to \forall x \in \mathcal{P}_s(b)\,(x \subseteq y \vee x \not\subseteq y). \tag{41}$$

Assume $y \in \mathcal{P}_s(b)$ and $x \in \mathcal{P}_s(b)$. 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

$$\begin{aligned} y &\in \mathcal{P}_s(b) && \text{assumed above,} \\ z \cup \{c\} &\in \mathcal{P}_s(b) && \text{since } y = z \cup \{c\}. \end{aligned}$$

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

I say that also $x - \{c\} \in \mathcal{P}_s(b)$. 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 $x \in \mathcal{P}_s(b)$ 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 $x - \{c\} \in \mathcal{P}_s(b)$, as claimed.

By (40) and $z \in \mathcal{P}_s(b)$, we have

$$\forall x \in \mathcal{P}_s(b)\,(x \subseteq z \vee x \not\subseteq z). \tag{42}$$

Since $x \in \mathcal{P}_s(b)$, 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 (42), instantiated to $x - \{c\}$ in place of x (which is allowed since $x - \{c\} \in \mathcal{P}_s(b)$), 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 (41) follows from the induction hypothesis (40). That completes Case 2. That completes the induction step. □

Lemma 6.14. Suppose a and b are finite sets. Then $a \in \mathcal{P}_s(b) \to \mathcal{P}_s(a) \in \mathcal{P}_s(\mathcal{P}_s(b))$.

Proof. Suppose $a \in \mathcal{P}_s(b)$. By Lemma 6.12,

$$\mathcal{P}_s(a) \subseteq \mathcal{P}_s(b). \tag{43}$$

It remains to show that $\mathcal{P}_s(a)$ is a separable subset of $\mathcal{P}_s(b)$; that is, $\mathcal{P}_s(b) = \mathcal{P}_s(a) \cup (\mathcal{P}_s(b) - \mathcal{P}_s(a))$. By extensionality and the definitions of subset and union, it suffices to show

$$t \in \mathcal{P}_s(b) \leftrightarrow t \in \mathcal{P}_s(a) \vee (t \in \mathcal{P}_s(b) \wedge t \notin \mathcal{P}_s(a)). \tag{44}$$

The right-to-left direction follows logically from (43) and the definition of subset.

Ad the left-to-right direction of (44): suppose $t \in \mathcal{P}_s(b)$. Then $t \subseteq b$. By Lemma 6.13,

$$t \subseteq a \vee t \not\subseteq a. \tag{45}$$

We argue by cases using (45).

Case 1: $t \subseteq a$. It suffices to prove $t \in \mathcal{P}_s(a)$. It remains to prove $a = t \cup (a - t)$. We have

$$\begin{aligned} &\forall u \in b\,(u \in t \vee u \notin t) && \text{since } t \in \mathcal{P}_s(b),\\ &\forall u \in a\,(u \in t \vee u \notin t) && \text{since } a \subseteq b. \end{aligned}$$

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 $t \notin \mathcal{P}_s(a)$. Since $t \in \mathcal{P}_s(b)$, the second disjunct on the right of (44) holds. That completes Case 2. □

Lemma 6.15. For all a and $c \notin a$, we have $\mathcal{P}_1(a \cup \{c\}) = \mathcal{P}_1(a) \cup \{\{c\}\}$.

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

Left to right. Let $x \in \mathcal{P}_1(a \cup \{c\})$. Then $x = \{u\}$ for some $u \in a \cup \{c\}$. Then $u \in a \vee a = c$. If $u \in a$ then $x \in \mathcal{P}_1(a)$ and hence $x \in \mathcal{P}_1(a) \cup \{\{c\}\}$. That completes the left-to-right direction.

Right to left. Let $x \in \mathcal{P}_1(a) \cup \{\{c\}\}$. Then $x \in \mathcal{P}_1(a) \vee x = \{c\}$. If $x \in \mathcal{P}_1(a)$, then $x \in \mathcal{P}_1(a \cup \{c\})$ by Lemma 6.10. If $x = \{c\}$, then $x \in \mathcal{P}_1(a \cup \{c\})$ by definition of $\mathcal{P}_1$. □

Lemma 6.16. For all a, b we have $\mathcal{P}_1(a - b) = \mathcal{P}_1(a) - \mathcal{P}_1(b)$.

Proof. By the definitions of $\mathcal{P}_1$ and set difference, using about 50 straightforward inferences, which we choose to omit. □

Lemma 6.17. $\mathcal{P}_1(\varnothing) = \varnothing$.

Proof. Suppose $x \in \mathcal{P}_1(\varnothing)$. By definition of $\mathcal{P}_1$, there exists $a \in \varnothing$ such that $x = \{a\}$. But that contradicts the definition of $\varnothing$. □

Lemma 6.18. For every x and a, $x \in a \leftrightarrow \{x\} \in \mathcal{P}_1(a)$.

Proof. Left to right. By definition of $\mathcal{P}_1(a)$.

Right to left. If $\{x\} \in \mathcal{P}_1(a)$, then for some $y \in a$, $\{x\} = \{y\}$. Then by extensionality $x = y$. □

Lemma 6.19. $\mathcal{P}_s(\varnothing) = \{\varnothing\}$.

Proof. The only subset of $\varnothing$ is $\varnothing$, and it is a separable subset. □

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

Proof. Let $f\colon a \to b$ be a similarity. Since a is inhabited, there exists some $c \in a$. Fix c. Then $f(c) \in b$. Hence b is inhabited. □

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

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

Remark. This lemma is closely related to Lemma 3.29, and can be derived from that lemma, but here we just prove it directly.

Proof of Lemma 6.21. 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 5.30, $x < 0$ can never hold. That completes the base case.

Induction step. The key fact will be Lemma 5.34:

$$x < y^+ \leftrightarrow x < y \vee x = y. \tag{46}$$

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

$$\begin{aligned}
\forall x\,(x \in \mathbb{F} \to x < y^+ \to \neg\neg x \in P) &\quad \text{assumption,}\\
\forall x\,(x \in \mathbb{F} \to (x < y \vee x = y) \to \neg\neg x \in P) &\quad \text{by (46),}\\
\forall x\,(x \in \mathbb{F} \to (x < y \to \neg\neg x \in P) \wedge (x = y \to \neg\neg x \in P)) &\quad \text{by logic,}\\
\forall x\,(x \in \mathbb{F} \to (x < y \to \neg\neg x \in P)) \wedge \neg\neg y \in P &\quad \text{by logic,}\\
\neg\neg \forall x\,(x \in \mathbb{F} \to (x < y \to x \in P)) \wedge \neg\neg y \in P &\quad \text{by induction hypothesis,}\\
\neg\neg \forall x\,(x \in \mathbb{F} \to x \le y \to x \in P) &\quad \text{by (46).}
\end{aligned}$$

That completes the induction step. □

7 Cardinal exponentiation

Specker [19, Lemma 4.1] follows Rosser in defining 2^m for cardinals m. They define 2^m to be the cardinal of $\mathcal{P}(a)$ where $\mathcal{P}_1(a) \in m$. 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 $\mathcal{P}_s(a)$, the class of separable subsets of a, instead of $\mathcal{P}(a)$.

Definition 7.1. For finite cardinals m, we define $2^m = \{u : \exists a\,(\mathcal{P}_1(a) \in m \wedge u \sim \mathcal{P}_s(a))\}$.

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

Lemma 7.2. Let $m \in \mathbb{F}$ and $\mathcal{P}_1(a) \in m$. Then $\mathcal{P}_s(a) \in 2^m$, and $2^m = |\mathcal{P}_s(a)|$.

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 $\mathcal{P}_1(a)$.

Proof of Lemma 7.2. Suppose $m \in \mathbb{F}$ and $\mathcal{P}_1(a) \in m$. 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 $\mathcal{P}_1(a)$ and $\mathcal{P}_1(b)$ are both in m and $u \sim \mathcal{P}_s(a)$ and $v \sim \mathcal{P}_s(b)$. Then by Lemma 4.9, $\mathcal{P}_1(a) \sim \mathcal{P}_1(b)$. By Lemma 6.7, $a \sim b$. By Lemma 6.8, $\mathcal{P}_s(a) \sim \mathcal{P}_s(b)$. By Lemma 2.11, $u \sim v$. Hence, as claimed, 2^m is a cardinal.

Therefore 2^m and $|\mathcal{P}_s(a)|$ are both closed under similarity. Since they both contain $\mathcal{P}_s(a)$, they each consist of all sets similar to $\mathcal{P}_s(a)$. Hence by extensionality, they are equal. □

Remark. We note that $2^m \neq \varnothing$ does not *prima facie* imply that 2^m is inhabited, so we must carefully distinguish these two statements as hypotheses of lemmas. That is, 2^m is inhabited if m contains a set of the form $\mathcal{P}_1(a)$, and $2^m \neq \varnothing$ means not-not m contains such a set.

Discussion. It is possible, of course, to investigate what happens if we use intuitionistic logic, but keep the classical definitions of order and exponentiation. The most obvious difficulty with this approach is that the integers $\mathbb{F}$ are not closed under exponentiation. For example, let us calculate what 2^{one} would be. We have $\{\{\varnothing\}\} = \mathcal{P}_1(\{\varnothing\}) \in \mathsf{one}$. So 2^{zero} would be the cardinal of $\mathcal{P}(\{\varnothing\})$, instead of the cardinal of $\mathcal{P}_s(\{\varnothing\})$. But $\mathcal{P}(\{\varnothing\})$ contains every set of the form $X_P = \{x : x = \varnothing \wedge P\}$, where P is a stratified formula not containing the variable x. Unless we can prove or refute P, we cannot prove that X_P is one of the two members of $\mathcal{P}_s(\varnothing)$, and in fact there is no hope of proving 2^{one} is an integer. Hence this notion is useless for constructive mathematics in NF. Still we did investigate the matter further, in the hope that this approach might help analyze Specker's proof. In short, it did not help. Without the axiom of choice, one can prove nothing useful about large cardinals. For example, one cannot prove $2^x = 2^y \to x = y$ for cardinals; there might even be incomparable x, y such that $2^x = 2^y$. That might even be the case with $2^x = 2^\kappa = \kappa$, where κ is the cardinal of $\mathbb{V}$. We consider this subject no further.

Lemma 7.3. The graph of the exponentiation function $\{\langle m, 2^m\rangle : m \in \mathbb{F}\}$ is definable in $i\mathsf{NF}$.

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 $2^m = \{u : \exists a\,(\mathcal{P}_1(a) \in m \wedge u \sim \mathcal{P}_s(a))\}$. Stratify it, giving a index 0, $\mathcal{P}_1(a)$ and $\mathcal{P}_s(a)$ 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. □

Lemma 7.4. If 2^m is inhabited, then there exists a such that $\mathcal{P}_1(a) \in m$ and $\mathcal{P}_s(a) \in 2^m$.

Proof. Suppose 2^m is inhabited. Then by Definition 7.1, there exists a with $\mathcal{P}_1(a) \in m$, and 2^m contains any set similar to $\mathcal{P}_s(a)$. Since $\mathcal{P}_s(a) \sim \mathcal{P}_s(a)$, by Lemma 2.11, we have $\mathcal{P}_s(a) \in 2^m$. □

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 $\mathcal{P}_1(a) \in m$ and $\mathcal{P}_s(a) \in 2^m$. Then $|\mathcal{P}_s(a)| = 2^m$, by Definition 7.1. We have

$$\begin{aligned}
\mathcal{P}_1(a) &\in \mathsf{FINITE} && \text{by Lemma 4.4,}\\
a &\in \mathsf{FINITE} && \text{by Lemma 3.11,}\\
\mathcal{P}_s(a) &\in \mathsf{FINITE} && \text{by Lemma 3.18,}\\
|\mathcal{P}_s(a)| &\in \mathbb{F} && \text{by Lemma 4.20,}\\
2^m &\in \mathbb{F} && \text{since } |\mathcal{P}_s(a)| = 2^m.
\end{aligned}$$

□

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

Proof. Since $\mathsf{zero} = \{\varnothing\}$, it contains $\varnothing = \mathcal{P}_1(\varnothing)$. Hence 2^{zero} is inhabited and contains $\mathcal{P}_s(\varnothing)$. But $\varnothing$ has only one subset, namely $\varnothing$, which is a separable subset, so $\mathcal{P}_s(\varnothing) = \{\varnothing\} = \mathsf{zero}$. Thus $2^{\mathsf{zero}} = |\mathsf{zero}| = \mathsf{one}$. □

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

Proof. Since one is the set of all singletons, it contains $\{\mathsf{zero}\} = \mathcal{P}_1(\mathsf{zero})$. Then 2^{one} contains $\mathcal{P}_s(\mathsf{zero})$. There are exactly two subsets of $\{\varnothing\}$, namely $\varnothing$ and $\{\varnothing\}$, and both are separable. Hence 2^{one} contains the two-element set $\mathcal{P}_s(\mathsf{zero}) = \{\varnothing, \{\varnothing\}\}$. That set belongs to $\mathsf{two} = \mathsf{one}^+$ since it is equal to $\{\{\varnothing\}\} \cup \{\varnothing\}$, and the singleton $\{\{\varnothing\}\}$ belongs to one and $\{\varnothing\} \notin \{\{\varnothing\}\}$. Therefore 2^{one} and one^+ have a common element. Both are cardinals, by Lemma 7.5. Then by Lemma 4.23, $2^{\mathsf{one}} = \mathsf{two}$. □

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 $\mathcal{P}_1(\{\mathsf{one}, \mathsf{two}\}) = \{\{\mathsf{one}\}, \{\mathsf{two}\}\} \in \mathsf{two}$. Therefore, by the definition of exponentiation,

$$\mathcal{P}_s(\{\mathsf{one}, \mathsf{two}\}) = \{\varnothing, \{\mathsf{one}\}, \{\mathsf{two}\}, \{\mathsf{one}, \mathsf{two}\}\} \in 2^{\mathsf{two}}.$$

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

Lemma 7.9. $u \in \mathsf{two} \leftrightarrow \exists a, b\,(a \neq b \wedge u = \{a, b\})$.

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 $u = \{a, b\}$. □

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 $\mathsf{three} = \mathsf{two}^+$, $\{a, b\} \cup \{c\} = \{a, b, c\} \in \mathsf{three}$. 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. □

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

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 5.38. □

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 5.17, $m < \mathsf{zero} \vee m = \mathsf{zero} \vee \mathsf{zero} < m$. By Lemma 5.30, $m < \mathsf{zero}$ is ruled out. It remains to rule out $\mathsf{zero} < m$. Assume $\mathsf{zero} < m$. Then

$$\begin{array}{rl}
m < \mathsf{one} & \text{by hypothesis,} \\
m^+ \leq \mathsf{one} & \text{by Lemma 5.31,} \\
m^+ \leq \mathsf{zero}^+ & \text{since } \mathsf{zero}^+ = \mathsf{one}, \\
m \leq \mathsf{zero} & \text{by Lemma 5.10,} \\
\mathsf{zero} < \mathsf{zero} & \text{by Lemma 5.22, since } \mathsf{zero} \leq m < \mathsf{zero}, \\
\mathsf{zero} \not< \mathsf{zero} & \text{by Lemma 5.30.}
\end{array}$$

□

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

$$\begin{array}{rl}
\mathsf{zero} \neq \mathsf{one} & \text{by Lemma 5.37,} \\
\{\mathsf{zero}, \mathsf{one}\} \in \mathsf{two} & \text{by Lemma 7.9,} \\
m \leq \mathsf{two} & \text{by Definition 5.2,} \\
a \in m \wedge a \in \mathcal{P}_s(\{\mathsf{zero}, \mathsf{one}\}) & \text{for some } a\text{, by Lemma 5.8,} \\
a \neq \{\mathsf{zero}, \mathsf{one}\} & \text{since } m \neq \mathsf{two}, \\
\mathsf{zero} \in a \vee \mathsf{zero} \notin a & \text{since } a \in \mathcal{P}_s(\{\mathsf{zero}, \mathsf{one}\}), \\
\mathsf{one} \in a \vee \mathsf{one} \notin a & \text{since } a \in \mathcal{P}_s(\{\mathsf{zero}, \mathsf{one}\}).
\end{array}$$

An argument by cases (about 170 steps, which we omit) shows that $a = \varnothing$, or $a = \{\mathsf{zero}\}$, or $a = \{\mathsf{one}\}$. Then $a = \mathsf{zero}$ or one, by Lemma 4.23. 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. □

Lemma 7.14. For all a, a is a unit class if and only if $\mathcal{P}_1(a)$ is a unit class.

Proof. Left to right. Suppose $a = \{x\}$. Then the only unit subset of a is $\{a\}$, so $\mathcal{P}_1(a)$ is a unit class.

Right to left. Suppose $\mathcal{P}_1(a) = \{u\}$. Then $u \in a$. Let $t \in a$. Then $\{t\} \in \mathcal{P}_1(a)$, so $\{t\} = u$. Hence every element of a is equal to u. Hence $a = \{u\}$. □

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

$$\begin{aligned} b &= \varnothing && \text{by definition of zero,} \\ a &= \varnothing && \text{since } a \subseteq b, \\ \varnothing &\in x \cap \mathsf{zero} && \text{by definition of } \cap, \\ x &= \mathsf{zero} && \text{by Lemma 4.23.} \end{aligned}$$

□

Lemma 7.16 (Specker, [19, Lemma 4.6])**.** If m is a finite cardinal and 2^m is inhabited, then $m < 2^m$.

