Notes on Constructive Set Theory
DRAFT

Peter Aczel and Michael Rathjen

June 18, 2008

Contents

1 Introduction

The general topic of Constructive Set Theory originated in the seminal 1975 paper of John Myhill, where a specific axiom system CST was introduced. Constructive Set Theory provides a standard set theoretical framework for the development of constructive mathematics in the style of Errett Bishop[1] and is one of several such frameworks for constructive mathematics that have been considered. It is distinctive in that it uses the standard first order language of classical axiomatic set theory [2] and makes no explicit use of specifically constructive ideas. Of course its logic is intuitionistic, but there is no special notion of construction or constructive object. There are just the sets, as in classical set theory. This means that mathematics in constructive set theory can look very much like ordinary classical mathematics. The advantage of this is that the ideas, conventions and practise of the set theoretical presentation of ordinary mathematics can be used also in the set theoretical development of constructive mathematics, provided that a suitable discipline is adhered to. In the first place only the methods of logical reasoning available in intuitionistic logic should be used. In addition only the set theoretical axioms allowed in constructive set theory can be used. With some practise it is not difficult for the constructive mathematician to adhere to this discipline.

Of course the constructive mathematician is concerned to know that the axiom system she is being asked to use as a framework for presenting her mathematics makes good constructive sense. What is the constructive notion of set that constructive set theory claims to be about? The first first author believes that he has answered this question in a series of three papers on the Type Theoretic Interpretation of Constructive Set Theory. These papers are based on taking Martin-Löf's Constructive Type Theory as the most acceptable foundational framework of ideas that make precise the constructive approach to mathematics. They show how a particular type of the type theory can be used as the type of sets forming a universe of objects to interprete constructive set theory so that by using the Curry-Howard 'propositions as types' idea the axioms of constructive set theory get interpreted as provable propositions.

Why not present constructive mathematics directly in the type theory? This is an obvious option for the constructive mathematician. It has the drawback that there is no extensive tradition of presenting mathematics in

[1]See *Constructive Analysis*, by Bishop and Bridges

[2]Myhill's original paper used some other primitives in CST besides the notion of set. But this was inessential and we prefer to keep to the standard language in the axiom systems that we use.

a type theoretic setting. So, many techniques for representing mathematical ideas in a set theoretical language have to be reconsidered for a type theoretical language. This can be avoided by keeping to the set theoretical language.

Surprisingly there is still no extensive presentation of an approach to constructive mathematics that is based on a completely explicitly described axiom system - neither in constructive set theory, constructive type theory or any other axiom system.

One of the aims of these notes is to initiate an account of how constructive mathematics can be developed on the basis of a set theoretical axiom system. At first we will be concerned to prove each basic result relying on as weak an axiom system as possible. But later we will be content to explore the consequences of stronger axiom systems provided that they can still be justified on the basis of the type theoretic interpretation. Because of the open ended nature of constructive type theory we also think of constructive set theory as an open ended discipline in which it may always be possible to consider adding new axioms to any given axiom system.

In particular there is current interest in the formulation of stronger and stronger notions of type universes and hierarchies of type universes in type theory. This activity is analogous to the pursuit of ever larger large cardinal principles by classical set theorists. In the context of constructive set theory we are led to consider set theoretical notions of universe. As an example there is the notion of inaccessible set of Rathjen (see [61]). An aim of these notes is to lay the basis for a thorough study of the notion of inaccessible set and other notions of largeness in constructive set theory.

A further motivation for these notes is the current interest in the development of a 'formal topology' in constructive mathematics. It would seem that constructive set theory may make a good setting to represent formal topology. We wish to explore the extent to which this is indeed the case.

These notes represent work in progress and are necessarily very incomplete and open to change.

2 Intuitionistic Logic

2.1 Constructivism

Up till the early years of the 20th century, there was just “one true logic”, *classical logic* as it came to be called later. In that logic, any statement was either true or false. The law of excluded middle, $A \vee \neg A$, had been a pillar of logic for more than 2000 years. It was because of questioning by Brouwer, a Dutch mathematician, that *intuitionism* or *intuitionistic mathematics* arose about the year 1907. Brouwer rejected the use of the law of excluded middle and in particular that of indirect existence proofs in mathematics. He is particularly notorious for basing mathematics on principles that are false classically.

Constructivism did not originate with Brouwer though. As the nineteenth century began, virtually all of mathematical research was of a concrete, constructive, algorithmic nature. By the end of that century much abstract, non-constructive, non-algorithmic mathematics was under development. Middle nineteenth century and early twentieth century mathematics look quite different. In addition to the growth of new subjects, there is a growing preference for short conceptual non-computational proofs (often indirect) over long computational proofs (usually direct). Besides Brouwer, such great names as Kronecker, Poincaré, Clebsch, Gordan, E. Borel had reservations about the non-computational methods. But only a few tried their hand at systematic development of mathematics from a constructive point of view.