Remark. This version of [19, Lemma 4.6] phrases the matter positively, so it is constructively stronger.

Proof of Lemma 7.16. Since $\mathbb{F}$ has decidable equality, by Corollary 5.18

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

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 $\varnothing$ of the set $\{\varnothing\}$, and noting that $\varnothing \in \mathsf{zero}$, while $\{\varnothing\} \in \mathsf{one}$.

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 5.10, or more directly, from the definition of $<$ by exhibiting the separable subset $\{\varnothing\}$ of $\{\{\varnothing\}, \varnothing\}$, 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 $\mathcal{P}_1(a) \in m$. Since $m \in \mathbb{F}$, we have

$$\begin{aligned} \mathcal{P}_1(a) &\in \mathsf{FINITE} && \text{by Lemma 4.4,} \\ a &\in \mathsf{FINITE} && \text{by Lemma 3.11,} \\ \mathcal{P}_s(a) &\in \mathsf{FINITE} && \text{by Lemma 3.18,} \\ a &\in \mathsf{DECIDABLE} && \text{by Lemma 3.3.} \end{aligned}$$

Then by Lemma 3.19, $\mathcal{P}_1(a)$ is a separable subset of $\mathcal{P}_s(a)$. Now with $u = \mathcal{P}_1(a)$ and $v = \mathcal{P}_s(a)$ 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 $\mathcal{P}_1(a) \subseteq \mathcal{P}_s(a)$. I say that it is a proper subset, $\mathcal{P}_1(a) \subset \mathcal{P}_s(a)$. It suffices to prove $\mathcal{P}_1(a) \ne \mathcal{P}_s(a)$. We have to produce an element of $\mathcal{P}_s(a)$ that does not belong to $\mathcal{P}_1(a)$. We propose a as this element. We have $a \in \mathcal{P}_s(a)$ since a is a separable subset of itself. It remains to show that $a \notin \mathcal{P}_1(a)$. Assume $a \in \mathcal{P}_1(a)$. Then a is a unit class. By Lemma 7.14, $\mathcal{P}_1(a)$ is also a unit class. Any two unit classes are similar, so $\mathcal{P}_1(a) \sim \mathsf{zero}$. Since $\mathsf{zero} \in \mathsf{one}$, $\mathcal{P}_1(a) \in \mathsf{one}$, by Lemma 4.8. Then $m \cap \mathsf{one}$ is inhabited, since it contains $\mathcal{P}_1(a)$. Then by Lemma 4.23, $m = \mathsf{one}$, contradiction. That completes the proof that $\mathcal{P}_1(a)$ is a proper subset of $\mathcal{P}_s(a)$.

We have

$$\begin{aligned} \mathcal{P}_1(a) &\subset \mathcal{P}_s(a) && \text{as proved above,} \\ \mathcal{P}_1(a) &\sim \mathcal{P}_s(a) && \text{by Lemma 4.9, since } \mathcal{P}_1(a) \in m \text{ and } \mathcal{P}_s(a) \in 2^m, \\ \mathcal{P}_s(a) &\text{ is infinite} && \text{since } \mathcal{P}_s(a) \sim \mathcal{P}_1(a) \subset \mathcal{P}_s(a), \\ \neg\,(\mathcal{P}_s(a) &\in \mathsf{FINITE}) && \text{by Theorem 3.25,} \\ \mathcal{P}_s(a) &\in \mathsf{FINITE} && \text{by Lemma 3.18, since } a \in \mathsf{FINITE}. \end{aligned}$$

That is a contradiction. □

Lemma 7.17. For all $m \in \mathbb{F}$, we have $\exists u\,(u \in 2^m) \to m^+ \leq 2^m$.

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

$$\begin{aligned} m &< 2^m && \text{by Lemma 7.16,} \\ 2^m &\in \mathbb{F} && \text{by Lemma 7.5,} \\ m^+ &\leq 2^m && \text{by Lemma 5.31.} \end{aligned}$$

□

Lemma 7.18 (Specker, [19, Lemma 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

$$\begin{aligned} \exists u\,(u \in n) && \text{by Corollary 4.7,} \\ \exists b\,(\mathcal{P}_1(b) \in n) && \text{by Lemma 7.4,} \\ \exists b\,(\mathcal{P}_1(b) \in m) && \text{by Lemma 7.4.} \end{aligned}$$

Since $m \leq n$, by Lemma 5.8 there is a separable subset x of $\mathcal{P}_1(b)$ such that $x \in m$. Let $a = \bigcup x$. Then using the definitions of $\bigcup$ and $\mathcal{P}_1$, we have $x = \mathcal{P}_1(a)$. Therefore 2^m is inhabited. Now $2^m = |\mathcal{P}_s(a)|$ and $2^n = |\mathcal{P}_s(b)|$.

I say that b is finite. We have

$$\begin{aligned} \mathcal{P}_1(b) &\in n, \\ \mathcal{P}_1(b) &\in \mathsf{FINITE} && \text{by Lemma 4.4,} \\ b &\in \mathsf{FINITE} && \text{by Lemma 3.11.} \end{aligned}$$

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 $x = \mathcal{P}_1(a)$). 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 3.26.

Since $x = \mathcal{P}_1(a)$ is a separable subset of $\mathcal{P}_1(b)$, we have

$$\begin{aligned} \mathcal{P}_1(a) &\in \mathcal{P}_s(\mathcal{P}_1(b)), \\ a &\in \mathcal{P}_s(b) && \text{by Lemma 6.11 (right to left),} \\ \mathcal{P}_s(a) &\in \mathcal{P}_s(\mathcal{P}_s(b)) && \text{by Lemma 6.14, since } a \text{ and } b \text{ are finite.} \end{aligned}$$

Then $\mathcal{P}_s(a)$ belongs to 2^m, and is a separable subset of $\mathcal{P}_s(b)$, which belongs to 2^n. Therefore, by Definition 5.2, $2^m \leq 2^n$. □

8 Addition

Specker uses addition in [19, § 5], 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, [19, Lemma 3.1]; Rosser, [18, Theorem XI.2.9])**.** For any sets x and y we define $x + y := \{z : \exists u, v\, (u \in x \wedge v \in y \wedge u \cap v = \varnothing \wedge z = u \cup v)\}$.

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 $i\mathsf{NF}$. (See Definition 2.2 for ordered triples.)

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

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

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

Proof of Lemma 8.2. 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 $\mathsf{zero} = \{\varnothing\}$, we have $v = \lambda$, so $z = u \cup \varnothing = u \in x$. That completes the left-to-right implication.

Right to left. Let $z \in x$. Then $z \cup \varnothing \in x + \mathsf{zero}$, by the definition of addition. Since $z \cup \varnothing = z$, 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

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

That completes the left-to-right implication.

Right to left. We have

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

That completes the proof of the right-to-left implication. 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. We have

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

That completes the left-to-right direction.

Right to left. We have

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

That completes the right-to-left direction. □

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

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

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 $\varnothing$.

Proof of Lemma 8.3. 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

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

□

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

Proof. We have

$$\begin{aligned} \mathsf{two} &= \mathsf{one}^+ && \text{by definition of } \mathsf{two}, \\ \mathsf{two} &= \mathsf{one} + \mathsf{one} && \text{by Lemma 8.4.} \end{aligned}$$

□

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 of Lemma 8.6. By induction on μ, which is legal since the formula is stratified.

Base case. We have $\kappa + \mathsf{zero} = \kappa$ 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. □

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 of Lemma 8.8. 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 $a \cap b = \varnothing$. By definition of successor, $b = x \cup \{c\}$ for some x and c, so $c \in b$. Since $a \cap b = \varnothing$, we have $c \notin a$. Then $a \cup \{c\} \in p^+$. Then $p^+ \in \mathbb{F}$. □

Lemma 8.9. If $p, q \in \mathbb{F}$ and $p + q^+ \in \mathbb{F}$, then $p + q \in \mathbb{F}$.

Proof. We have

$$\begin{aligned} p + q^+ &\in \mathbb{F} && \text{by hypothesis}, \\ p + q + \mathsf{one} &\in \mathbb{F} && \text{by definition of } \mathsf{one} \text{ and Lemma 8.2}, \\ p + q &\in \mathbb{F} && \text{by Lemma 8.7.} \end{aligned}$$

□

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 $w \in b + q$ for some w, by Corollary 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 $u \cap v = \varnothing$. By Lemma 5.8, since $a \le b$ there exists $r \in a$ with $r \in \mathcal{P}_s(u)$. By Lemma 5.8, since $p \le q$, there exists $s \in p$ with $s \in \mathcal{P}_s(v)$. Then one can verify that $r \cup s \in \mathcal{P}_s(u \cup v)$. (We omit the details of that verification.) Since $u \cup v = w$ we have $r \cup s \in \mathcal{P}_s(w)$. We have $r \cap s = \varnothing$, since $r \subseteq u$, $s \subseteq v$, and $u \cap v = \varnothing$. Then $r \cup s \in a + p$, by the definition of addition. Then $a + p \le b + q$, as witnessed by $r \cup s \in a + p$, $r \cup s \in \mathcal{P}_s(w)$, and $w \in b + q$. □

Lemma 8.11. For $a, p, b, q \in \mathbb{F}$, if $b + q \in \mathbb{F}$ we have $a < b \wedge p \le q \to a + p < b + q$.

Remark. It is not assumed that $a + p \in \mathbb{F}$, which would make the proof easier.

Proof of Lemma 8.11. Suppose $a < b$ and $p \le q$. Then

$$
\begin{aligned}
a^+ &\le b && \text{by Lemma 5.31,}\\
\exists u\,(u \in a^+) &&& \text{by the definition of addition,}\\
a^+ &\in \mathbb{F} && \text{by Lemma 4.19,}\\
a^+ + p &\le b + q && \text{by Lemma 8.10,}\\
(a+p)^+ &\le b + q && \text{by Lemma 8.3,}\\
\exists u\,(u \in (a+p)^+) &&& \text{by the definition of } \le,\\
\exists u\,(u \in a + p) &&& \text{by definition of successor,}\\
a + p &\in \mathbb{F} && \text{by Lemma 8.6,}\\
(a+p)^+ &\in \mathbb{F} && \text{by Lemma 4.19,}\\
a + p &< (a+p)^+ && \text{by Lemma 5.38,}\\
a + p &< b + q && \text{by Lemma 5.22.}
\end{aligned}
$$

□

Lemma 8.12. For $m \in \mathbb{F}$ we have $\mathcal{P}_1(x) \in m \to \mathcal{P}_s(x) \in 2^m$.

Proof. Suppose $\mathcal{P}_1(x) \in m$. By Definition 7.1, 2^m contains all sets similar to $\mathcal{P}_s(x)$. By Lemma 2.11, $\mathcal{P}_s(x)$ is one of those sets, so $\mathcal{P}_s(x) \in 2^m$. □

Lemma 8.13. For all z we have $2^z \ne \mathsf{zero}$.

Proof. Suppose $2^z = \mathsf{zero}$. Then

$$
\begin{aligned}
\varnothing &\in \mathsf{zero} && \text{by Definition 5.14,}\\
\varnothing &\in 2^z && \text{since } 2^z = \mathsf{zero},\\
\varnothing &\sim \mathcal{P}_s(a) \wedge \mathcal{P}_1(a) \in x && \text{by Definition 7.1,}\\
\mathcal{P}_s(a) &= \varnothing && \text{since only } \varnothing \text{ is similar to } \varnothing.
\end{aligned}
$$

But $a \in \mathcal{P}_s(a)$, contradiction. □

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 $|p \cup q| = |p| + |q|$.

Proof. We have

$$\begin{aligned}
p \cup q \in \mathsf{FINITE} &\quad \text{by Lemma 3.12,}\\
|p \cup q| \in \mathbb{F} &\quad \text{by Lemma 4.20,}\\
|p| \in \mathbb{F} &\quad \text{by Lemma 4.20,}\\
|q| \in \mathbb{F} &\quad \text{by Lemma 4.20,}\\
p \cup q \in |p \cup q| &\quad \text{by Lemma 4.11,}\\
p \in |p| &\quad \text{by Lemma 4.11,}\\
q \in |q| &\quad \text{by Lemma 4.11,}\\
p \cup q \in |p| + |q| &\quad \text{by the definition of addition,}\\
|p \cup q| \cap |p| + |q| \neq \varnothing &\quad \text{since both contain } p \cup q,\\
|p| + |q| \in \mathbb{F} &\quad \text{by Lemma 8.6,}\\
|p \cup q| = |p| + |q| &\quad \text{by Lemma 4.23.}
\end{aligned}$$

□

Lemma 8.16. For $p, q, r \in \mathbb{F}$, if $q + p \in \mathbb{F}$ we have

$$\begin{aligned}
&q + p = r + p \to q = r,\\
&p + q = p + r \to q = r.
\end{aligned}$$

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

$$\begin{aligned}
(q+p)^+ = (r+p)^+ &\quad \text{by Lemma 8.2,}\\
q + p \in \mathbb{F} &\quad \text{by Lemma 8.9,}\\
r + p \in \mathbb{F} &\quad \text{by Lemma 8.9,}\\
\exists u\,(u \in q + p) &\quad \text{by Corollary 4.7,}\\
\exists u\,(u \in r + p) &\quad \text{by Corollary 4.7,}\\
(q+p)^+ = q + p^+ &\quad \text{by Lemma 8.2,}\\
(r+p)^+ = r + p^+ &\quad \text{by Lemma 8.2,}\\
(q+p)^+ \in \mathbb{F} &\quad \text{equality substitution,}\\
(r+p)^+ \in \mathbb{F} &\quad \text{equality substitution,}\\
\exists u\,(u \in (q+p)^+) &\quad \text{by Corollary 4.7,}\\
\exists u\,(u \in (r+p)^+) &\quad \text{by Corollary 4.7,}\\
q + p = r + p &\quad \text{by Lemma 5.11, since } (q+p)^+ = (r+p)^+,\\
q = r &\quad \text{by the induction hypothesis.}
\end{aligned}$$

That completes the induction step. □

Lemma 8.17. Let $b \in \mathsf{FINITE}$ and $c \notin b$. Then $|\mathcal{P}_s(b \cup \{c\})| = |\mathcal{P}_s(b)| + |\mathcal{P}_s(b)|$.

Proof. Define $R := \{x \cup \{c\} : x \in \mathcal{P}_s(b)\}$. The definition can be rewritten in stratified form, so R can be defined in $i\mathsf{NF}$. Define $f\colon x \mapsto x \cup \{c\}$, which can also be defined in $i\mathsf{NF}$: $f := \{\langle x, x \cup \{c\}\rangle : x \in \mathcal{P}_s(b)\}$. The formula is stratified, since all the occurrences of x can be given index 0, and $\{c\}$ and $\mathcal{P}_s(b)$ are just parameters. Then $f\colon \mathcal{P}_s(b) \to R$ is a similarity. (We omit the 150 steps required to prove that.)

We first note that if $x \in \mathcal{P}_s(b \cup \{c\})$ 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 $x \in \mathcal{P}_s(b \cup \{c\})$ either contains c or not. If $c \in x$ then $x \in R$. If $c \notin x$ then $x \in \mathcal{P}_s(b)$. Therefore

$$
\begin{aligned}
\mathcal{P}_s(b \cup \{c\}) &= \mathcal{P}_s(b) \cup R, \\
\mathcal{P}_s(b) &\sim R && \text{since } f\colon \mathcal{P}_s(b) \to R \text{ is a similarity,} \\
|\mathcal{P}_s(b)| &= |R| && \text{by Lemma 4.12,} \\
\mathcal{P}_s(b) \cap R &= \varnothing && \text{since } c \notin b, \\
\mathcal{P}_s(b) &\in \mathsf{FINITE} && \text{by Lemma 3.18,} \\
R &\in \mathsf{FINITE} && \text{by Lemma 3.15,} \\
|\mathcal{P}_s(b \cup \{c\})| &= |\mathcal{P}_s(b)| + |R| && \text{by Lemma 8.15,} \\
|\mathcal{P}_s(b \cup \{c\})| &= |\mathcal{P}_s(b)| + |\mathcal{P}_s(b)| && \text{since } |\mathcal{P}_s(b)| = |R|.
\end{aligned}
$$

□

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

$$
\begin{aligned}
\exists u\,\big(u \in 2^{p^+}\big) && \text{by Corollary 4.7,} \\
\mathcal{P}_1(a) \in p^+ && \text{for some } a \in p, \text{ by the definition of exponentiation,} \\
u \in p^+ \wedge q \in u && \text{for some } q, u, \text{ by Lemma 4.15,} \\
u \sim \mathcal{P}_1(a) && \text{by Lemma 4.9, since both are in } p^+, \\
w \in \mathcal{P}_1(a) && \text{for some } w, \text{ by Lemma 6.20,} \\
c \in a \wedge w = \{c\}; && \text{for some } c, \text{ by the definition of } \mathcal{P}_1(a), \\
\mathcal{P}_1(a) \in \mathsf{FINITE} && \text{by Lemma 4.4,} \\
a \in \mathsf{FINITE} && \text{by Lemma 3.11,} \\
a \in \mathsf{DECIDABLE} && \text{by Lemma 3.3,} \\
b := a - \{c\} && \text{definition of } b, \\
a = b \cup \{c\} && \text{since } a \in \mathsf{DECIDABLE}, && (47) \\
\mathcal{P}_1(a) = \mathcal{P}_1(b) \cup \{\{c\}\} && \text{by Lemma 6.15,} \\
\mathcal{P}_s(b \cup \{c\}) \in 2^{p^+} && \text{by the definition of exponentiation,} \\
|\mathcal{P}_s(b \cup \{c\})| = 2^{p^+} && \text{by Lemma 4.11,} \\
|\mathcal{P}_s(b \cup \{c\})| = |\mathcal{P}_s(b)| + |\mathcal{P}_s(b)| && \text{by Lemma 8.17,} && (48) \\
\mathcal{P}_1(a) \in \mathsf{DECIDABLE} && \text{by Lemma 3.3,} \\
\mathcal{P}_1(b) = \mathcal{P}_1(a) - \{\{c\}\} && \text{since } \mathcal{P}_1(a) \in \mathsf{DECIDABLE}, \\
\mathcal{P}_1(b) \in p && \text{by Lemma 5.9,} \\
\mathcal{P}_s(b) \in 2^p && \text{by the definition of exponentiation,} \\
\mathcal{P}_s(b) \in |\mathcal{P}_s(b)| && \text{by Lemma 4.11,}
\end{aligned}
$$

$$\begin{array}{rl} \mathcal{P}_s(b) \in \mathsf{FINITE} & \text{by Lemma 3.18,} \\ |\mathcal{P}_s(b)| \in \mathbb{F} & \text{by Lemma 4.20,} \\ |\mathcal{P}_s(b)| = 2^p & \text{by Lemma 4.23.} \end{array}$$

Then $2^{p^+} = 2^p + 2^p$ as desired, by (48). □

Lemma 8.19. For $m \in \mathbb{F}$, $2^m = \mathsf{one} \leftrightarrow m = \mathsf{zero}$.

Proof. Left to right. We have

$$\begin{array}{rl} 2^m = \mathsf{one} & \text{assumption,} \\ 2^{\mathsf{two}} = \mathsf{four} & \text{by Lemma 7.8,} \\ \mathsf{two} \le m \to 2^{\mathsf{two}} \le 2^m & \text{by Lemma 7.18,} \\ \mathsf{two} \le m \to \mathsf{four} \le \mathsf{one} & \text{by transitivity of } \le, \\ \mathsf{one} < \mathsf{four} & \text{by Lemma 7.11,} \\ \mathsf{two} \not\le m & \text{otherwise } \mathsf{one} < \mathsf{four} \wedge \mathsf{four} \le \mathsf{one}, \\ m < \mathsf{two} \vee \mathsf{two} \le m & \text{by Theorem 5.17,} \\ m < \mathsf{two} & \text{since } \mathsf{two} \not\le m, \\ m = \mathsf{zero} \vee m = \mathsf{one} & \text{by Lemma 7.13,} \\ 2^{\mathsf{one}} = \mathsf{two} & \text{by Lemma 7.7,} \\ \mathsf{one} \ne \mathsf{two} & \text{by Lemma 5.37,} \\ m \ne \mathsf{one} & \text{since } 2^m = \mathsf{zero}, \\ m = \mathsf{zero} & \text{since } m = \mathsf{zero} \vee m = \mathsf{one} \text{ but } m \ne \mathsf{one}. \end{array}$$

Right to left. Suppose $m = \mathsf{zero}$. Then $2^m = 2^{\mathsf{zero}} = \mathsf{one}$, by Lemma 7.6. □

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 of Lemma 8.20. We prove by induction on n that for $n \in \mathbb{F}$ with 2^n inhabited, we have

$$\exists u\,(u \in 2^n) \to \forall m \in \mathbb{F}\,(2^n = 2^m \to n = m).$$

The formula is stratified giving n and m both index 0, so it is legal to proceed by induction.

Base case. This follows from Lemma 8.19.

Induction step. Suppose $2^{n^+} = 2^m$ and n^+ is inhabited. We have $m = \mathsf{zero} \vee m \ne \mathsf{zero}$, by Corollary 5.18.

Case 1: $m = \mathsf{zero}$. Then by Lemma 8.19, $n^+ = \mathsf{zero}$, contradiction.

Case 2: $m \ne \mathsf{zero}$. Then

$$\begin{array}{rl} \exists r \in \mathbb{F}\,(m = r^+) & \text{by Lemma 4.17,} \\ 2^{n^+} = 2^{r^+} & \text{since } 2^{n^+} = 2^m, \\ 2^n + 2^n = 2^r + 2^r & \text{by Lemma 8.18,} \\ r < n \vee r = n \vee n < r & \text{by Theorem 5.17.} \end{array}$$

We argue by cases.

Case 2a: $r < n$. Then

$$\begin{aligned}
2^r &\le 2^n && \text{by Lemma 7.18,}\\
2^r &\ne 2^n && \text{by the induction hypothesis,}\\
2^r &< 2^n && \text{by the definition of } <,\\
2^{n^+} &\in \mathbb{F} && \text{by Lemma 7.5,}\\
2^{r^+} &= 2^r + 2^r && \text{by Lemma 8.18,}\\
2^r + 2^r &< 2^n + 2^n && \text{by Lemma 8.11,}\\
2^n + 2^n &= 2^{n+} && \text{by Lemma 8.18,}\\
2^{r^+} &< 2^{n+} && \text{by Lemma 5.22.}
\end{aligned}$$

But that contradicts $2^{n^+} = 2^{r^+}$. That completes Case 2a.

Case 2b: $n < r$. This similarly leads to a contradiction. We omit the steps.

Case 2c: $n = r$. 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. □

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

$$\begin{aligned}
m &\le n && \text{by the definition of } <,\\
2^m &\le 2^n && \text{by Lemma 7.18,}\\
m &\ne n && \text{by the definition of } <,\\
2^m &\ne 2^n && \text{by Lemma 8.20,}\\
2^m &< 2^n && \text{by the definition of } <.
\end{aligned}$$

□

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. We have to prove $p \le \mathsf{zero} \leftrightarrow \exists k \in \mathbb{F}, p + k = \mathsf{zero}$.

Left to right. Suppose $p \le \mathsf{zero}$. Then $p = \mathsf{zero} \vee p < \mathsf{zero}$, by Lemma 5.20. But $p \not< \mathsf{zero}$ by Lemma 5.30. 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 exist sets $a \in p$ and $b \in k$ such that $a \cup b \in \mathsf{zero}$. By definition of zero, $\mathsf{zero} = \{\varnothing\}$, so $a \cup b = \varnothing$. Then $a = \varnothing$. Then $\varnothing \in p$ and $\varnothing \in \mathsf{zero}$. Then by Lemma 4.23, $p = \mathsf{zero}$. 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 5.33.

Case 1: $p \le q$. Then by the induction hypothesis, there exists $k \in \mathbb{F}$ such that $p + k = q$. We have

$$\begin{aligned}
\exists u\,(u \in q^+) && \text{by hypothesis,}\\
\exists u\, u \in (p + k)^+ && \text{since } p + k = q,\\
p + (k^+) = (p + k)^+ = q^+ && \text{by Lemma 8.2,}\\
\exists u\,(u \in k^+) && \text{by the definition of addition,}\\
k^+ \in \mathbb{F} && \text{by Lemma 4.19.}
\end{aligned}$$

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 $a \cap b = \varnothing$ 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. □

Lemma 8.23. 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

$$\begin{aligned}
u &\in q && \text{for some } u\text{, by Corollary 4.7,}\\
\varnothing &\in \mathsf{zero} && \text{by the definition of } \mathsf{zero},\\
\varnothing \subseteq u \wedge u &= \varnothing \cup (u - \varnothing) && \text{by the definitions of subset and difference,}\\
\mathsf{zero} &\le q && \text{by the definition of } \le,\\
p &\le p && \text{by Lemma 5.19,}\\
p + \mathsf{zero} &\le p + q && \text{by Lemma 8.10,}\\
p &\le p + q && \text{by Lemma 8.2.}
\end{aligned}$$

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 $q \le p + q$. □

Lemma 8.24. Let $p \in \mathbb{F}$. Then $p \ne \mathsf{zero} \to p \ne \mathsf{one} \to 2^p \in \mathbb{F} \to p^+ < 2^p$.

Remark. Specker [19, Lemma 4.6] says $p < 2^p$. Of course the exponent grows faster than linearly, so larger things can be put on the left side, at the price of small exceptions.

Proof of Lemma 8.24. By induction on p. For the base case, there is nothing to prove. For the induction step, assume p^+ is inhabited and $2^{p^+} \in \mathbb{F}$ and $p^+ \ne \mathsf{zero}$ and $p^+ \ne \mathsf{one}$. We have to prove

$$p^{++} < 2^{p^+}. \tag{49}$$

We have $p \ne \mathsf{zero}$ since $p^+ \ne \mathsf{one}$. Since equality on $\mathbb{F}$ is decidable, $p = \mathsf{one} \vee p \ne \mathsf{one}$. We argue by cases.

Case 1: $p = \mathsf{one}$. Then

$$\begin{aligned}
p^{++} = \mathsf{two}^+ &= \mathsf{three} && \text{by definitions of } \mathsf{two} \text{ and } \mathsf{three},\\
2^{p^+} &= \mathsf{four} && \text{by Lemma 7.8,}\\
\mathsf{three} &< \mathsf{four} && \text{by Lemma 5.38,}\\
p^{++} &< 2^{p+} && \text{since } p^{++} = \mathsf{three} \text{ and } 2^{p^+} = \mathsf{four}.
\end{aligned}$$

That completes the case $p = \mathsf{one}$.

Case 2: $p \ne \mathsf{one}$. Then

$$\begin{aligned}
p &\ne \mathsf{zero} && \text{since } p^+ \ne \mathsf{one} \text{ by hypothesis,} && (50)\\
2^{p^+} &\in \mathbb{F} && \text{by hypothesis,}\\
2^{p^+} &= 2^p + 2^p && \text{by Lemma 8.18,} && (51)\\
p^+ &\in \mathbb{F} && \text{by Lemma 4.19,}\\
2^p &< 2^{p+} && \text{by Lemma 8.21, since } 2^{p^+} \in \mathbb{F} \text{ and } p < p^+,\\
2^p &\in \mathbb{F} && \text{by Lemma 7.5, since it is inhabited,} && (52)
\end{aligned}$$

$$
\begin{array}{rl}
p^+ < 2^p & \text{by the induction hypothesis and (50) and (52),} \\
p^+ + p^+ < 2^p + 2^p & \text{by Lemma 8.11,} \\
p^+ + p^+ < 2^{p^+} & \text{by (51),} \\
p^{++} + p < 2^{p^+} & \text{by the law } x + y^+ = x^+ + y, \\
p^{++} \le p^{++} + p & \text{by Lemma 8.23,} \\
p^{++} \text{ is inhabited} & \text{by the definitions of } \le \text{ and addition,} \\
p^{++} \in \mathbb{F} & \text{by Lemma 4.19,} \\
p^{++} + p \in \mathbb{F} & \text{by the definition of } \le \text{ and Lemma 8.6,} \\
p^{++} < 2^{p^+} & \text{by Lemma 5.25.}
\end{array}
$$

But that is (49), the desired goal. That completes the induction step. □

Lemma 8.25. Let $q \in \mathbb{F}$. Then for all $n \in \mathbb{F}$ and $p \in \mathbb{F}$, $n = p + q \to \mathsf{zero} < q \to p < n$.

Remark. This lemma links addition and order. It probably can be proved directly from the definitions of addition and order, but here we prove it by induction. Nevertheless we do have to use the definition of addition directly at one of the steps.

Proof of Lemma 8.25. By induction on q, which is legal since the formula is stratified. The formula to be proved includes the quantifiers on n and p.

Base case. There is nothing to prove because of the hypothesis $q \neq \mathsf{zero}$.

Induction step. Suppose $n = p + q^+$ and $\mathsf{zero} < q^+$. As usual in induction proofs, we also assume q^+ is inhabited. Then

$$
\begin{array}{rl}
n = p^+ + q & \text{by Lemma 8.2,} \\
q < \mathsf{zero} \vee q = \mathsf{zero} \vee \mathsf{zero} < q & \text{by Theorem 5.17.}
\end{array}
$$

Case 1: $q < \mathsf{zero}$. This is impossible, by Lemma 5.30.

Case 2: $q = \mathsf{zero}$. Then $q^+ = \mathsf{one}$ so $n = p + \mathsf{one} = p^+$. Then $p < n$ by Lemma 5.38.

Case 3: $\mathsf{zero} < q$. Then

$$
\begin{array}{rl}
n \text{ is inhabited} & \text{by Corollary 4.7,} \\
p^+ \text{ is inhabited} & \text{by the definition of addition, since } n\ p^+ q, \\
p^+ < n & \text{by the induction hypothesis, since } n = p^+ + q, \\
p < p^+ & \text{by Lemma 5.38,} \\
p < n & \text{by transitivity.}
\end{array}
$$

That completes the induction step. □

Lemma 8.26. Let X and Y be finite sets with $X \subseteq Y$ and $Y - X \neq \varnothing$. Then $|X| < |Y|$.

Remarks.

(1) Of course this is not true without the finiteness hypotheses.
(2) The lemma does not mention addition, but the proof uses it; hence its placement in the section on addition.

Proof of Lemma 8.26. We have

$$\begin{aligned}
Y = X \cup (Y - X) &\quad \text{by Lemma 3.19,}\\
Y - X \in |Y - X| &\quad \text{by Lemma 4.11,}\\
\mathsf{zero} = \{\varnothing\} &\quad \text{by definition of } \mathsf{zero},\\
\mathsf{zero} \neq |Y - X| &\quad \text{since } Y - X \neq \varnothing,\\
Y - X \in \mathsf{FINITE} &\quad \text{by Lemma 3.21,}\\
|Y - X| \in \mathbb{F} &\quad \text{by Lemma 4.20,}\\
\neg\,(|Y - X| < \mathsf{zero}) &\quad \text{by Lemma 5.30,}\\
\mathsf{zero} < |Y - X| &\quad \text{by Theorem 5.17,}\\
X \cap (Y - X) = \varnothing &\quad \text{by the definitions of } - \text{ and } \cap,\\
|Y| = |X| + |Y - X| &\quad \text{by Lemma 8.15, since } Y = X \cup (Y - X),\\
|X| < |Y| &\quad \text{by Lemma 8.25.}
\end{aligned}$$

□

9 Definition of multiplication

Specker did not make any use of multiplication. If one could manage to prove that $\mathbb{F}$ is infinite, one would need multiplication to interpret HA in iNF. But without knowing that $\mathbb{F}$ is infinite, there are technical difficulties with multiplication. 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. We carried out those details (and they can still be found in earlier versions of this paper on arXiv [3]), but we have not included them here.

10 Results about $\mathbb{T}$

Here we constructivize Specker's [19, § 5].

Definition 10.1. $\mathbb{T}(\kappa) = \mathbb{T}\kappa = \{u : \exists x\,(x \in \kappa \wedge u \sim \mathcal{P}_1(x))\}$.

The formula is stratified, giving x index 0, and 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 10.2. If $\kappa \in \mathbb{F}$, then $x \in \kappa \leftrightarrow \mathcal{P}_1(x) \in \mathbb{T}(\kappa)$.

Proof. Left to right. We have

$$\begin{aligned}
x \in \kappa &\quad \text{by hypothesis,}\\
\mathcal{P}_1(x) \sim \mathcal{P}_1(x) &\quad \text{by Lemma 2.11,}\\
\mathcal{P}_1(x) \in \mathbb{T}(\kappa) &\quad \text{by Definition 10.1.}
\end{aligned}$$

That completes the left-to-right direction.

Right to left. We have

$$\begin{array}{rl} \mathcal{P}_1(x) \in \mathbb{T}(\kappa) & \text{by hypothesis,} \\ \exists z\,(z \in \kappa \wedge \mathcal{P}_1(z) \sim \mathcal{P}_1(x)) & \text{by definition of } \mathbb{T}, \\ z \sim x & \text{by Lemma 6.7,} \\ x \in \kappa & \text{by Lemma 4.8.} \end{array}$$

That completes the right-to-left direction. □

Lemma 10.3. If $\kappa \in \mathbb{F}$ then for every $x \in \kappa$, $\mathbb{T}(\kappa) = |\mathcal{P}_1(x)|$.