Intuitionists trace their constructive lineage at least as far back as Leopold Kronecker (1823-91), who initiated a programme for arithmetizing higher algebra; in this, he demanded for arithmetic a primacy irreducible to natural science or logic and refused to countenance non-constructive existence proofs. He developed much of algebra and algebraic number theory as a subject dealing with finite manipulations of finite expressions. Writings of the so-called semi-intuitionists, particularly Poincaré and Borel, exerted a strong influence on Brouwer and his followers.

Brouwer’s motivation for intuitionism was always a philosophical one. Still in the 1970s, Michael Dummett in his *Elements of intuitionism* [19] maintained that intuitionism would be pointless without a philosophical motivation. In [19], Dummett argues that intuitionism survives as the only tenable position among the rival over-all philosophies of mathematics known as logicism, formalism, and intuitionism.

Bishop’s constructive mathematics (see [11]) challenges this attitude. He advocates constructive mathematics because it supports the computational view of mathematics.

In general, the demand for constructivism is the demand that E be respected:

> (E) *The correctness of an existential claim* $(\exists x \in A)\varphi(x)$ *is to be guaranteed by warrants from which both an object* $x \in A$ *and a further warrant for* $\varphi(x)$ *are constructible.*

Or as Bishop ([11], p. 5) put it:

> *When a man proves a positive integer to exist, he should show how to find it. If God has mathematics of his own that needs to be done, let him do it himself.*

Here is an example of a non-constructive existence proof that one finds in almost every book and article concerned with constructive issues.[3]

Proposition: 2.1 *There exist irrational numbers* $\alpha, \beta \in \mathbb{R}$ *such that* α^β *is rational.*

Proof: $\sqrt{2}$ is irrational, and ${\sqrt{2}}^{\sqrt{2}}$ is either rational or irrational. If it is rational, let $\alpha := \beta := \sqrt{2}$. If not, put $\alpha := {\sqrt{2}}^{\sqrt{2}}$ and $\beta := \sqrt{2}$. Thus in either case a solution exists. $\square$

The proof provides two pairs of candidates for solving the equation $x^y = z$ with x and y irrational and z, without giving us a means of determining which. Due to a non-trivial result of Gelfand and Schneider it is known that ${\sqrt{2}}^{\sqrt{2}}$ is transcendental, and thus the first pair provides the answer.

Similarly classical proofs of disjunctions can be unsatisfactory. H. Friedman pointed out that classically either $e - \pi$ or $e + \pi$ is a irrational number since assuming that both $e - \pi$ and $e + \pi$ are rational entails the contradiction that e is rational. But to this day we don't which of these numbers is irrational.

Another example is the standard proof of the Bolzano-Weierstraß Theorem.

Examples: 2.2 *If* S *is an infinite subset of the closed interval* $[a, b]$*, then* $[a, b]$ *contains at least one point of accumulation of* S*.*

[3]Dummett [19] writes that this example is due to Peter Rososinski and Roger Hindley.

Proof: We construct an infinite nested sequence of intervals $[a_i, b_i]$ as follows:

Put $a_0 = a$, $b_0 = b$. For each i, consider two cases:

(i) if $[a_i, \frac{1}{2}(a_i + b_i)]$ contains infinitely many points of S, put $a_{i+1} = a_i$, $b_{i+1} = \frac{1}{2}(a_i + b_i)$.

(ii) if $[a_i, \frac{1}{2}(a_i + b_i)]$ contains only finitely many points of S, put $a_{i+1} = \frac{1}{2}(a_i + b_i)$, $b_{i+1} = b_i$.

By induction on i, it is plain that each interval $[a_i, b_i]$ contains infinitely many points of S. This being a sequence of nested intervals, it converges to a point every neighbourhood of which contains infinitely many points of S. $\square$

The foregoing proof specifies a 'method' which we cannot, in general, carry out, because we may be unable to decide whether case (i) or case (ii) applies. The 'method' enlists a principle of omniscience (see Definition 2.7).

2.2 The Brouwer-Heyting-Kolmogorov interpretation

The notion of a mathematical proposition is a semantic notion. In a first approach, a proposition could be construed as a meaningful statement describing a state of affairs. Traditionally, a proposition is something that is either true or false. In the case of mathematical statements involving quantifiers ranging over infinite domains, however, by adopting such a view one is compelled to postulate an objective transcendent realm of mathematical objects which determines their meaning and truth value. Most schools of constructive mathematics reject such an account as a myth. Kolmogorov observed that the laws of the constructive propositional calculus become evident upon conceiving propositional variables as ranging over problems or tasks. The constructivists restatement of the meaning of the logical connectives is known as the *Brouwer-Heyting-Kolmogorov interpretation.* It is couched in terms of a semantical notion of proof. It instructive, though, to recast this interpretation in terms of *evidence* rather than proofs.