Proof. Suppose $\kappa \in \mathbb{F}$. Then κ is inhabited, by Corollary 4.7. Let $x \in \kappa$. Then

$$\begin{array}{rl} x \in \mathsf{FINITE} & \text{by Lemma 4.4,} \\ \mathcal{P}_1(x) \in \mathsf{FINITE} & \text{by Lemma 3.11,} \\ |\mathcal{P}_1(x)| \in \mathbb{F} & \text{by Lemma 4.20,} \\ \mathcal{P}_1(x) \in \mathbb{T}(\kappa) & \text{by Lemma 10.2,} \\ \mathcal{P}_1(x) \sim \mathcal{P}_1(x) & \text{by Lemma 2.11,} \\ \mathcal{P}_1(x) \in |\mathcal{P}_1(x)| & \text{by Definition 4.10.} \end{array}$$

We remark that we cannot finish the proof at this point by Lemma 4.23, because we do not yet know $\mathbb{T}(\kappa) \in \mathbb{F}$. Instead, by extensionality it suffices to prove

$$\forall u\,(u \in \mathbb{T}(\kappa) \leftrightarrow u \in |\mathcal{P}_1(x)|). \tag{53}$$

Left to right. Suppose $u \in \mathbb{T}(\kappa)$. By definition of $\mathbb{T}$, there exists $w \in \kappa$ with $u \sim \mathcal{P}_1(w)$. Then

$$\begin{array}{rl} w \sim x & \text{by Lemma 4.9, since } w \in \kappa \text{ and } x \in \kappa, \\ \mathcal{P}_1(w) \sim \mathcal{P}_1(x) & \text{by Lemma 6.7,} \\ u \sim \mathcal{P}_1(x) & \text{by Lemma 2.11 (transitivity of } \sim\text{), since } u \sim \mathcal{P}_1(w). \end{array}$$

That completes the proof of the right-to-left direction of (53).

Right to left. Suppose $u \in |\mathcal{P}_1(x)|$. Then $u \sim \mathcal{P}_1(x)$. Since $x \in \kappa$, we have $u \in \mathbb{T}(\kappa)$ by definition of $\mathbb{T}$. □

Lemma 10.4. If $\kappa \in \mathbb{F}$ and $x \in \kappa$ then $\kappa = |x|$.

Proof. Let $\kappa \in \mathbb{F}$ and $x \in \kappa$. By extensionality, it suffices to prove that for all u, $u \in \kappa \leftrightarrow u \in |x|$.

Left to right. Suppose $u \in \kappa$. Then

$$\begin{array}{rl} u \sim x & \text{by Lemma 4.9,} \\ x \sim u & \text{by Lemma 2.11,} \\ u \in |x| & \text{by Definition 4.10.} \end{array}$$

Right to left. Suppose $u \in |x|$. Then

$$\begin{array}{rl} u \sim x & \text{by Definition 4.10,} \\ u \in \kappa & \text{by Lemma 4.8.} \end{array}$$

□

Lemma 10.5. If $|x| \in \mathbb{F}$, then $\mathbb{T}(|x|) = |\mathcal{P}_1(x)|$.

Proof. By Lemma 10.3, with $\kappa = |x|$. □

Lemma 10.6. If $m \in \mathbb{F}$ then $\mathbb{T}m \in \mathbb{F}$.

Remark. Since the graph of $\mathbb{T}$ is not definable, we cannot express the lemma as $\mathbb{T}\colon \mathbb{F} \to \mathbb{F}$.

Proof of Lemma 10.6. Let $m \in \mathbb{F}$. By Corollary 4.7, m is inhabited. Let $a \in m$. Then

$$\begin{aligned} \mathcal{P}_1(a) &\in \mathbb{T}(m) && \text{by Lemma 10.2,} \\ a &\in \mathsf{FINITE} && \text{by Lemma 4.4,} \\ \mathcal{P}_1(a) &\in \mathsf{FINITE} && \text{by Lemma 3.11,} \\ |\mathcal{P}_1(a)| &\in \mathbb{F} && \text{by Lemma 4.20,} \\ \mathbb{T}(m) &\in \mathbb{F} && \text{by Lemma 10.3.} \end{aligned}$$

□

Lemma 10.7. Every singleton has cardinal one. That is, $\forall x\, (|\{x\}| = \mathsf{one})$.

Proof. By definition, $\mathsf{one} = \mathsf{zero}^+$ and $\mathsf{zero} = \{\varnothing\}$. Then the members of one are sets of the form $\varnothing \cup \{r\}$, by the definition of successor. But $\varnothing \cup \{r\} = \{r\}$. Hence the members of one are exactly the unit classes. Let x be given; then by definition of $|\{x\}|$, $|\{x\}|$ contains exactly the sets similar to $\{x\}$. By Lemma 6.3, that is exactly the unit classes. Hence $|\{x\}|$ and one have the same members, namely all unit classes. By extensionality, $|\{x\}| = \mathsf{one}$. □

Lemma 10.8. 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 $m^+ \in \mathbb{F}$ by Lemma 4.19, and

$$\begin{aligned} \mathbb{T}(m^+) &= |\mathcal{P}_1(x \cup \{a\})| && \text{by Lemma 10.3,} \\ &= |\mathcal{P}_1(x) \cup \{\{a\}\}| && \text{by Lemma 6.15,} \\ &= (|\mathcal{P}_1(x)|)^+ && \text{by Lemma 4.13,} \\ &= (\mathbb{T}m)^+ && \text{by Lemma 10.3.} \end{aligned}$$

□

Lemma 10.9 (Specker, [19, Lemma 5.2])**.** $\mathbb{T}(\mathsf{zero}) = \mathsf{zero}$.

Proof. We have $\mathcal{P}_1(\varnothing) = \varnothing$ as there are no singleton subsets of $\varnothing$. Since $\mathsf{zero} = |\varnothing|$, by Lemma 10.5 we have $\mathbb{T}(\mathsf{zero}) = |\mathcal{P}_1(\varnothing)| = |\varnothing| = \mathsf{zero}$. □

Lemma 10.10 (Specker, [19, Lemma 5.2])**.** $\mathbb{T}(\mathsf{one}) = \mathsf{one}$.

Proof. We have

$$\begin{aligned} \{\varnothing\} &\in \mathsf{one} && \text{by definition of one,} \\ \mathbb{T}(\mathsf{one}) &= |\mathcal{P}_1(\{\varnothing\}| && \text{by Lemma 10.3,} \\ \mathbb{T}(\mathsf{one}) &= |\{\{\varnothing\}\}| && \text{since } \mathcal{P}_1(\{\varnothing\}) = \{\{\varnothing\}\}, \\ |\{\{\varnothing\}\}| &= \mathsf{one} && \text{by Lemma 10.7,} \\ \mathbb{T}(\mathsf{one}) &= \mathsf{one} && \text{by the two previous lines.} \end{aligned}$$

□

Lemma 10.11 (Specker, [19, Lemma 5.2])**.** $\mathbb{T}(\mathsf{two}) = \mathsf{two}$.

Proof. We have

$$\begin{aligned} \mathbb{T}(\mathsf{two}) &= \mathbb{T}(\mathsf{one}^+) && \text{since } \mathsf{two} = \mathsf{one}^+, \\ &= (\mathbb{T}(\mathsf{one}))^+ && \text{by Lemma 10.8,} \\ &= \mathsf{one}^+ && \text{by Lemma 10.10,} \\ &= \mathsf{two}. \end{aligned}$$

□

Lemma 10.12 (Specker, [19, Lemma 5.5]). Let $m, n \in \mathbb{F}$. Then $n < m \to \mathbb{T}n < \mathbb{T}m$.

Remarks. Specker [19, Lemma 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.

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 5.17, 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 5.35, the first one is impossible. We turn to the second. Suppose $\mathbb{T}m = \mathsf{zero}$. Since $m \in \mathbb{F}$, by Corollary 4.7 we have $a \in m$ for some a. Then $\mathcal{P}_1(a) \in \mathbb{T}m$, by definition of $\mathbb{T}$. Since $\mathbb{T}m = \mathsf{zero}$, we have $\mathcal{P}_1(a) \in \mathsf{zero}$. Since $\mathsf{zero} = \{\varnothing\}$, we have $\mathcal{P}_1(a) = \varnothing$. Then $a = \varnothing$. Since $\varnothing \in \mathsf{zero}$, by Lemma 4.23 and the fact that $a \in m$, we have $m = \mathsf{zero}$. But that contradicts the assumption $\mathsf{zero} < m$, by Lemma 5.35. 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 5.13,
$\mathbb{T}n < \mathbb{T}r$	by the induction hypothesis,
$\exists a\,(a \in m)$	by Corollary 4.7,
$\exists a\,(a \in r^+)$	since $m = r^+$,
$(\mathbb{T}r)^+ = \mathbb{T}(r^+)$	by Lemma 10.8,
$\exists u\,(u \in n^+)$	by the definition of $\le$, since $n^+ < r^+$,
$(\mathbb{T}n)^+ = \mathbb{T}(n^+)$	by Lemma 10.8, since n^+ is inhabited,
$\mathbb{T}(r^+) \in \mathbb{F}$	by Lemma 10.6,
$\mathbb{T}(n^+) \in \mathbb{F}$	by Lemma 10.6,
$\exists u\,(u \in \mathbb{T}(r^+))$	by Corollary 4.7,
$\exists u\,(u \in \mathbb{T}(n^+))$	by Corollary 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. □

Lemma 10.13 (Specker, [19, Lemma 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 of Lemma 10.13. By induction on m we prove

$$\forall n \in \mathbb{F}\,(n + m \in \mathbb{F} \to \mathbb{T}(n+m) = \mathbb{T}n + \mathbb{T}m). \tag{54}$$

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 10.9, 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 (54). 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 (54), we have $\mathbb{T}(n + m) = \mathbb{T}n + \mathbb{T}m$. Taking the successor of both sides, we have

$$
\begin{aligned}
(\mathbb{T}(n+m))^+ &= (\mathbb{T}n + \mathbb{T}m)^+, \\
\mathbb{T}((n+m)^+) &= (\mathbb{T}n + \mathbb{T}m)^+ && \text{by Lemma 10.8,} \\
\mathbb{T}(n+m^+) &= (\mathbb{T}n + \mathbb{T}m)^+ && \text{by Lemma 8.2,} \\
&= \mathbb{T}n + (\mathbb{T}m)^+ && \text{by Lemma 8.2,} \\
&= \mathbb{T}n + \mathbb{T}(m^+) && \text{by Lemma 10.8.}
\end{aligned}
$$

That is the desired goal. That completes the induction step. □

Lemma 10.14 (Specker, [19, Lemma 5.8])**.** For $m \in \mathbb{F}$, $2^{\mathbb{T}m}$ is inhabited.

Proof. Let $m \in \mathbb{F}$. Then

$$
\begin{aligned}
u &\in m && \text{for some } u\text{, by Corollary 4.7,} \\
\mathcal{P}_1(u) &\in \mathbb{T}m && \text{by Definition 10.1,} \\
\mathcal{P}_s(u) &\in 2^{\mathbb{T}m} && \text{by the definition of exponentiation.}
\end{aligned}
$$

□

Lemma 10.15. 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 10.14. Then by the definition of exponentiation, for some u we have $\mathcal{P}_s(u) \in 2^{\mathbb{T}m} \wedge \mathcal{P}_1(u) \in \mathbb{T}m$. Then

$$
\begin{aligned}
\mathbb{T}m &\in \mathbb{F} && \text{by Lemma 10.6,} \\
\mathcal{P}_1(u) &\in \mathsf{FINITE} && \text{by Lemma 4.4,} \\
u &\in \mathsf{FINITE} && \text{by Lemma 3.11,} \\
\mathcal{P}_1(u) &\in \mathbb{T}m && \text{by definition of } \mathbb{T}, \\
\mathcal{P}_s(u) &\in \mathsf{FINITE} && \text{by Lemma 3.18,} \\
\mathcal{P}_s(u) &\in 2^{\mathbb{T}m} && \text{by Lemma 8.12,} \\
2^{\mathbb{T}m} &\in \mathbb{F} && \text{by Lemma 7.5.}
\end{aligned}
$$

□

Lemma 10.16. Suppose $m \in \mathbb{F}$. Then $(\mathbb{T}m)^+ \in \mathbb{F}$.

Proof. Suppose $m \in \mathbb{F}$. Then

$$
\begin{aligned}
2^{\mathbb{T}m} &\in \mathbb{F} && \text{by Lemma 10.15,} \\
\mathbb{T}m &\in \mathbb{F} && \text{by Lemma 10.6,} \\
\exists u\left(u \in 2^{\mathbb{T}m}\right) & && \text{by Corollary 4.7,} \\
\mathbb{T}m &< 2^{\mathbb{T}m} && \text{by Lemma 7.16,} \\
(\mathbb{T}m)^+ &\in \mathbb{F} && \text{by Lemma 5.32.}
\end{aligned}
$$

□

Lemma 10.17 (Specker, [19, Lemma 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 $\mathcal{P}_1(a) \in m$. Then

$$\begin{aligned}
2^m &= |\mathcal{P}_s(a)| && \text{by Lemma 7.2,}\\
\mathcal{P}_s(a) &\in 2^m && \text{by Lemma 8.12,}\\
\mathcal{P}_1(\mathcal{P}_s(a)) &\in \mathbb{T}(2^m) && \text{by Lemma 10.2,}\\
\mathcal{P}_1(\mathcal{P}_1(a)) &\in \mathbb{T}m && \text{by Lemma 10.2,}\\
\mathbb{T}m &\in \mathbb{F} && \text{by Lemma 10.6,}\\
\mathcal{P}_s(\mathcal{P}_1(a)) &\in 2^{\mathbb{T}m} && \text{by Lemma 8.12,}\\
2^m &\in \mathbb{F} && \text{by Lemma 7.5,}\\
2^{\mathbb{T}m} &\in \mathbb{F} && \text{by Lemma 7.5,}\\
|\mathcal{P}_s(\mathcal{P}_1(a))| &= |\mathcal{P}_1(\mathcal{P}_s(a))| && \text{by Lemma 6.2,}\\
2^{\mathbb{T}m} &= |\mathcal{P}_s(\mathcal{P}_1(a))| && \text{by Lemma 10.4,}\\
\mathbb{T}(2^m) &= |\mathcal{P}_1(\mathcal{P}_s(a))| && \text{by Lemma 10.3,}\\
2^{\mathbb{T}m} &= \mathbb{T}(2^m) && \text{from the last three equations.}
\end{aligned}$$ □

Lemma 10.18. 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 Corollary 4.7, we can find $a \in n$ and $b \in m$. Then

$$\begin{aligned}
\mathcal{P}_1(a) &\in \mathbb{T}n && \text{by definition of } \mathbb{T},\\
\mathcal{P}_1(b) &\in \mathbb{T}m && \text{by definition of } \mathbb{T},\\
\mathbb{T}n &= \mathbb{T}m && \text{by hypothesis,}\\
\mathcal{P}_1(a) &\in \mathbb{T}n && \text{by the previous two lines,}\\
\mathbb{T}m &\in \mathbb{F} && \text{by Lemma 10.6,}\\
\mathcal{P}_1(a) &\sim \mathcal{P}_1(b) && \text{by Lemma 4.9,}\\
a &\sim b && \text{by Lemma 6.7,}\\
b &\in n && \text{by Lemma 4.8,}\\
n &= m && \text{by Lemma 4.23.}
\end{aligned}$$ □

Lemma 10.19 (Converse to Specker [19, Lemma 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 of Lemma 10.19. The formula is stratified, giving a, b, and c all index zero. Therefore we may proceed by induction on b.

Base case. We have

$$\begin{aligned}
\mathbb{T}a + \mathbb{T}(\mathsf{zero}) &= \mathbb{T}c && \text{by assumption,}\\
\mathbb{T}a + \mathsf{zero} &= \mathbb{T}c && \text{by Lemma 10.9,}\\
\mathbb{T}a &= \mathbb{T}c && \text{by Lemma 8.2,}\\
a &= c && \text{by Lemma 10.18,}\\
a + \mathsf{zero} &= c && \text{by Lemma 8.2.}
\end{aligned}$$

That completes the base case.

Induction step. We have

$\mathbb{T}a + \mathbb{T}(b^+) = \mathbb{T}c$	by assumption,
$\exists u\,(u \in b^+)$	by assumption,
$b^+ \in \mathbb{F}$	by Lemma 4.19,
$\mathbb{T}(b^+) = (\mathbb{T}b)^+$	by Lemma 10.8,
$\mathbb{T}a + (\mathbb{T}b)^+ = \mathbb{T}c$	by the preceding lines,
$(\mathbb{T}a + \mathbb{T}b)^+ = \mathbb{T}c$	by Lemma 8.2,
$c \neq \mathsf{zero}$	by Lemma 10.9 Lemma 4.16,
$c = r^+$	for some r, by Lemma 4.17,
$(\mathbb{T}a + \mathbb{T}b)^+ = \mathbb{T}(r^+)$	by the preceding two lines,
$(\mathbb{T}a + \mathbb{T}b)^+ = (\mathbb{T}r)^+$	by Lemma 10.8,
$\mathbb{T}a + \mathbb{T}(b^+) \in \mathbb{F}$	by assumption,
$(\mathbb{T}a + \mathbb{T}b)^+ \in \mathbb{F}$	by Lemma 10.8 Lemma 8.2,
$\exists u\,(u \in (\mathbb{T}a + \mathbb{T}b)^+)$	by Corollary 4.7,
$\exists u\,(u \in (\mathbb{T}a + \mathbb{T}b))$	by definition of successor,
$\exists u\,(u \in (\mathbb{T}r)^+)$	by Corollary 4.7,
$\mathbb{T}r \in \mathbb{F}$	by Lemma 10.6,
$\mathbb{T}a \in \mathbb{F}$	by Lemma 10.6,
$\mathbb{T}b \in \mathbb{F}$	by Lemma 10.6,
$\mathbb{T}a + \mathbb{T}b \in \mathbb{F}$	by Lemma 8.6,
$\mathbb{T}a + \mathbb{T}b = \mathbb{T}r$	by Lemma 5.11,
$a + b = r$	by the induction hypothesis,
$(a+b)^+ = r^+$	by the preceding line,
$a + b^+ = r^+$	by Lemma 8.2,
$a + b^+ = c$	since $r^+ = c$.

That completes the induction step. □

Lemma 10.20. For $n, m \in \mathbb{F}$, we have $n < m \leftrightarrow \mathbb{T}n < \mathbb{T}m$.

Proof. Left to right. This is Lemma 10.12.

Right to left. Suppose $\mathbb{T}n < \mathbb{T}m$. By Theorem 5.17, 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 10.6, $\mathbb{T}n \in \mathbb{F}$ and $\mathbb{T}m \in \mathbb{F}$, so by Theorem 5.17, $\mathbb{T}n = \mathbb{T}m$ contradicts $\mathbb{T}n < \mathbb{T}m$. That completes Case 2.

Case 3: $m < n$. Then $\mathbb{T}m < \mathbb{T}n$ by Lemma 10.12. □

Lemma 10.21 (Specker, [19, Lemma 5.6])**.** 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

$$\forall q \in \mathbb{F}\,(p < \mathbb{T}q \to \exists r \in \mathbb{F}\,(p = \mathbb{T}r)). \tag{55}$$

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 10.9. That completes the base case.

Induction step. The induction hypothesis is (55). Suppose $p^+ < \mathbb{T}q$ and p^+ is inhabited. Then

$p < p^+$	by Lemma 5.27,
$p < \mathbb{T}q$	by Lemma 5.26,
$p = \mathbb{T}r$	for some r, by (55).

Now I say that r^+ is inhabited. To prove that:

$\mathbb{T}r = p < p^+ < \mathbb{T}q$	as already proved,
$\mathbb{T}r < \mathbb{T}q$	from the previous line,
$r < q$	by Lemma 10.20,
$r^+ \leq q$	by Lemma 5.31,
$\exists u\,(u \in r^+)$	by the definition of $\leq$.

That completes the proof that r^+ is inhabited. Then since $p = \mathbb{T}r$, we have $p^+ = (\mathbb{T}r)^+ = \mathbb{T}(r^+)$ by Lemma 10.8. That completes the induction step. □

Lemma 10.22. 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 $\mathcal{P}_1(a) \in p$ and $\mathcal{P}_s(a) \in 2^p$. By definition of $\mathbb{T}$ we have $p = \mathbb{T}(|a|)$. By Lemma 4.20, we have $|a| \in \mathbb{F}$. □

Lemma 10.23 (Specker, [19, Lemma 5.5])**.** For $n, m \in \mathbb{F}$, we have $n \leq m \leftrightarrow \mathbb{T}n \leq \mathbb{T}m$.

Remark. It is also possible to prove this lemma directly from the definitions of $\leq$ and $\mathbb{T}$, instead of from Lemma 10.20 as we do here, and then prove Lemma 10.20 from this lemma. Or we could prove this lemma by induction as we did Lemma 10.20.

Proof of Lemma 10.23. We have

$n \leq m \leftrightarrow n < m \vee n = m$	by Lemma 5.20,
$\mathbb{T}n \leq \mathbb{T}m \leftrightarrow \mathbb{T}n < \mathbb{T}m \vee \mathbb{T}n = \mathbb{T}m$	by Lemma 5.20.

Now to prove the desired conclusion:

Left to right. If $n < m$ then $\mathbb{T}n < \mathbb{T}m$ by Lemma 10.20, so $\mathbb{T}n \leq \mathbb{T}m$. And if $n = m$, then $\mathbb{T}n = \mathbb{T}m \leq \mathbb{T}m$, by Lemma 5.19.

Right to left. If $\mathbb{T}n < \mathbb{T}m$ then $n < m$ by Lemma 10.20, so $n \leq m$. And if $\mathbb{T}n = \mathbb{T}m$, then $n = m$ by Lemma 10.18. □

Lemma 10.24. Let $e \in \mathbb{F}$ and $e + e \in \mathbb{F}$. Then $e^+ \in \mathbb{F}$.

Proof. By Corollary 5.18, $e = \mathsf{zero} \vee e \neq \mathsf{zero}$. If $e = \mathsf{zero}$ then $e^+ = \mathsf{one}$, so we are done by Lemma 5.15. Therefore we may assume $e \neq \mathsf{zero}$. By Corollary 4.7, $e + e$ is inhabited. By the definition of $<$, there exist x and y with $x \in e$ and $y \in e$ and $x \cap y = \varnothing$. Then

$y \neq \varnothing$	since if $y = \varnothing$ then $e = \mathsf{zero}$, by Lemma 4.23,
$y \in \mathsf{FINITE}$	by Lemma 4.4,
$a \in y$	for some a, by Lemma 3.4,
$a \notin x$	since $x \cap y = \varnothing$,
$x \cup \{a\} \in e^+$	by definition of successor,
$e^+ \in \mathbb{F}$	by Lemma 4.19. □

Lemma 10.25. 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, and $\mathbb{F}$ 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

$$\begin{array}{rl} \mathsf{zero} + \mathsf{zero} = \mathsf{zero} & \text{since } x + \mathsf{zero} = x, \\ \mathbb{T}(\mathsf{zero}) = \mathsf{zero} & \text{by Lemma 10.9}, \\ \mathbb{T}c = \mathsf{zero} & \text{since } \mathbb{T}c = \mathsf{zero} + \mathsf{zero} = \mathsf{zero}, \\ c = \mathsf{zero} & \text{by Lemma 10.18}, \\ \exists b\,(c = b + b) & \text{namely, } b = \mathsf{zero}. \end{array}$$

Induction step. Suppose a^+ is inhabited and $a^+ \in \mathbb{F}$ and $\mathbb{T}c = a^+ + a^+$, and $a \in \mathbb{F}$ and $a^+ + a^+ \in \mathbb{F}$. (The assumption $a^+ \in \mathbb{F}$ is part of the induction hypothesis, while the assumptions $a \in \mathbb{F}$ and a^+ is inhabited come with every proof by induction on $\mathbb{F}$.) Then

$$\begin{array}{rl} a^+ + a^+ = (a + a)^{++} & \text{by Lemma 8.2}, \\ (a + a)^{++} \in \mathbb{F} & \text{since } a^+ + a^+ \in \mathbb{F}. \end{array}$$

I say that

$$a + a \in \mathbb{F}. \tag{56}$$

It is surprisingly difficult to prove that. I had to go back to the definition of addition. Since $a^+ + a^+ \in \mathbb{F}$, there exists $x \in a^+ + a^+$, by Corollary 4.7. By the definition of addition, x has the form

$$\begin{array}{rl} x = u \cup v & \text{with } u \cap v = \varnothing \text{ and } u \in a^+ \text{ and } v \in a^+, \\ u = z \cup \{p\} \wedge v = w \cup \{q\} & \text{with } z \in a \text{ and } w \in a, \text{ by definition of successor}, \\ z \cup w \in a + a & \text{by the definition of addition}, \\ a + a \in \mathbb{F} & \text{by Lemma 8.6}. \end{array}$$

That completes the proof of (56).

Similarly, $x \cup u \in a^+ + a$, so

$$\begin{array}{rl} a^+ \in \mathbb{F} & \text{by Lemma 4.19, since } a \in F \text{ and } a^+ \text{ is inhabited}, \\ a^+ + a \in \mathbb{F} & \text{by Lemma 8.6}, \\ (a + a)^+ = a^+ + a & \text{by Lemma 8.2}, \\ (a + a)^+ \in \mathbb{F} & \text{by the preceding lines}. \end{array}$$

Continuing, we have

$$\begin{array}{rl} \mathbb{T}c = (a + a)^{++} & \text{by Lemma 8.2}, \\ \mathbb{T}c \neq \mathsf{zero} & \text{by Lemma 4.16}, \\ \mathsf{one} \neq (a + a)^{++} & \text{by Lemma 5.11}, \\ \mathbb{T}c \neq \mathsf{one} & \text{since } \mathbb{T}c = (a + a)^{++}, \\ c \neq \mathsf{zero} & \text{by Lemma 10.9}, \\ c = r^+ & \text{for some } r \in \mathbb{F}, \text{ by Lemma 4.17}, \\ r \neq \mathsf{zero} & \text{since if } r = \mathsf{zero} \text{ then } r^+ = c = \mathsf{one}, \text{ so } \mathbb{T}c = \mathsf{one}, \end{array}$$

$$\begin{aligned}
r &= t^+ && \text{for some } t \in \mathbb{F}\text{, by Lemma 4.17,}\\
c &= t^{++} && \text{by the preceding lines,}\\
\mathbb{T}c &= (\mathbb{T}t)^{++} && \text{by Lemma 10.8,}\\
(a+a)^{++} &= (\mathbb{T}t)^{++} && \text{since } \mathbb{T}c = (a+a)^{++},\\
\mathbb{T}t &\in \mathbb{F} && \text{by Lemma 10.6,}\\
\mathbb{T}t &= a+a && \text{by Lemma 5.11,}\\
t &= e+e && \text{for some } e \in \mathbb{F}\text{, by the induction hypothesis,}\\
t^{++} &= (e^+ + e^+) && \text{by Lemma 8.2,}\\
c &= b+b && \text{with } b = e^+\text{, by the preceding lines,}\\
e^+ &\in \mathbb{F} && \text{by Lemma 10.24, since } e+e = t \in \mathbb{F}.
\end{aligned}$$

That completes the induction step. □

Lemma 10.26 (Specker, [19, Lemma 5.4])**.** Let $m \in \mathsf{NC}$. Then $m \neq \mathbb{T}(m) + \mathsf{one}$.

Remark. And so on, with one replaced by two or 23, 457, and any number you could name. If $\mathbb{T}m \neq m$, $\mathbb{T}m$ must be a non-standard distance away from m.

Proof of Lemma 10.26. We give the proof for one. Recall that m is even if $m = p + p$ for some $p \in \mathbb{F}$, and odd if $m = p + p + \mathsf{one}$ for some $p \in \mathbb{F}$. Then if m is even, $m + \mathsf{one}$ is odd, and vice versa. One can verify by induction that every integer is either even or odd, and not both. Suppose $\mathbf{m} = \mathbb{T}\mathbf{m} + \mathsf{one}$. If m is even, then $\mathbb{T}m$ is even, by Lemma 10.25, so $\mathbb{T}m + \mathsf{one}$ is odd, contradiction. If m is odd, then $m = k^+ = k + \mathsf{one}$ for some $k \in \mathbb{F}$, since zero is even. Then k is even. Then $\mathbb{T}m = \mathbb{T}(k^+) = \mathbb{T}(k + \mathsf{one}) = \mathbb{T}k + \mathsf{one}$, which is odd since $\mathbb{T}k$ is even. Then $\mathbb{T}m + \mathsf{one}$ is even, contradiction, since m is odd and equal to $\mathbb{T}m + \mathsf{one}$. □

Lemma 10.27. For all p, q, if $p + q = \mathsf{zero}$ then $p = \mathsf{zero}$.

Remark. No additional hypothesis is needed.

Proof of Lemma 10.27. By definition, $\mathsf{zero} = \{\varnothing\}$. By the definition of addition, there exist a and b with $a \in p$ and $b \in q$ and $a \cap b = \varnothing$, such that $a \cup b \in \mathsf{zero}$. Then $a \cup b = \varnothing$. It follows that $a = \varnothing$ and $b = \varnothing$. 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 $p = q = \{\varnothing\} = \mathsf{zero}$. □

Lemma 10.28. 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 10.27, $y = \mathsf{zero}$. That completes the base case.

Induction step. Suppose $x^+ + x^+ = y + y$, and suppose (as always in induction proofs) that x^+ is inhabited. Then we have

$$\begin{aligned}
x^+ + x^+ &= (x+x)^{++} && \text{by Lemma 8.2,}\\
y &\neq \mathsf{zero} && \text{by Lemma 4.16,}\\
y &= r^+ && \text{for some } r\text{, by Lemma 4.17,}\\
(x+x)^{++} &= (r+r)^{++} && \text{by Lemma 8.2,}\\
x+x &= r+r && \text{by Lemma 5.11,}\\
x &= r && \text{by the induction hypothesis,}
\end{aligned}$$

$$
\begin{array}{rl}
x^+ = r^+ & \text{by the preceding line,} \\
x^+ = y & \text{since } y = r^+.
\end{array}
$$

That completes the induction step. □

Lemma 10.29. 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. We have

$$
\begin{array}{rl}
2^p \in \mathbb{F} & \text{assumption,} \\
\exists u\,(u \in 2^p) & \text{by Corollary 4.7,} \\
\mathcal{P}_1(a) \in p & \text{for some } a\text{, by the definition of exponentiation,} \\
\mathcal{P}_1(a) \in \mathsf{FINITE} & \text{by Lemma 4.4,} \\
a \in \mathsf{FINITE} & \text{by Lemma 3.11,} \\
|a| \in \mathbb{F} & \text{by Lemma 4.20,} \\
a \in |a| & \text{by Lemma 4.11,} \\
\mathcal{P}_1(a) \in \mathbb{T}(|a|) & \text{by definition of } \mathbb{T}, \\
\mathbb{T}(|a|) \in \mathbb{F} & \text{by Lemma 10.6,} \\
\mathcal{P}_1(a) \in p \cap \mathbb{T}(|a|) & \text{by definition of intersection,} \\
p = \mathbb{T}(|a|) & \text{by Lemma 4.23,} \\
\exists q \in \mathbb{F}\,(p = \mathbb{T}a) & \text{namely } q = |a|.
\end{array}
$$

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

Right to left. Suppose $p = \mathbb{T}q$ and $q \in \mathbb{F}$. Then

$$
\begin{array}{rl}
u \in q & \text{for some } u\text{, by Corollary 4.7,} \\
\mathcal{P}_1(u) \in \mathbb{T}q & \text{by definition of } \mathbb{T}, \\
\mathbb{T}q \in \mathbb{F} & \text{by Lemma 10.6,} \\
 & \\
\mathcal{P}_s(u) \in 2^{\mathbb{T}q} & \text{by definition of exponentiation,} \\
\mathcal{P}_s(u) \in 2^p & \text{since } p = \mathbb{T}q, \\
2^p \in \mathbb{F} & \text{by Lemma 7.5.}
\end{array}
$$

That completes the proof of the right-to-left direction. □

Definition 10.30. Let X be any set of cardinals. Then we define $\mathbb{T}``(X) = \{\mathbb{T}(u) : u \in X\}$, or more explicitly $\mathbb{T}``(X) = \{\mathbb{T}(u) : u \in X\} = \{y : \exists u \in X\,(y = \mathbb{T}u)\}$.

The formula in the definition is stratified, giving u index 0 and y and X index 1. Actually, X is just a parameter and does not even need an index. Therefore the definition is legal in $i\mathsf{NF}$. We note that it is not a function definable in $i\mathsf{NF}$. It is just an abbreviation for a comprehension term. Note also that the set X can be finite or not, and the cardinals in X can be finite or not.

In general images commute with union. For images under $\mathbb{T}$ we have:

Lemma 10.31. $\mathbb{T}``(X \cup Y) = \mathbb{T}``(X) \cup \mathbb{T}``(Y)$.

Proof. This is proved in a few short steps from the definitions of $T``(X)$ and $\cup$. □

Lemma 10.32. Let a and b be finite disjoint sets. Then $|a \cup b| = |a| + |b|$.

Proof. Left to right. Suppose $t \in |a \cup b|$. Then

$$
\begin{aligned}
a \cup b &\in |a \cup b| && \text{by Lemma 4.11,}\\
a &\in |a| && \text{by Lemma 4.11,}\\
b &\in |b| && \text{by Lemma 4.11,}\\
a \cap b &= \varnothing && \text{by hypothesis,}\\
a \cup b &\in \mathsf{FINITE} && \text{by Lemma 3.12,}\\
|a| &\in \mathbb{F} && \text{by Lemma 4.20,}\\
|b| &\in \mathbb{F} && \text{by Lemma 4.20,}\\
|a \cup b| &\in \mathbb{F} && \text{by Lemma 4.20,}\\
|a| + |b| &\in \mathbb{F} && \text{by Lemma 8.6,}\\
a \cup b &\in |a| + |b| && \text{by the definition of addition,}\\
|a \cup b| &= |a| + |b| && \text{by Lemma 4.23.}
\end{aligned}
$$

□

Lemma 10.33. Let X be a finite set of cardinal numbers. Then $|\mathbb{T}``(X)| = \mathbb{T}(|X|)$.

Proof. The displayed formula in the lemma is stratified, giving X index 1; then $|X|$ gets index 2 and $\mathbb{T}(|X|)$ gets index 3. On the left, the members of $\mathbb{T}``(X)$ are $\mathbb{T}u$ for $u \in X$, so $u$ gets index 0, and $\mathbb{T}u$ gets index 1, so $\mathbb{T}``X$ gets index 2, so $|\mathbb{T}``(X)|$ gets index 3, the same as the right side of the equation. So it is stratified, as claimed.

The part of the lemma involving X is $\forall X\,(X \in \mathsf{FINITE} \to X \subset \mathsf{NC} \to |\mathbb{T}``(X)| = \mathbb{T}(|X|))$, and this is also stratified, since FINITE and NC are just parameters. Therefore we can prove it by induction on finite sets.