Definition: 2.3

1. p proves $\perp$ is impossible, so there is no proof of $\perp$.
2. p proves $\varphi \wedge \psi$ iff p is pair $\langle a, b\rangle$, where a is proof for φ and b is proof for ψ.
3. p proves $\varphi \vee \psi$ iff p is pair $\langle n, q\rangle$, where $n = 0$ and q proves φ, or $n = 1$ and q is proves ψ.

4. p proves $\varphi \to \psi$ iff p is a function (or rule) which transforms any proof s of φ into a proof $p(s)$ of ψ.

5. p proves $\neg\varphi$ iff p proves $\varphi \to \bot$.

6. p proves $(\exists x \in A)\varphi(x)$ iff p is a pair $\langle a, q\rangle$ where a is a member of of the set A and q is a proof of $\varphi(a)$.

7. p proves $(\forall x \in A)\varphi(x)$ iff p is a function (rule) such that for each member a of the set A, $p(a)$ is a proof of $\varphi(a)$.

Many objections can be raised against the above definition. The explanations offered for implication and universal quantification are notoriously imprecise because the notion of function (or rule) is left unexplained. Another problem is that the notions of set and set membership are in need of clarification. But in practice these rules suffice to codify the arguments which mathematicians want to call constructive. Note also that the above interpretation (except for $\bot$) does not address the case of atomic formulas.

Definition: 2.4 "BHK" will be short for "Brouwer-Heyting-Kolmogorov". We say that a formula φ is *valid under the BHK-interpretation*, if a construction p can be exhibited that is a proof of φ in the sense of the BHK-interpretation. The construction p is often called a *proof object*.

Examples: 2.5 Here are some examples of the BHK-interpretation. We use λ-notation for functions.

1. The identity map, $\lambda x.x$, is a proof of any proposition of the form $\varphi \to \varphi$ for if a is a proof of φ then $(\lambda x.x)(a) = a$ is a proof of φ.

2. A proof of $\varphi \wedge \psi \to \psi \wedge \varphi$ is provided by the function $f(\langle a, b\rangle) = \langle b, a\rangle$.

3. Any function is a proof of $\bot \to \varphi$ as $\bot$ has no proof.

4. Recall that $\neg\theta$ is $\theta \to \bot$. The law of contraposition

$$(\varphi \to \psi) \to (\neg\psi \to \neg\varphi)$$

   is valid under the BHK-interpretation. To see this, assume that f proves $\varphi \to \psi$, g proves $\neg\psi$, and a proves φ. Then $f(a)$ proves ψ, and hence $g(f(a))$ proves $\bot$. Consequently, $\lambda a.g(f(a))$ proves $\neg\varphi$, and therefore $\lambda g.\lambda a.g(f(a))$ proves $\neg\psi \to \neg\varphi$. As a result, we have shown that the construction $\lambda f.\lambda g.\lambda a.g(f(a))$ is a proof of the law of contraposition.

5. The principle of excluded middle is not valid under a reasonable reading of the BHK-interpretation because given a sentence θ we might not be able to find a proof of θ nor a proof of $\neg\theta$. However, the double negation of that principle is valid under the BHK-interpretation. This may be seen as follows. Suppose g proves $\neg(\psi \vee \neg\psi)$. One easily constructs functions $\mathfrak{f}_0$ and $\mathfrak{f}_1$ such that $\mathfrak{f}_0$ transforms a proof of ψ into a proof of $\psi \vee \neg\psi$ and $\mathfrak{f}_1$ transforms a proof of $\neg\psi$ into a proof of $\psi \vee \neg\psi$, respectively. Thus, $\lambda a.g(\mathfrak{f}_0(a))$ is a proof of $\neg\psi$ while $\lambda b.g(\mathfrak{f}_1(b))$ is a proof of $\neg\psi \to \bot$. Consequently, $g(\mathfrak{f}_1(\lambda a.g(\mathfrak{f}_0(a))))$ is a proof of $\bot$. As a result, $\lambda g.g(\mathfrak{f}_1(\lambda a.g(\mathfrak{f}_0(a))))$ proves $\neg\neg(\psi \vee \neg\psi)$ for any formula ψ.