Base case: $X = \varnothing$. On the right, $|\varnothing| = \mathsf{zero}$, so $\mathbb{T}(|\varnothing|) = \mathbb{T}(\mathsf{zero}) = \mathsf{zero}$. On the left, $\mathbb{T}``(\varnothing) = \varnothing$, so $|\mathbb{T}``(\varnothing)| = \mathsf{zero}$. That completes the base case.

Induction step. Suppose X is finite and $c \notin X$. We have to show $|\mathbb{T}``(X \cup \{c\}| = \mathbb{T}(|X \cup \{c\}|)$. We have

$$
\begin{aligned}
X \cup \{c\} &\in \mathsf{FINITE} && \text{by Lemma 3.7, since } c \notin X,\\
\mathbb{T}``(X \cup \{c\}) &= \mathbb{T}``(X) \cup \{\mathbb{T}c\} && \text{by Lemma 10.31,} && (57)\\
|\mathbb{T}``(X \cup \{c\})| &= |\mathbb{T}``(X) \cup \{\mathbb{T}c\}| && \text{by the preceding line,}\\
\mathbb{T}c &\notin \mathbb{T}``(X) && \text{by Lemma 10.18, since } c \notin X, && (58)\\
|\mathbb{T}``(X)| &= \mathbb{T}(|X|) && \text{by the induction hypothesis,} && (59)\\
|X| &\in \mathbb{F} && \text{by Lemma 4.20, since } X \in \mathsf{FINITE},\\
\mathbb{T}(|X|) &\in \mathbb{F} && \text{by Lemma 10.6,}\\
\mathbb{T}``(X) &\in \mathsf{FINITE} && \text{by Lemma 4.4,}\\
\{\mathbb{T}c\} &\in \mathsf{FINITE} && \text{by Lemma 3.9,}\\
\mathbb{T}``(X) \cap \{\mathbb{T}c\} &= \varnothing && \text{by (58),}\\
|\mathbb{T}``(X) \cup \{\mathbb{T}c\})| &= |\mathbb{T}``(X)| + |\{\mathbb{T}c\}| && \text{by Lemma 10.32,}\\
|\mathbb{T}``(X) \cup \{\mathbb{T}c\})| &= |\mathbb{T}``(X)| + \mathsf{one} && \text{by Lemma 10.7,}\\
|\mathbb{T}``(X) \cup \{\mathbb{T}c\})| &= \mathbb{T}(|X|) + \mathsf{one} && \text{by the induction hypothesis (59),}\\
|\mathbb{T}``(X) \cup \{\mathbb{T}c\})| &= \mathbb{T}(|X|) + \mathbb{T}(\mathsf{one}) && \text{since } \mathbb{T}(\mathsf{one}) = \mathsf{one},\\
|X| + \mathsf{one} &= |X \cup \{c\}| && \text{by Lemma 10.32 since } c \notin X,
\end{aligned}
$$

$$
\begin{array}{rl}
|X| + \mathsf{one} \in \mathbb{F} & \text{by Lemma 8.6,} \\
|\mathbb{T}\,``(X) \cup \{\mathbb{T}c\})| = \mathbb{T}(|X| + \mathsf{one}) & \text{by Lemma 10.13,} \\
|\mathbb{T}\,``(X) \cup \{\mathbb{T}c\}| = \mathbb{T}(|X \cup \{c\}|) & \text{by the preceding lines,} \\
|\mathbb{T}\,``(X \cup \{c\})| = \mathbb{T}(|X \cup \{c\}|) & \text{by (57).}
\end{array}
$$

That completes the induction step. □

Lemma 10.34. Let X be a finite set of cardinals. Then $\mathbb{T}\,``(X)$ is finite.

Proof. Let X be a finite set of cardinals. Then

$$
\begin{array}{rll}
X \subseteq \mathsf{FINITE} & \text{by hypothesis,} & \\
\mathbb{T}\,``(X) \in \mathsf{FINITE} & \text{by hypothesis,} & \\
|\mathbb{T}\,``(X)| = \mathbb{T}(|X|) & \text{by Lemma 10.33,} & (60) \\
|X| \in \mathbb{F} & \text{by Lemma 4.20,} & \\
\mathbb{T}(|X|) \in \mathbb{F} & \text{by Lemma 10.6,} & (61) \\
|\mathbb{T}\,``(X)| \in \mathbb{F} & \text{by (60) and (61),} & \\
\mathbb{T}\,``(X) \in |\mathbb{T}\,``(X)| & \text{by Lemma 4.11,} & \\
\mathbb{T}\,``(X) \in \mathsf{FINITE} & \text{by Lemma 4.4.} &
\end{array}
$$

□

11 Cartesian products

The Cartesian product of two sets is defined as usual; the definition is stratified, so it can be given in $i\mathsf{NF}$. 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 11.1. Let X, Y, and Z be finite sets. Then $(X \cup Y) \times Z = (X \times Z) \cup (Y \times Z)$.

Proof. This follows in a few steps from extensionality, the definition of $\times$, and the logical fact that $(P \vee Q) \wedge R \leftrightarrow (P \wedge R) \vee (Q \wedge R)$. □

Lemma 11.2. Let Y be a finite set and let a be any set. Then $\{a\} \times Y$ is finite. If $\kappa = |Y|$ then $\mathbb{T}^2\kappa = |\{a\} \times Y|$.

Proof. Consider the map $f\colon \mathcal{P}_1^2(Y) \to \{a\} \times Y$ 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 $\{\{y\}\}$, and Y gets index 1. Since the formula is stratified, f can be defined in $i\mathsf{NF}$.

One then proves without any surprises that f is a similarity from $\mathcal{P}_1^2(Y)$ to $\{a\} \times Y$. We omit the straightforward 196-line verification of that fact.

Then we have

$$
\begin{array}{rl}
\mathcal{P}_1^2(Y) \sim \{a\} \times Y & \text{since } f \text{ is a similarity,} \\
\mathcal{P}_1(Y) \in \mathsf{FINITE} & \text{by Lemma 3.11,} \\
\mathcal{P}_1^2(Y) \in \mathsf{FINITE} & \text{by Lemma 3.11,} \\
\{a\} \times Y \in \mathsf{FINITE} & \text{by Lemma 4.22,} \\
|\mathcal{P}_1^2(Y)| = \mathbb{T}^2\kappa & \text{by definition of } \mathbb{T}, \\
|\{a\} \times Y| = \mathbb{T}^2\kappa & \text{by Lemma 4.8.}
\end{array}
$$

□

Lemma 11.3. Let X and Y be finite sets. Then $X \times Y$ is finite. Moreover, if $\kappa = |X|$ and $\mu = |Y|$, then $\mathbb{T}^2(\kappa) \cdot \mathbb{T}^2(\mu) = |X \times Y|$.

Proof. The formula to be proved is $X \in \mathsf{FINITE} \to \forall Y \in \mathsf{FINITE}\,(X \times Y \in \mathsf{FINITE})$. That formula (and the hypotheses listed before it) are stratified, giving X and Y index 1; then $X \times Y$ gets index 3, $|X \times Y|$ gets index 4, $\kappa = |X|$ 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. We have to show $\varnothing \times Y \in \mathsf{FINITE}$. One shows $\varnothing \times Y = \varnothing$ using the definition of $\times$, and then $\varnothing \in \mathsf{FINITE}$ by Lemma 3.6.

Induction step. Assume X is finite and $a \notin X$. The induction hypothesis is

$$\forall Y \in \mathsf{FINITE}\,(X \times Y \in \mathsf{FINITE}). \tag{62}$$

Assume $X \cup \{a\} \in \mathsf{FINITE}$. We have to prove $(X \cup \{a\}) \times Y \in \mathsf{FINITE}$. We have

$$\begin{aligned}
X &\in \mathsf{FINITE} && \text{by hypothesis,}\\
X \times Y &\in \mathsf{FINITE} && \text{by the induction hypothesis (62),}\\
\{a\} \times Y &\in \mathsf{FINITE} && \text{by Lemma 11.2,}\\
(X \cup \{a\}) \times Y &= (X \times Y) \cup (\{a\} \times Y) && \text{by Lemma 11.1,}\\
(X \times Y) \cap (\{a\} \times Y) &= \varnothing && \text{since } a \notin X,\\
(X \cup Y) \cup (\{a\} \times Y) &\in \mathsf{FINITE} && \text{by Lemma 3.12,}\\
(X \cup \{a\}) \times Y &\in \mathsf{FINITE} && \text{by the preceding lines.}
\end{aligned}$$

That completes the induction step. □

Lemma 11.4. Let X and Y be finite sets. If $\kappa = |X|$ and $\mu = |Y|$, then $\mathbb{T}^2(\kappa) \cdot \mathbb{T}^2(\mu) = |X \times Y|$.

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 4.20.

Proof. By induction on finite sets, like Lemma 11.3. We omit the proof, since we never use this lemma. It is included only because it illustrates the general situation that arises from using Kuratowski pairing, which increases the type. □

12 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

(1) $f\colon X \to Y$,
(2) $\mathrm{Rel}(f)$,
(3) $f \in \mathsf{FUNC}$,
(4) $\mathrm{oneone}(f, X, Y)$.

The expression $\mathrm{Rel}(f)$ means that all the members of f are ordered pairs. The expression $f \in \mathsf{FUNC}$ 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.) The expression $f\colon X \to Y$ 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 $x \notin X$.) The expression "f is one-to-one from X to Y", or oneone(f, X, Y), means $f\colon X \to Y$ 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, $f\colon X \to Y$ does not require $\mathrm{dom}(f) \subseteq X$, 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 12.1. We define f to be a *permutation* of a finite set X if and only if $f\colon X \to X$, and $\mathrm{Rel}(f)$ and $f \in \mathsf{FUNC}$, and $\mathrm{dom}(f) \subseteq X$, and f is both one-to-one and onto from X to X.

In this section we will prove that for finite X, 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 $\mathrm{range}(f) \subseteq X$, because that follows from $\mathrm{dom}(f) \subseteq X$ and $f\colon X \to X$. The reader can check that none of the conditions in the definition are superfluous.

Lemma 12.2. Let A and B be finite sets, let f be a function with domain A, and $f\colon A \to B$. Then f is finite.

Proof. By induction on finite sets A we prove that for all finite sets B, if the domain of f is A and $f\colon A \to B$, then f is finite.

Base case. A function with domain $\varnothing$ is the empty function, which is finite.

Induction step. Let A and B be finite sets, and let $c \notin A$, and suppose $f\colon A \cup \{c\} \to B$. Then $\langle c, y\rangle \in f$ for some $y \in B$. Let $g := f - \{\langle c, y\rangle\}$. One can verify that $g\colon A \to B$ and the domain of g is A.[12] Then by the induction hypothesis, g is finite. Since A and B are finite, equality on A and B is decidable, so any member of f is either equal to $\langle c, y\rangle$ or not. Therefore $f = g \cup \{\langle c, y\rangle\}$. Since g is finite and $\{\langle c, y\rangle\} \notin f$, f is also finite. □

Lemma 12.3 (Decidable image)**.** Let X and Y be finite sets. Let $f\colon X \to Y$ and suppose the domain of f is X. Then the set P defined by $f(X) = \{y \in Y : \exists x \in X\, \langle x, y\rangle \in f\}$ is a decidable subset of Y.

Proof. Let $y \in X$. Define $Z := \{x \in X : \exists y \in Y\, (\langle x, y\rangle \in f)\}$. The formula is stratified, giving x and y index 0, f index 3, and X index 1. Therefore the definition is legal. Then

$$\begin{aligned}
f &\subseteq X \times Y && \text{since } \mathrm{dom}(f) = X,\\
f &\in \mathsf{FINITE} && \text{by Lemma 12.2,}\\
X &\in \mathsf{DECIDABLE} && \text{by Lemma 3.3,}\\
X \times Y &\in \mathsf{FINITE} && \text{by Lemma 11.3,}\\
f \text{ is a separable relation on } X & && \text{by Lemma 3.19,}\\
Z &\in \mathsf{FINITE} && \text{by Lemma 3.22,}\\
Z = \varnothing &\vee \exists x\, (x \in Z) && \text{by Lemma 3.4.}
\end{aligned}$$

Putting in the definition of Z, we have the formula in the conclusion of the lemma. □

Theorem 12.4. Let X be a finite set, and let $f\colon X \to X$ be a one-to-one function. Then f is onto.

Proof. By induction on finite sets, we prove that if $f\colon X \to X$ 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.

[12] Formalizing this sort of lemma makes one appreciate the informal functional notation; this lemma took 330 lines of Lean and several hours. I changed "One can easily verify" to the present "One can verify."

Induction step. Let $X = B \cup \{a\}$, where $a \notin B$, and B is finite. Suppose $f\colon X \to X$ is one-to-one. We have to prove $\forall y \in X\, \exists x \in X\, (\langle x, y\rangle \in f)$. By Lemma 12.3, $a \in \text{range}(f) \vee a \notin \text{range}(f)$. Explicitly, $\exists x \in X\, (\langle x, a\rangle \in f) \vee \neg \exists x \in X\, (\langle x, a\rangle \in f)$. 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 $c = a \vee c \neq a$. We argue by cases.

Case 1a: $c = a$. Then $f\colon B \to B$. Let g be f restricted to B. Then g is one-to-one, since f is one-to-one. By the induction hypothesis, $g\colon B \to B$ is onto. Now let $y \in X$. Then $y = a \vee y \in B$. 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 $f\colon X \to X$, 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 $g := (f - \{\langle c, a\rangle\} - \{\langle a, b\rangle\}) \cup \{\langle c, b\rangle\}$.

Remark. In case the formal use of ordered pairs is difficult for the reader accustomed to functional notation, we put the matter informally: We have $a = f(c)$ and $b = f(a)$, and we make g agree with f except at a and c, where we make $g(c) = b$. Thus having eliminated a from both domain and range, we will be able to show $g\colon B \to B$. The formal details follow.

We have $\text{Rel}(g)$, since by hypothesis $\text{Rel}(f)$. I say $\text{dom}(g) = B$. By extensionality, it suffices to show

$$\exists y\, (\langle t, y\rangle \in g) \leftrightarrow t \in B. \tag{63}$$

Left to right. Assume $\langle t, y\rangle \in g$. Then $(\langle t, y\rangle \in f \wedge \langle t, y\rangle \neq \langle c, a\rangle \wedge \langle t, y\rangle \neq \langle a, b\rangle) \vee (t = c \wedge y = b)$. 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: $\langle t, y\rangle \in f \wedge \langle t, y\rangle \neq \langle c, a\rangle \wedge \langle t, y\rangle \neq \langle a, b\rangle$. Then $t \in X$ since $\text{dom}(f) = X$. 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 (63).

Right to left. Suppose $t \in B$. Since $\text{dom}(f) = X$ 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 (63). That completes the proof that $\text{dom}(g) = B$.

Now I say that $g\colon B \to B$. Suppose $x \in B$. We must show there exists y with $\langle x, y\rangle \in g$. Since $f\colon X \to X$, there exists $y \in X$ such that $\langle x, y\rangle \in f$. Then $x = c \vee x \neq c$. 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 $g\colon B \to B$.

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 $\text{dom}(g) = B$. 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 $\text{Rel}(g)$, and $\text{dom}(g) = B$, and g is one-to-one, and $g\colon B \to B$. Then by the induction hypothesis, g is onto. Since $f\colon X \to X$, 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. □

Lemma 12.5. Let $B \in \mathsf{FINITE}$ and $a \notin B$. Then $|B \cup \{a\}| = (|B|)^+$.

Proof. We have

$$
\begin{array}{rl}
B \in |B| & \text{by Lemma 4.11,} \\
B \cup \{a\} \in |B \cup \{a\}| & \text{by Lemma 4.11,} \\
B \cup \{a\} \in (|B|)^+ & \text{by definition of successor,} \\
B \cup \{a\} \in \mathsf{FINITE} & \text{by Lemma 3.7,} \\
|B \cup \{a\}| \in \mathbb{F} & \text{by Lemma 4.20,} \\
|B| \in \mathbb{F} & \text{by Lemma 4.20,} \\
(|B|)^+ \in \mathbb{F} & \text{by Lemma 4.19,} \\
B \cup \{a\} \in |B \cup \{a\}| \cap (|B|)^+ & \text{by the definition of intersection,} \\
|B \cup \{a\}| = (|B|)^+ & \text{by Lemma 4.23.}
\end{array}
$$
□

Lemma 12.6. 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. We have

$$
\begin{array}{rl}
n = r^+ & \text{for some } r \in \mathbb{F}\text{, by Lemma 4.17,} \\
m + r^+ \leq m^+ & \text{since } m + n \leq m^+ \text{ and } n = r^+, \\
a \in m + n \wedge b \in m^+ & \text{for some } a \text{ and } b\text{, by definition of addition,} \\
m^+ \in \mathbb{F} & \text{by Lemma 4.19,} \\
m + r^+ + k = m^+ & \text{for some } k \in \mathbb{F}\text{, by Lemma 8.22,} \\
(m + r + k)^+ = m^+ & \text{by Lemma 8.2,} \\
m + r \in \mathbb{F} & \text{by Lemma 8.8,} \\
m + r + k^+ = m^+ & \text{by Lemma 8.2,} \\
m + r + k^+ \in \mathbb{F} & \text{since } m + r + k^+ = m^+ \in \mathbb{F}, \\
m + r + k \in \mathbb{F} & \text{by Lemma 8.9,} \\
m + r + k = m & \text{by Lemma 5.11,} \\
r + k + m = \mathsf{zero} + m & \text{by Lemma 8.2,} \\
m + r \in \mathbb{F} \wedge r + k \in \mathbb{F} & \text{by Lemma 8.7,} \\
r + k + m \in \mathbb{F} & \text{by commutativity and associativity, since } m + r + k \in \mathbb{F}, \\
r + k = \mathsf{zero} & \text{by Lemma 8.16,} \\
(m + r)^+ \leq m^+ & \text{by Lemma 8.2,} \\
m + r^+ \in \mathbb{F} & \text{since } m + n \in \mathbb{F}, \\
m + r \in \mathbb{F} & \text{by Lemma 8.9,} \\
m + r = m & \text{by Lemma 5.11,} \\
m + r = m + \mathsf{zero} & \text{by Lemma 8.2,} \\
r = \mathsf{zero} & \text{by Lemma 8.16,} \\
n = r^+ = \mathsf{zero}^+ = \mathsf{one} & \text{since } \mathsf{one} = \mathsf{zero}^+, \\
r = \mathsf{zero} & \text{by Lemma 10.27,} \\
r^+ = \mathsf{one} & \text{by the definition of } \mathsf{one}, \\
n = \mathsf{one} & \text{since } n = r^+.
\end{array}
$$
□

Lemma 12.7. Let $X \in \mathsf{FINITE}$ and let Z be a separable subset of X. Then $|Z| \le |X|$.

Proof. We have

$$\begin{aligned} |X| &\in \mathbb{F} && \text{by Lemma 4.20,}\\ Z &\in \mathsf{FINITE} && \text{by Lemma 3.20,}\\ |Z| &\in \mathbb{F} && \text{by Lemma 4.20,}\\ X &\in |X| && \text{by Lemma 4.11,}\\ Z &\in |Z| && \text{by Lemma 4.11,}\\ |Z| &\le |X| && \text{by the definition of } \le. \end{aligned}$$

□

Theorem 12.8. Let X be a finite set, and let $f\colon X \to X$ be onto, with $\mathrm{dom}(f) \subseteq X$. Then f is one-to-one.

Proof. We prove the more general fact that if X and Y are finite sets with $|X| \le |Y|$, and $f\colon X \to Y$ 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

$$\begin{aligned} \forall Y \in \mathsf{FINITE}\, \forall X \in \mathsf{FINITE}\, \big(|X| \le |Y| \to \forall f\, \big(f \in \mathsf{FUNC} &\to \mathrm{Rel}(f) \to \mathrm{dom}(f) \subseteq X\\ &\to \forall x \in X\, \exists y \in Y\, (\langle x, y\rangle \in f)\\ &\to \forall y \in Y\, \exists x \in X\, (\langle x, y\rangle \in f)\\ &\to \forall y \in Y\, \forall x, z \in X\, (\langle x, y\rangle \in f \to \langle z, y\rangle \in f \to x = z)\big)\big). \end{aligned}$$

The formula is stratified, giving x, y, z index 0, f index 3, X and Y index 1, and $|X|$ and $|Y|$ index 2. FUNC and FINITE are parameters; $\mathrm{Rel}(f)$ is stratified giving f index 3; $\mathrm{dom}(f) \subseteq X$ 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: $Y = \varnothing$. 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. Let $Y = B \cup \{a\}$ with $a \notin B$ and $B \in \mathsf{FINITE}$. Suppose $X \in \mathsf{FINITE}$, and $f\colon X \to Y$ is onto, and $f \in \mathsf{FUNC}$ and $\mathrm{Rel}(f)$ and $\mathrm{dom}(f) \subseteq X$. We must prove $f\colon X \to Y$ is one-to-one. Define

$$Z := \{x \in X : \langle x, a\rangle \in f\}. \tag{64}$$

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,

$$\forall x \in X\, (\langle x, a\rangle \in f \vee \langle x, a\rangle \notin f). \tag{65}$$

To prove that, let $x \in X$. Since $f\colon X \to Y$, 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 $y = a \vee y \ne a$ by Lemma 3.3. That completes the proof of (65). Then by Lemma 3.20, $Z \in \mathsf{FINITE}$ and $X - Z \in \mathsf{FINITE}$.

Let g be f restricted to $X - Z$. Then $g\colon X - Z \to B$ and g is onto B. I say that

$$|X - Z| \ne |X|. \tag{66}$$

To prove that, assume $|X - Z| = |X|$. Then

$$\begin{aligned} |X - Z| &\in \mathbb{F} && \text{by Lemma 4.20,}\\ |X| &\in \mathbb{F} && \text{by Lemma 4.20,}\\ X &\sim X - Z && \text{by Lemma 4.9,}\\ u &\in Z && \text{for some } u \in X, \text{ since } f \text{ is onto } Y,\\ X - Z &\subseteq X && \text{by the definition of } Z,\\ X &\ne X - Z && \text{since } u \notin X - Z \text{ but } u \in X. \end{aligned}$$

Therefore X is similar to a proper subset of X. Then by Definition 3.24, X is infinite. Then by Theorem 3.25, X is not finite. But that contradicts the hypothesis. That completes the proof of (66).

Now I say that $|X - Z| \le |B|$. To prove that:

$$
\begin{array}{rl}
|X - Z| \le |X| & \text{by Lemma 12.7,}\\
|X - Z| < |X| & \text{by (66) and the definition of } <,\\
|X| \le |B \cup \{a\}| & \text{by hypothesis,}\\
|B \cup \{a\}| = (|B|)^+ & \text{since } a \notin B,\\
|X - Z| < |B|^+ & \text{by the previous two lines,}\\
|X - Z| \le |B| & \text{by Lemma 12.6.}
\end{array}
$$

Therefore we can apply the induction hypothesis to g. Hence $g\colon X - Z \to B$ is one-to-one. Therefore g is a similarity. Then

$$
\begin{array}{rl}
|X - Z| = |B| & \text{by Lemma 4.9 and ten omitted steps,}\\
|X| = |X - Z| + |Z| & \text{by Lemma 8.15,}\\
|X| = |B| + |Z| & \text{by the previous two lines,}\\
|X| \le |Y| & \text{by hypothesis,}\\
|B| + |Z| \le |Y| & \text{by the previous two lines,}\\
|Y| = |B|^+ & \text{since } Y = B \cup \{a\} \text{ and } a \notin B,\\
|B| + |Z| \le |B|^+ & \text{by the previous two lines,}\\
|Z| = \mathsf{one} & \text{by Lemma 12.6.}
\end{array}
$$

By Lemma 6.5, Z is a unit class $\{c\}$ for some c. By (64), $\forall x\,(\langle x, a\rangle \in f \leftrightarrow x = c)$. 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 $y = a \vee y \ne a$. 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: $y \ne a$. 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. □

Theorem 12.9. Let X and Y be finite sets, and suppose $f\colon X \to Y$ is onto, and the domain of f is X. Then $|Y| \le |X|$.

Proof. By induction on finite sets X, we prove the theorem for all Y.

Base case. If $f\colon \varnothing \to Y$ has domain $\varnothing$ and is onto Y then $Y = \varnothing$, so $|X| = |Y| = |\varnothing| = \mathsf{zero}$.

Induction step. Suppose $c \notin X$ and f has domain $X \cup \{c\}$, and $f\colon X \cup \{c\} \to Y$ is onto. Let g be f restricted to X, which is conveniently defined as $f \cap X \times Y$. Then the domain of g is exactly X.

We have $f\colon X \cup \{c\} \to Y$, from which it follows in a few steps that also $g\colon X \to Y$. Then by Lemma 12.3, the image $g(X)$ of X under g is a decidable subset of Y. (That lemma requires that the domain of g be exactly X, not larger, which is why we had to use g instead of f.) That is, $(\exists x \in X\; g(x) = f(c)) \vee (\neg\exists x \in X\; g(x) = f(c))$. We argue by cases, as justified by that disjunction.

Case 1: $\exists x \in X\, g(x) = f(c)$. Then $g\colon X \to Y$ is onto. Then

$$\begin{aligned} |Y| &\le |X| && \text{by the induction hypothesis,}\\ |X| &< |X|^+ && \text{by Lemma 5.27,}\\ |X|^+ &= |X \cup \{c\}| && \text{by Lemma 4.13,}\\ |Y| &\le |X \cup \{c\}| && \text{by the preceding lines.} \end{aligned}$$

That completes Case 1.

Case 2: $\neg\,\exists x \in X\, g(x) = f(c)$. Let $t = f(c)$. Then $g\colon X \to Y - \{t\}$ is onto. We have $Y - \{t\} \in \mathsf{FINITE}$ by Lemma 3.32. Then $g\colon X \to Y - \{t\}$ and g is onto, as one can check, and the domain of g is X. Then by the induction hypothesis, $|Y - \{t\}| \le |X|$. We want to take the successor of both sides, but to do that we have to check that those successors are inhabited.

$$\begin{aligned} Y \text{ has decidable equality} &&& \text{by Lemma 3.3,}\\ (Y - \{t\}) \cup \{t\} = Y &&& \text{by decidable equality on } Y,\\ \exists u\,(u \in |X|^+) &&& \text{namely } u = X \cup \{c\},\\ \exists u\,(u \in |Y - \{t\}|^+) &&& \text{namely } u = (Y - \{t\}) \cup \{t\} = Y,\\ |X|^+ \in \mathbb{F} &&& \text{by Lemma 4.19,}\\ |Y - \{t\}|^+ \in \mathbb{F} &&& \text{by Lemma 4.19.} \end{aligned}$$

Now we can take the successors:

$$|Y - \{t\}|^+ \le |X|^+ \qquad \text{by Lemma 5.10,} \tag{67}$$

$$\begin{aligned} Y &\in |Y| && \text{by Lemma 4.11,}\\ (Y - \{t\}) \cup \{t\} &\in |Y - \{t\}|^+ && \text{by definition of successor,}\\ Y &\in |Y - \{t\}|^+ && \text{since } (Y - \{t\}) \cup \{t\} = Y,\\ |Y - \{t\}|^+ &= |Y| && \text{by Lemma 4.23,}\\ |Y| &\le |X|^+ && \text{by (67) and the preceding line,}\\ |X \cup \{c\}| &= |X|^+ && \text{by Lemma 4.13,}\\ |Y| &\le |X \cup \{c\}| && \text{since } |Y| \le |X|^+ = |X \cup \{c\}|. \end{aligned}$$

That completes the induction step. □

Lemma 12.10. Let A and B be finite sets, and let f be a function mapping A onto B. Then $|B| \le |A|$.

Proof. We may assume without loss of generality that A is the domain of f. Then

$$\begin{aligned} f &\in \mathsf{FINITE} && \text{by Lemma 12.2,}\\ A \times B &\in \mathsf{FINITE} && \text{by Lemma 11.3,}\\ f &\in \mathsf{FINITE} && \text{by Lemma 12.2,}\\ f &\in \mathcal{P}_s(A \times B) && \text{by Lemma 3.19.} \end{aligned}$$

That is, f is a decidable relation on $A \times B$. Define $Z := \{s \in B : \exists b \in A\,(\langle b, s\rangle \in f)$. By Lemma 12.3, since f is a decidable relation on $A \times B$, Z is a separable subset of B. That is,

$$\forall t \in B\,(t \in Z \vee t \notin Z). \tag{68}$$

Now we will proceed by induction on finite sets A to prove that for all finite sets B and all $g\colon A \to B$ onto, $|B| \le |A|$.

Base case. If $g\colon \varnothing \to B$ is onto, then $B = \varnothing$, so $|A| = |B| = |\varnothing|$.

Induction step. Let $g\colon A \cup \{c\} \to B$ be onto, where $c \notin A$. Let $t = g(c)$ and let $f = g - \{\langle c, t\rangle\}$. Then $f\colon A \to B$. By (68), $t \in Z \vee t \notin Z$. That is, $\exists b \in A\,(\langle b, t\rangle \in f) \vee \neg\exists b \in A\,(\langle b, t\rangle \in f)$. We may therefore argue by these two cases.

Case 1. If there exists $b \in A$ with $f(b) = t$, then $f\colon A \to B$ is onto, so by the induction hypothesis $|B| \le |A| < (|A|)^+ = |A \cup c|$, as desired.

Case 2. If there does not exist such a b then $f\colon A \to (B - \{t\})$ is onto. Also $B - \{t\}$ is a finite set, by Lemma 3.21. Hence by the induction hypothesis, $|B - \{t\}| \le |A|$. Then $B = (B - \{t\}) \cup \{t\}$, since equality on the finite set B is decidable, so

$$\begin{aligned} |B| &= |B - \{t\}|^+, && \\ |B - \{t\}|^+ &\le (|A|)^+ && \text{by Lemma 5.10,} \\ |B| &\le (|A|)^+ && \text{by the previous two lines,} \\ |A|^+ &= |A \cup \{c\}| && \text{by Lemma 4.13, since } c \notin A, \\ |B| &\le |A \cup \{c\}| && \text{by the previous two lines.} \end{aligned}$$

That completes Case 2, and that completes the induction step. □

Lemma 12.11. Let X be a finite set and let a and b be finite subsets of X. Then $a \cup b$ is finite.

Remark. We cannot prove the union of two finite sets is finite without some additional hypothesis, for consider $\{p\} \cup \{q\}$, where we do not know whether $p = q$ or not, e.g., $p = \varnothing$ and $q = \{x : x = \{\varnothing\} \wedge P\}$, where P is Goldbach's conjecture or the Riemann hypothesis. Does the union contain one or two elements?

Proof of Lemma 12.11. We have

$$\begin{aligned} a &\in \mathcal{P}_s(X) && \text{by Lemma 3.19,} \\ b &\in \mathcal{P}_s(X) && \text{by Lemma 3.19,} \\ \forall x \in X\,(x \in a &\vee x \notin a) && \text{by the definition of } \mathcal{P}_s(X), \\ \forall x \in X\,(x \in b &\vee x \notin b) && \text{by the definition of } \mathcal{P}_s(X), \\ \forall x \in X\,(x \in a \cup b &\vee x \notin a \cup b) && \text{by the preceding lines and logic,} \\ a \cup b &\subset X && \text{by the definition of } \subseteq, \\ a \cup b &\in \mathcal{P}_s(X) && \text{by the definition of } \mathcal{P}_s(X), \\ a \cup b &\in \mathsf{FINITE} && \text{by Lemma 3.20.} \end{aligned}$$

□

Lemma 12.12. Let X be a finite set and let y be a finite subset of $\mathcal{P}_s(X)$ (that is, the members of y are separable subsets of X). Then the union of y is a finite set. That is, $\bigcup y \in \mathsf{FINITE}$.

Proof. By induction on finite sets y (for fixed X).

Base case. When $y = \varnothing$, the union of y is also $\varnothing$, which is finite.

Induction step. Suppose $c \notin y$ and $y \cup \{c\} \subseteq \mathcal{P}_s(X)$. Then

$$\begin{aligned} \textstyle\bigcup (y \cup \{c\}) &= (\textstyle\bigcup y) \cup c && \text{in a few steps from the definitions of } \textstyle\bigcup \text{ and } \cup, && (69) \\ \textstyle\bigcup y &\in \mathsf{FINITE} && \text{by the induction hypothesis,} \end{aligned}$$

$$\begin{array}{rl} c \in \mathcal{P}_s(X) & \text{since } y \cup \{c\} \subseteq \mathcal{P}_s(X), \\ c \in \mathsf{FINITE} & \text{by Lemma 3.20,} \\ y \subseteq \mathcal{P}_s(X) & \text{since } y \cup \{c\} \subseteq \mathcal{P}_s(X), \\ \bigcup y \subseteq X & \text{since } y \subseteq \mathcal{P}_s(X), \\ \bigcup y \cup c \in \mathsf{FINITE} & \text{by Lemma 12.11,} \\ \bigcup (y \cup \{c\}) \in \mathsf{FINITE} & \text{by (69).} \end{array}$$

That completes the induction step. □

13 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 13.1. 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 13.2. For each $m \in \mathbb{F}$, if $m^+ \in \mathbb{F}$ then $\mathbb{J}(m^+) = \mathbb{J}(m) \cup \{m\}$ and $\bar{\mathbb{J}}(m^+) = \bar{\mathbb{J}}(m) \cup \{m^+\}$.

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 5.34. □

Lemma 13.3. 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. Since $\mathbb{F}$ and FINITE are parameters, they do not require an index.

Base case: $m = \mathsf{zero}$. Then $\mathbb{J}(\mathsf{zero}) = \varnothing$, by Lemma 5.35. By Lemma 3.6, $\varnothing \in \mathsf{FINITE}$. 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 13.2, $\mathbb{J}(m^+) = \mathbb{J}(m) \cup \{m\}$, so by Lemma 3.7, $J(m^+) \in \mathsf{FINITE}$. Similarly for $\bar{\mathbb{J}}(m)$. That completes the induction step. □

Lemma 13.4. Suppose $m \in \mathbb{F}$. Then $|\mathbb{J}(m)| = \mathbb{T}^2 m$.

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 $|\mathbb{J}(m)|$ gets index 2, so the two sides of the equation both get index 2. Therefore the lemma may be proved by induction.