Exercise: 2.6 *Convince yourself that the following classical laws are not valid under the BHK-interpretations:*

$$\varphi \vee \neg\varphi \qquad \neg\neg\varphi \to \varphi \qquad \neg\varphi \vee \neg\neg\varphi.$$

Show that on the other hand, $\varphi \to \neg\neg\varphi$ *and* $\neg\neg\neg\varphi \to \neg\varphi$ *are valid according to the BHK-interpretation.*

2.3 Counterexamples

Certain basic principles of classical mathematics are taboo for the constructive mathematician. Bishop called them *principles of omniscience*. They can be stated in terms of binary sequences, where a binary sequence is a function $\alpha : \mathbb{N} \to \{0, 1\}$. Below, the quantifier $\forall\alpha$ is supposed to range over all binary sequences and the variables n, m range over natural numbers. Let $\alpha_n := \alpha(n)$.

Definition: 2.7 *Limited Principle of Omniscience* (**LPO**):

$$\forall\alpha\,[\exists n\, \alpha_n = 1 \;\;\vee\;\; \forall n\, \alpha_n = 0].$$

Weak Limited Principle of Omniscience (**WLPO**):

$$\forall\alpha\,[\forall n\, \alpha_n = 0 \;\;\vee\;\; \neg\forall n\, \alpha_n = 0].$$

Lesser Limited Principle of Omniscience (**LLPO**):

$$\forall\alpha\,(\forall n, m[\alpha_n = \alpha_m = 1 \to n = m] \;\to\; [\forall n\, \alpha_{2n} = 0 \;\;\vee\;\; \forall n\, \alpha_{2n+1} = 0]).$$

The following implications hold:

$$\textbf{LPO} \;\Rightarrow\; \textbf{WLPO} \;\Rightarrow\; \textbf{LLPO}. \tag{1}$$

Classically we have the principle

$$\forall x, y \in \mathbb{R}\, [x = y \ \vee \ x \neq y].$$

This principle entails **WLPO** and is thus not acceptable constructively.

One way to make the BHK-interpretation precise is by requiring functions to be computable (recursive). This is the recursive reading of the BHK-interpretation. We will later see that such an interpretation is possible, even for full-fledged set theory. The recursive BHK-interpretation refutes all of the above principles of omniscience.

2.4 Natural Deductions

Though in what follows, intuitionistic reasoning will be carried out mainly informally when developing set theory and constructive mathematics within a system of set theory based on intuitionistic reasoning, it is convenient to have a set of logical rules available, so that we do not have to go back to the Brouwer-Heyting-Kolmogorov interpretation each time we want to justify the use of a logical principle in our arguments.

We present two formal system of rules for intuitionistic logic, the natural deduction calculus and the sequent calculus. Both calculi were invented by Gentzen.

In the following we assume that we are given a language $\mathcal{L}$ of predicate logic (aka first order logic) with equality $=$. Terms are defined as usual. The logical primitives are $\wedge, \vee, \rightarrow, \bot, \forall, \exists$, where $\bot$ stands for absurdity and the negation $\neg\psi$ of a formula ψ is defined by $\psi \rightarrow \bot$. Formulas are then defined as usual. Contrary to the situation in classical logic, none of the connectives and quantifiers of the above list is definable by means of the others.

Definition: 2.8 Natural deduction are pictorially presented as trees labelled with formulas. We want to give a formal definition of *deduction* as well as the *open assumptions* and *cancelled* (=*discharged*) *assumptions* of a deduction. We use $\mathcal{D}, \mathcal{D}_1, \mathcal{D}_2, \ldots$ to range over deductions. We write

$$\begin{array}{c} \mathcal{D} \\ \psi \end{array}$$

to convey that ψ is the conclusion of $\mathcal{D}$.

Deductions are defined inductively as follows:

Basis: The single-node tree with label ψ is a deduction whose sole open assumption is ψ; there are no cancelled assumptions.

Inductive step: Let $\mathcal{D}, \mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3$ be deductions. Then a deduction may be constructed from these by any of the rules below. Some of these rules are subject to restrictions to be specified afterwards.

For $\bot$ we have the *intuitionistic absurdity rule*

$$\frac{\begin{array}{c}\mathcal{D}\\ \bot\end{array}}{\psi}\,\bot_i$$

For the other logical constants the rules can be nicely grouped into introduction and elimination rules:

Introduction Rules (I-rules) | Elimination Rules (E-rules)

$$\frac{\begin{array}{c}\mathcal{D}_1\\ \varphi\end{array}\qquad\begin{array}{c}\mathcal{D}_2\\ \psi\end{array}}{\varphi\wedge\psi}\,\wedge\mathrm{I} \qquad\qquad \frac{\begin{array}{c}\mathcal{D}\\ \varphi\wedge\psi\end{array}}{\varphi}\,\wedge\mathrm{E}_r \qquad \frac{\begin{array}{c}\mathcal{D}\\ \varphi\wedge\psi\end{array}}{\psi}\,\wedge\mathrm{E}_l$$