Base case. We have $\mathbb{J}(\mathsf{zero}) = \varnothing$, by Lemma 5.30. We have $|\varnothing| = \mathsf{zero}$, by Lemma 4.11 and the definition of zero. By Lemma 10.9, we have $\mathbb{T}^2(\mathsf{zero}) = \mathsf{zero}$. That completes the base case.

Induction step. We have

$\mathbb{J}(m^+) = \mathbb{J}(m) \cup \{m^+\}$	by Lemma 13.2,
$\lvert\mathbb{J}(m)\rvert = \mathbb{T}^2 m$	by the induction hypothesis,
$\mathbb{J}(m) \in \mathbb{T}^2 m$	by Lemma 4.11,
$\exists u\,(u \in m^+)$	assumed for proof by induction,
$m^+ \in \mathbb{F}$	by Lemma 4.19,
$m \notin \mathbb{J}(m)$	by definition of $\mathbb{J}(m)$,
$\mathbb{J}(m) \cup \{m\} \in (\mathbb{T}^2 m)^+$	by definition of successor,
$(\mathbb{T}m)^+ = \mathbb{T}(m^+)$	by Lemma 10.8,
$\mathbb{T}(m^+) \in \mathbb{F}$	by Lemma 10.6,
$(\mathbb{T}m)^+ \in \mathbb{F}$	by the preceding two lines,
$\exists u\,(u \in (\mathbb{T}m)^+)$	by Corollary 4.7,
$(\mathbb{T}^2 m)^+ = \mathbb{T}^2(m^+)$	by Lemma 10.8,
$\mathbb{J}(m^+) \in \mathbb{T}^2(m^+)$	by the preceding lines,
$\mathbb{J}(m^+) \in \lvert\mathbb{J}(m^+)\rvert$	by Lemma 4.11,
$\mathbb{J}(m^+) \in \mathbb{T}^2(m^+) \cap \lvert\mathbb{J}(m^+)\rvert$	by definition of intersection,
$\lvert\mathbb{J}(m^+)\rvert = \mathbb{T}^2(m^+)$	by Corollary 4.7.

That completes the induction step. □

14 Rosser's counting axiom

Rosser [18, p. 485] introduced the "counting axiom", which is $m \in \mathbb{F} \to \mathbb{J}(m) \in m$. In view of Lemma 13.4, 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 [15], so this observation does not help with the problem of finiteness in iNF.

15 Infinity in intuitionistic NF

We use Dedekind's definition, that a set is infinite if it is similar to a proper subset. The *axiom of infinity* says there is an infinite set. Before going further, we remind the reader that with intuitionistic logic, "not finite" does not imply "infinite". There are two obvious candidates for infinite sets: $\mathbb{V}$ and $\mathbb{F}$. Specker showed that, with classical logic, $\mathbb{V}$ is not finite; we will discuss that proof below.

If $\mathbb{F}$ is finite, then by Lemma 5.36, there is a maximal finite cardinal $\mathbf{m}$. Then by Corollary 4.7, $\mathbf{m}$ has a member U, and by Lemma 4.20, U is finite. If we could find some $c \notin U$, then $\mathbf{m}^+$ would be inhabited and hence in $\mathbb{F}$, contradicting the maximality of $\mathbf{m}$. Therefore $\forall x\,\neg\neg\,(x \in U)$; that is, $\mathbb{V}$ is the double complement of U. However unlikely this may seem, nobody has yet been able to find anything contradictory about it, without using classical logic. The following lemma states this remarkable result.

Lemma 15.1. Suppose $\mathbf{m}$ is a maximal element of $\mathbb{F}$, and $U \in \mathbf{m}$. Then $\forall x\,\neg\neg\,(x \in U)$.

Lemma 15.2. Suppose $\mathbf{m}$ is a maximal element of $\mathbb{F}$ and $n \in \mathbb{F}$. Then $\mathbb{T}\mathbf{m} < n$ implies $2^n = \varnothing$.

Proof. Suppose $\mathbb{T}\mathbf{m} < n$ and 2^n is inhabited; we must derive a contradiction.

$$\begin{aligned} \mathcal{P}_1(u) &\in n && \text{for some } u \text{, by definition of exponentiation,}\\ u &\in |u| && \text{by Lemma 4.11,}\\ \mathcal{P}_1(u) &\in \mathbb{T}(|u|) && \text{by definition of } \mathbb{T},\\ \mathbb{T}n &= \mathbb{T}(|u|) && \text{by Lemma 4.23,}\\ \mathbb{T}\mathbf{m} &< \mathbb{T}(|u|) && \text{since } \mathbb{T}\mathbf{m} < n,\\ \mathbf{m} &< |u| && \text{by Lemma 10.20.} \end{aligned}$$

But that contradicts the maximality of $\mathbf{m}$. ☐

Lemma 15.3. If $\mathbb{V}$ is infinite then $\mathbb{F}$ is not finite.

Remark. Note that Specker's proof shows $\mathbb{V}$ is not finite, but not that $\mathbb{V}$ is infinite, which is stronger.

Proof of Lemma 15.3. Suppose $\mathbb{V}$ is infinite and $\mathbb{F}$ is finite, with maximal integer $\mathbf{m}$ and $U \in \mathbf{m}$ and $f : \mathbb{V} \to \mathbb{V}$ with c not in the range of f. Then

$$\begin{aligned} \forall x\, \neg\neg\, (x \in U) & && \text{since } U \in \mathbf{m},\\ \forall x\, (x \in U \to \neg\neg\, (f(x) \in U)) & && \text{by the previous line,}\\ \neg\neg \forall x\, (x \in U \to f(x) \in U) & && \text{by Lemma 3.29,}\\ \neg\neg\, (f : U \to U) & && \text{by definition of } f : U \to U,\\ \neg\neg\, (c \in U) & && \text{since } \forall x\, \neg\neg\, (x \in U). \end{aligned}$$

That implies that U is not not infinite. But since U is finite, it is not infinite, by Theorem 3.25. ☐

Lemma 15.4. With classical logic, if $\mathbb{V}$ is not finite then $\mathbb{F}$ is not finite.

Proof. Suppose $\mathbb{V}$ is not finite and $\mathbb{F}$ is finite. Let $\mathbf{m}$ be the maximal integer and $U \in \mathbf{m}$. Then U is finite and $\forall x\, \neg\neg\, (x \in U)$. Then by classical logic, $\mathbb{V} = U$, contradiction, since U is finite and $\mathbb{V}$ is not. ☐

But constructively, the situation is more complicated: we can prove $\mathbb{V}$ is not finite, but it is an open problem whether $\mathbb{F}$ is finite or not.

To prove $\mathbb{F}$ is infinite, we would hope to prove that successor maps $\mathbb{F}$ into $\mathbb{F}$, so it is of some interest whether that follows from the apparently weaker proposition that $\mathbb{F}$ is not finite. We cannot answer that question: it is an open problem whether

$$\mathbb{F} \in \mathsf{FINITE} \to \forall x \in \mathbb{F}\, (x^+ \in \mathbb{F}).$$

In other words, as far as we know, it might be that $\forall U \in \mathsf{FINITE}\, (\mathbb{V} - U \neq \varnothing)$, but nevertheless we cannot prove $\forall U \in \mathsf{FINITE}\, \exists x\, (x \in \mathbb{V} - U)$. The former is equivalent to successor being nonempty on $\mathbb{F}$, the latter to successor being inhabited on $\mathbb{F}$. We cannot shift the double negation left through $\neg\neg$. (We shall see below that FINITE is not finite, so Lemma 3.29 is no use here.)

Nevertheless, if we did somehow prove that $\mathbb{F}$ is not finite, we *could* prove that Heyting's arithmetic HA is interpretable in $i\mathsf{NF}$. Here is how we would do that:

Recall that $\mathbb{F}$ is the least set containing zero and closed under inhabited successor. Now define $\mathbb{H}$ to be the least set containing zero and closed under nonempty successor. Then we can prove things using $\mathbb{H}$-induction, in which at the induction step one is allowed to assume $x^+ \neq \varnothing$, instead of the usual $\exists u\, (u \in x^+)$. Assume that $\mathbb{F}$ is not finite. We do not give all the details, but here is a sketch: First we prove $\mathbb{F} \subseteq \mathbb{H}$, by $\mathbb{F}$-induction.

Then by $\mathbb{H}$-induction, we prove $\forall x \in \mathbb{H}\,(\neg\neg\, x \in \mathbb{F})$, then $\varnothing \notin \mathbb{H}$; then that $\mathbb{H}$ is closed under successor and has decidable equality, and that successor is one-to-one on $\mathbb{H}$. Then we could use $\mathbb{H}$ as the interpretation of the variables of HA. But that would *still* not prove that $\mathbb{F}$ is closed under successor!

In the sea of open problems, there is an island: the theorem of Specker that $\mathbb{V}$ is not finite. This theorem, proved classically in [19], is widely acknowledged as constructively correct, for reasons I will now explain. Let P be any stratified formula and let $X_P = \{x \in \{\varnothing\} : P\}$. Then X_P is zero or $\varnothing$ according as P or $\neg\, P$. If $\mathbb{V}$ is finite then $\mathbb{V}$ has decidable equality, so by deciding whether $X_P = \varnothing$ or not, we decide $P \vee \neg\, P$. That is, $\mathbb{V}$ finite implies the stratified law of excluded middle. Then, folklore has it, Specker's proof of infinity uses classical logic only for stratified formulas, so it will go through under the assumption that $\mathbb{V}$ is finite, and produce a contradiction.

While this metamathematical argument is appealing, it still requires checking the details of Specker's proof to ensure that classical logic is used only for stratified formulas. I studied Specker's proof, trying to make it constructive, and using Lean to check my proofs. Assume there is a maximal integer $\mathbf{m}$. Then $\mathbf{m}$ has a member U, which is *unenlargeable*, as discussed above. I thought that perhaps U could be made to play the role that $\mathbb{V}$ plays in Specker's proof. That plan did not succeed, unless we assume $\mathbb{V}$ is finite, in which case Specker's proof does provide a Lean-checkable proof that $\mathbb{V}$ is not finite. I chose not to present it here.[13]

Rosser, in an appendix to [18] (but not the first edition [17]), gave another proof that $\mathbb{V}$ is not finite, in which Specker's ideas are recognizable. Rosser proves $\mathbb{V}$ is not finite and then immediately concludes that $\mathbb{F}$ is not finite, since classically $m \in \mathbb{F}$ and $U \in m$, U is finite so $\mathbb{V} - U$ is inhabited, so m^+ is inhabited. The proof that $\mathbb{V}$ is not finite might well be constructive. I did not check it in Lean, since I already checked Specker's proof in Lean.

Once we know that $\mathbb{V}$ is not finite, we can try to prove other sets are not finite. For example, FINITE is not finite, as we shall prove soon.

Lemma 15.5. $\forall x\,(x \in \mathsf{FINITE} \to x \in \mathcal{P}_1(\mathbb{V}) \vee x \notin \mathcal{P}_1(\mathbb{V}))$.

Proof. A set x is a singleton if and only if $|x| = \mathsf{one}$. That is, $\forall x\,(x \in \mathcal{P}_1(\mathbb{V}) \leftrightarrow |x| = \mathsf{one})$ by the definitions of $\mathcal{P}_1$ and one. Since equality on $\mathbb{F}$ is decidable, it is decidable whether a finite set is a singleton or not. Therefore $\forall x\,(x \in \mathsf{FINITE} \to x \in \mathcal{P}_1(\mathbb{V}) \vee x \notin \mathcal{P}_1(\mathbb{V}))$. □

Lemma 15.6. FINITE is not finite.

Remark. This depends on the fact that $\mathbb{V}$ is not finite, which we do not list as a hypothesis, since it is a theorem, even if the proof has not been presented here.

Proof of Lemma 15.6. Assume FINITE is finite. We must derive a contradiction. We have

$$\begin{aligned} \mathcal{P}_1(\mathbb{V}) &\subseteq \mathsf{FINITE} && \text{by Lemma 3.9,} \\ \mathcal{P}_1(\mathbb{V}) &\in \mathcal{P}_s(\mathsf{FINITE}) && \text{by Lemma 15.5,} \\ \mathcal{P}_1(\mathbb{V}) &\in \mathsf{FINITE} && \text{by Lemma 3.20, since } \mathsf{FINITE} \in \mathsf{FINITE}, \\ \mathbb{V} &\in \mathsf{FINITE} && \text{by Lemma 3.11.} \end{aligned}$$

□

16 Conclusions

This paper lays the foundations for future studies of intuitionistic NF set theory $i\mathsf{NF}$, by providing coherent definitions for the basic concepts, including order, exponentiation, addition, finite sets, and $\mathbb{T}$. The concept of separability plays an important role in order and power set, and hence in exponentiation as well. The theory

[13] It is not very short; the details are in no doubt; it leads to an even lengthier discussion of the problem of infinity, but not to a solution of that problem.

presented here — if supplemented by a proof that the set of integers is not finite — would serve well as a basis for formalizing constructive mathematics in the style of Bishop. These basic theorems will surely be both useful and necessary for deeper investigations of the metamathematical properties of iNF. That subject has yet to begin, as at present we cannot even show that the law of the excluded middle is not provable in iNF.

Acknowledgements. 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 [4], which has enabled me to state with high confidence that there are no errors in this paper. Thanks to the users of Lean who helped me acquire sufficient expertise in using Lean by answering my questions, especially Mario Carneiro.

References

[1] T. Adlešić & V. Čačić. A modern rigorous approach to stratification in NF/NFU. *Log. Univers.* 16:3 (2022), pp. 451–468. DOI: 10.1007/s11787-022-00310-y.

[2] M. Beeson. *Foundations of Constructive Mathematics: Metamathematical Studies*. Ergebnisse der Mathematik und ihrer Grenzgebiete, Vol. 6. Berlin, Heidelberg: Springer, 1985. DOI: 10.1007/978-3-642-68952-9.

[3] M. Beeson. *Intuitionistic* NF *set theory*. 2021. arXiv: 2104.00506v4.

[4] L. M. de Moura, S. Kong, J. Avigad, F. van Doorn & J. von Raumer. The Lean theorem prover (system description). In: *25th International Conference on Automated Deduction, Berlin, Germany, August 1–7, 2015, Proceedings*. Springer, Cham, 2015, pp. 378–388. DOI: 10.1007/978-3-319-21401-6_26.

[5] D. Dzierzgowski. Intuitionistic typical ambiguity. *Arch. Math. Log.* 31:2 (1992), pp. 171–182. DOI: 10.1007/BF01269945.

[6] D. Dzierzgowski. Models of intuitionistic TT and NF. *J. Symb. Log.* 60:2 (1995), pp. 640–653. DOI: 10.2307/2275855.

[7] D. Dzierzgowski. Finite sets and natural numbers in intuitionistic TT. *Notre Dame J. Form. Log.* 37:4 (1996), pp. 585–601. DOI: 10.1305/ndjfl/1040046143.

[8] T. Forster. Quine's new foundations. In: E. N. Zalta & U. Nodelman, eds. *The Stanford Encyclopedia of Philosophy*. Summer 2019 edition. URL: https://plato.stanford.edu/archives/sum2019/entries/quine-nf/.

[9] T. E. Forster. *N.F.* PhD thesis. University of Cambridge, 1976.

[10] T. E. Forster. *Set Theory With a Universal Set: Exploring an Untyped Universe*. Second edition. Oxford Logic Guides, Vol. 31. Oxford Science Publications, 1995. DOI: 10.1093/oso/9780198514770.001.0001.

[11] T. E. Forster. A tutorial on constructive NF. In: M. Crabbé & T. Forster, eds. *Proceedings of the 70th Anniversary* NF *Meeting in Cambridge*. Cahiers du Centre de Logique, Vol. 16. Louvain-la-Neuve: Academia-Bruylant, 2009.

[12] C. Grabmayer, J. Leo, V. van Oostrom & A. Visser. On the termination of Russell's description elimination algorithm. *Rev. Symb. Log.* 4:3 (2011), pp. 367–393. DOI: 10.1017/S1755020310000286.

[13] M. R. Holmes. *Bibliography of set theories with a universal set*. Accessed October 2025. URL: https://randall-holmes.github.io/Bibliography/setbiblio.html.

[14] R. Holmes & S. Wilshaw. *New foundations is consistent*. Accessed June 15, 2025. URL: https://tinyurl.com/holmes-wilshaw-nf.

[15] S. Orey. New foundations and the axiom of counting. *Duke Math. J.* 31:4 (1964), pp. 655–660. DOI: 10.1215/S0012-7094-64-03163-1.

[16] J. B. Rosser. The axiom of infinity in Quine's new foundations. *J. Symb. Log.* 17:4 (1952), pp. 238–242. DOI: 10.2307/2266610.

[17] J. B. Rosser. *Logic for Mathematicians*. First edition. New York, Toronto, London: McGraw-Hill, 1953.

[18] J. B. Rosser. *Logic for Mathematicians*. Second edition. Minneola, New York: Dover, 1978.

[19] E. P. Specker. The axiom of choice in Quine's new foundations for mathematical logic. *Proc. Natl. Acad. Sci. U.S.A.* 39:9 (1953), pp. 972–975. DOI: 10.1073/pnas.39.9.972.