$$\frac{\begin{array}{c}[\varphi]\\ \mathcal{D}\\ \psi\end{array}}{\varphi\to\psi}\,\to\mathrm{I} \qquad\qquad \frac{\begin{array}{c}\mathcal{D}_1\\ \varphi\to\psi\end{array}\qquad\begin{array}{c}\mathcal{D}_2\\ \varphi\end{array}}{\psi}\,\to\mathrm{E}$$

$$\frac{\begin{array}{c}\mathcal{D}\\ \varphi\end{array}}{\varphi\vee\psi}\,\vee\mathrm{I}_r \qquad \frac{\begin{array}{c}\mathcal{D}\\ \psi\end{array}}{\varphi\wedge\psi}\,\vee\mathrm{I}_l \qquad\qquad \frac{\begin{array}{c}\mathcal{D}_1\\ \varphi\vee\psi\end{array}\qquad\begin{array}{c}[\varphi]\\ \mathcal{D}_2\\ \theta\end{array}\qquad\begin{array}{c}[\psi]\\ \mathcal{D}_3\\ \theta\end{array}}{\theta}\,\vee\mathrm{E}$$

$$\frac{\begin{array}{c}\mathcal{D}\\ \varphi\end{array}}{\forall x\,\varphi}\,\forall\mathrm{I} \qquad\qquad \frac{\begin{array}{c}\mathcal{D}\\ \forall x\,\varphi\end{array}}{\varphi[x/t]}\,\forall\mathrm{E}$$

$$\frac{\begin{array}{c}\mathcal{D}\\ \varphi[x/t]\end{array}}{\exists x\,\varphi}\,\exists\mathrm{I} \qquad\qquad \frac{\begin{array}{c}\mathcal{D}_1\\ \exists x\,\varphi\end{array}\qquad\begin{array}{c}[\varphi]\\ \mathcal{D}_2\\ \theta\end{array}}{\theta}\,\exists\mathrm{E}$$

Next come the rules for equality:

$$\frac{\begin{array}{c}\mathcal{D}\\ t=t\to\psi\end{array}}{\psi}\,\mathrm{Eq}_{refl} \qquad\qquad \frac{\begin{array}{c}\mathcal{D}_1\\ \varphi[x/t]\end{array}\qquad\begin{array}{c}\mathcal{D}_2\\ t=s\end{array}}{\varphi[x/s]}\,\mathrm{Eq}_{repl}$$

The *open* and *cancelled* assumptions of the above deductions are declared as follows:

(i) In the deduction whose last inference rule is $\to$I, the open assumptions are those of $\mathcal{D}$ without φ. φ is a cancelled assumption of the deduction. This is indicated by putting φ in square brackets on top of the deduction. In the deduction whose last inference rule is $\vee$E, the open assumptions are those of $\mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3$ minus the formulas φ and ψ, which are cancelled assumptions of the deduction. The open assumptions of the deduction whose last inference rule is $\exists$E are those of $\mathcal{D}_1$ and $\mathcal{D}_2$ without φ and ψ, which are cancelled assumptions.

If the last inference rule of a deduction is different from $\to$I,$\vee$E, and $\exists$E, then the open and cancelled assumptions are those of the immediate subdeductions combined.

(ii) In the deductions whose last inference rule is $\forall$E $\exists$I, the term t must be free for x in φ. In the deduction whose last inference is Eq_{repl}, t and s must be free for x in φ.

The inference rules $\forall$I and $\exists$E are subject to the following eigenvariable conditions:

(iii) In the deduction whose last inference is $\forall$I, the variable x is an eigenvariable; i.e., x is not to occur free in any of the open assumptions of $\mathcal{D}$. In the deduction whose last inference is $\exists$E, x is an eigenvariable; i.e., x is not to occur free in in θ and in any of the open assumptions of $\mathcal{D}_2$ other than φ.

If φ is among the open assumptions of a deduction $\mathcal{D}$ with conclusion ψ, the conclusion φ is said to *depend on* φ in $\mathcal{D}$. A deduction without open assumptions is said to be *closed*. A formula θ is *deducible* if there is a closed deduction with conclusion θ. We shall convey by writing $\vdash \theta$.

Examples: 2.9 Our first example is a natural deduction of the law of contraposition.

$$\dfrac{\dfrac{\dfrac{\dfrac{\neg\psi \qquad \dfrac{\varphi \to \psi \qquad \varphi}{\psi}\,\to\mathrm{E}}{\bot}\,\to\mathrm{E}}{\neg\varphi}\,\to\mathrm{I}}{\neg\psi \to \neg\varphi}\,\to\mathrm{I}}{(\varphi \to \psi) \to (\neg\psi \to \neg\varphi)}\,\to\mathrm{I}$$

The second example is a deduction of the double negation of the law of excluded middle.

$$\dfrac{\neg(\psi \vee \neg\psi) \qquad \dfrac{\dfrac{\neg(\psi \vee \neg\psi) \qquad \dfrac{\psi}{\psi \vee \neg\psi}\,\vee\mathrm{I}}{\dfrac{\bot}{\neg\psi}\,\to\mathrm{I}}\,\to\mathrm{E}}{\psi \vee \neg\psi}\,\vee\mathrm{I}}{\dfrac{\bot}{\neg\neg(\psi \vee \neg\psi)}\,\to\mathrm{I}}\,\to\mathrm{E}$$

The third example features an application of the intuitionistic absurdity rule $\bot_i$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\psi \wedge \neg\psi}{\psi}\,\wedge\mathrm{E}_r \qquad \dfrac{\psi \wedge \neg\psi}{\neg\psi}\,\wedge\mathrm{E}_l}{\bot}\,\to\mathrm{E}}{\theta}\,\bot_i}{\psi \wedge \neg\psi \to \theta}\,\to\mathrm{I}$$

Lemma: 2.10 *Here is a list of intuitionistic laws that we shall need in the future, and that (of course) have natural deductions.*

1. $\neg\neg(\psi \vee \neg\psi)$
2. $\varphi \to \neg\neg\varphi$
3. $\neg\neg\neg\varphi \leftrightarrow \neg\varphi$
4. $(\neg\neg\psi \to \neg\neg\varphi) \leftrightarrow \neg\neg(\psi \to \varphi) \leftrightarrow (\psi \to \neg\neg\varphi)$
5. $(\psi \to \varphi) \to (\neg\varphi \to \neg\psi)$
6. $\neg\neg(\psi \to \varphi) \to (\psi \to \neg\neg\varphi)$.
7. $\neg\neg(\psi \wedge \varphi) \leftrightarrow (\neg\neg\varphi \wedge \neg\neg\psi)$.
8. $\neg\neg\forall x\varphi(x) \to \forall x\, \neg\neg\varphi(x)$
9. $\neg\exists x\varphi(x) \leftrightarrow \forall x\neg\varphi(x)$
10. $\neg\forall x\neg\varphi(x) \leftrightarrow \neg\neg\exists x\varphi(x)$.
11. $(\psi \vee \neg\psi) \to ([\psi \to \exists x\varphi(x)] \to \exists x[\psi \to \varphi(x)])$

Definition: 2.11 Thus far, we have only considered deductions in pure intuitionistic predicate logic with equality. Given a theory T, i.e. a collection of formulas in a first order language $\mathcal{L}$ with equality, we say that a formula θ is *intuitionistically deducible in* T if there is a deduction $\mathcal{D}$ with conclusion θ whose open assumptions are universal closures of T. We shall convey this by writing $T \vdash \theta$.

Exercise: 2.12 *Find intuitionistic proofs of the implications of (1).*

2.5 A Hilbert-style system for intuitionistic logic

For certain metamathematical purposes, such as showing that a structure satisfies the laws of intuitionistic logic, it is more convenient to work with a system based on axioms and a few rules, where the rules just act locally on the conclusions of derivations and do not involve sequences of formulae nor cancellation of open assumptions elsewhere in the derivation. Such codifications of logic are known by the generic name of Hilbert-type systems.

Definition: 2.13 We introduce a Hilbert-style system for intuitionistic predicate logic with equality.

Axioms

(A1) $\varphi \to (\psi \to \varphi)$

(A2) $(\varphi \to (\psi \to \chi)) \to ((\varphi \to \psi) \to (\varphi \to \chi))$

(A3) $\varphi \to (\psi \to (\varphi \wedge \psi))$

(A4) $(\varphi \wedge \psi) \to \varphi$

(A5) $(\varphi \wedge \psi) \to \psi$

(A6) $\varphi \to (\varphi \vee \psi)$

(A7) $\psi \to (\varphi \vee \psi)$

(A8) $(\varphi \vee \psi) \to ((\varphi \to \chi) \to ((\psi \to \chi) \to \chi))$

(A9) $(\varphi \to \psi) \to ((\varphi \to \neg\psi) \to \neg\varphi)$

(A10) $\varphi \to (\neg\varphi \to \psi)$

(A11) $\forall x\, \varphi \to \varphi[x/t]$

(A12) $\varphi[x/t] \to \exists x\, \varphi$

(Eq1) $t = t$

(Eq2) $s = t \to (\varphi[x/s] \to \varphi[x/t])$

As per usual, the term t must be free for x in φ in axioms (A11) and (A12). $\varphi[x/t]$ denotes the result of substituting t for x throughout φ. Also, the terms s and t must both be free for x in φ in axiom (Eq2).

Inference Rules $\vdash \varphi$ conveys that φ is deducible. All axioms are deducible.

(MP) If $\vdash \varphi$ and $\vdash \varphi \to \psi$, then $\vdash \psi$.

($\forall$I) If $\vdash \psi \to \varphi[x/y]$, then $\vdash \psi \to \forall x\, \varphi$.

($\exists$I) If $\vdash \varphi[x/y] \to \psi$, then $\vdash \exists x\, \varphi \to \psi$.

In ($\forall$I) and ($\exists$I), y is free for x in φ and occurs free in neither φ nor ψ. (MP) stands for "modus ponens".

3 Some Axiom Systems

Constructive Set Theory is a variant of Classical Set Theory which uses intuitionistic logic. It differs from another such variant called Intuitionistic Set Theory because of its avoidance of the full impredicativity that Intuitionistic Set Theory has. Constructive Set Theory does not have the Powerset axiom or the full Separation axiom scheme. We introduce constructive set theory here by contrasting it with the other two theories. Note that we consider each of these theories as a framework and consider representative axiom systems for them, **ZF** and **IZF** for the Classical and Intuitionistic Set Theories and **ECST** and **CZF** for Constructive Set Theory.

3.1 Classical Set Theory

The classical Zermelo-Fraenkel axiomatic set theory, **ZF**, is formulated in first order logic with equality, using a binary predicate symbol $\in$ as its only non-logical symbol. We will use $a \subseteq b$ to abbreviate $\forall u(u \in a \to u \in b)$. **ZF** is based on the following axioms and axiom schemes:

Extensionality

$$\forall a \forall b[\forall x[x \in a \ \leftrightarrow \ x \in b] \to a = b]$$

Pairing

$$\forall a \forall b \exists y \forall u[u \in y \leftrightarrow y = a \ \vee \ y = b]$$

Union

$$\forall a \exists y \forall x[x \in y \leftrightarrow \exists u \in a\,(x \in u)]$$

Powerset

$$\forall a \exists y \forall x\,[x \in y \leftrightarrow x \subseteq a]]$$

Infinity

$$\exists a\ [\exists x\ x \in a \ \wedge \ \forall x \in a \exists y \in a\ x \in y]$$

Foundation

$$\forall a[\exists x[x \in a] \ \to \ \exists x \in a \forall y \in a[y \notin x]]$$

Separation

$$\forall a \exists y \forall x\, [x \in y \;\leftrightarrow\; x \in a \wedge \phi(x)]$$

for all formulae $\phi(x)$, where y is not free in $\phi(x)$.

Replacement

$$\forall x \in a \exists ! y \phi(x, y) \;\rightarrow\; \exists b\, \forall y\, [y \in b \;\leftrightarrow\; \exists x \in a\, \phi(x, y)]$$

for all formulae $\phi(x, y)$, where b is not free in $\phi(x, y)$.

3.2 Intuitionistic Set Theory

A natural Intuitionistic version of **ZF** is Intuitionistic Zermelo-Fraenkel, **IZF**. It is like **ZF** except that the following changes are made.

1. It uses Intuitionistic logic instead of Classical logic.
2. It uses the Set Induction scheme instead of the Foundation axiom.
3. It uses the Collection scheme instead of the Replacement scheme.

Set Induction

$$\forall a\, [\forall x \in a \phi(x) \;\rightarrow\; \phi(a)] \;\rightarrow\; \forall a \phi(a)$$

for all formulae $\phi(a)$.

Collection

$$\forall x \in a \exists y \theta(x, y) \;\rightarrow\; \exists b\, \forall x \in a \exists y \in b\; \theta(x, y)]$$

for all formulae $\phi(x, y)$, where b is not free in $\phi(x, y)$.

3.3 An Elementary Constructive Set Theory

The most important set theory of this book is *Constructive Zermelo-Fraenkel Set Theory*, **CZF**, which takes the place of the standard classical set theory **ZF**. However, before we present a complete list of the axioms of **CZF** we will look at a fragment of it which allows one to carry out basic set-theoretic constructions.

3.3.1 ECST

Our first axiom system is Elementary Constructive Set Theory, **ECST**. It is like **IZF** except for the following changes.

1. It uses the Replacement Scheme instead of the Collection Scheme.
2. It drops the Powerset Axiom and the Set Induction Scheme.
3. It uses the Bounded Separation Scheme instead of the full Separation Scheme.
4. It uses the Strong Infinity axiom instead of the Infinity axiom.

Bounded Separation

$$\forall a \exists y \forall x\, [x \in y \ \leftrightarrow \ x \in a \wedge \phi(x)]$$

for all *bounded* formulae $\phi(x)$, where y is not free in $\phi(x)$. A formula is *bounded* if all its quantifiers are bounded; i.e. occur only in one of the forms $\exists x \in y$ or $\forall x \in y$. Bounded formulae have also been called *restricted* or Δ_0 formulae. Accordingly, Bounded Separation has been variously called *Restricted Separation* or Δ_0 *Separation.*

Strong Infinity

$$\exists a[Ind(a) \wedge \forall b[Ind(b) \rightarrow \forall x \in a(x \in b)]]$$

where we use the following abbreviations.

- $Empty(y)$ for $(\forall z \in y)\bot$,
- $Succ(x, y)$ for $\forall z[z \in y \ \leftrightarrow \ z \in x \vee z = x]$,
- $Ind(a)$ for $(\exists y \in a)Empty(y) \wedge (\forall x \in a)(\exists y \in a)Succ(x, y)$.

Some Consequences of the Axioms

Pairing By Pairing, for a given a and b we get a set y such that

$$\forall x(x \in y \ \leftrightarrow \ x = a \vee x = b).$$

This set is unique by Extensionality; we call this set $\{a, b\}$. $\{a\} = \{a, a\}$ is the set whose unique element is a. $\langle a, b\rangle = \{\{a\}, \{a, b\}\}$ is the *ordered pair* of a and b.

Proposition: 3.1 (**ECST**) *If* $\langle a, b\rangle = \langle c, d\rangle$ *then* $a = c$ *and* $b = d$.

Proof: The usual classical proof argues by cases depending, for example, whether or not $a = b$. This method is not available here as we cannot assume that instance of the classical law of excluded middle. Instead we can argue as follows. Assume that $\langle a, b\rangle = \langle c, d\rangle$.

As $\{a\}$ is an element of the left hand side it is also an element of the right hand side and so either $\{a\} = \{c\}$ or $\{a\} = \{c, d\}$. In either case $a = c$.

As $\{a, b\}$ is an element of the left hand side it is also an element of the right hand side and so either $\{a, b\} = \{c\}$ or $\{a, b\} = \{c, d\}$. In either case $b = c$ or $b = d$. If $b = c$ then $a = c = b$ so that the two sets in $\langle a, b\rangle$ are equal and hence $\{c\} = \{c, d\}$ giving $c = d$ and hence $b = d$. So in either case $b = d$. $\square$

We will also have use for ordered triples $\langle a, b, c\rangle$, ordered quadruples $\langle a, b, c, d\rangle$, etc. They are defined by iterating the ordered pairs formation as follows: $\langle a\rangle = a$ and $\langle a_1, \ldots, a_r, a_{r+1}\rangle = \langle\langle a_1, \ldots, a_r\rangle, a_{r+1}\rangle$.

Union For a given set b the Union axiom postulates the existence of a set y such that $\forall x[x \in y \leftrightarrow \exists u \in b\,(x \in u)]$. By Extensionality, there is exactly one such set, and we will denote it by $\bigcup b$.

Bounded Separation For each set a and each bounded formula ϕ without y free, the Bounded Separation axiom asserts that $\exists y\,\forall x\,[x \in y \;\leftrightarrow\; x \in a \wedge \phi(x)]$. The y asserted to exist is unique by Extensionality, and we denote this y by

$$\{x \in a \mid \phi(x)\} \quad \text{or} \quad \{x \mid x \in a \,\wedge\, \phi(x)\}.$$

Note that $\phi(x)$ may have any number of other variables free. These variables are thought of as parameters upon which the set $\{x \in a \mid \phi(x)\}$ depends.

The restriction on y not being free in ϕ is necessary to avoid inconsistencies as, for example,

$$\exists y \forall x(x \in y \;\leftrightarrow\; x \in a \,\wedge\, x \notin y)$$

would lead to an inconsistency when a is inhabited. In the future, however, we won't bother the reader with these syntactic niceties.

Replacement With the help of the other axioms, Replacement may be used to show the existence of functions. In set theory, functions are viewed as special relations. A *relation* is a set R all of whose elements are ordered pairs. The *domain* and *range* of a relation are defined by

$$\begin{aligned}
\mathbf{dom}(R) &= \{x \mid \exists y\,(\langle x, y\rangle \in R)\}, \\
\mathbf{ran}(R) &= \{y \mid \exists x\,(\langle x, y\rangle \in R)\}.
\end{aligned}$$

$\mathbf{dom}(R)$ and $\mathbf{ran}(R)$ are both sets due to Bounded Separation and Union as $\mathbf{dom}(R) = \{x \in A \mid \exists y \in A\,(\langle x, y\rangle \in R)\}$ and $\mathbf{ran}(R) = \{y \in A \mid \exists x \in A\,(\langle x, y\rangle \in R)\}$ with $A = \bigcup\bigcup R$ (check that $\langle x, y\rangle \in R$ can be expressed via a bounded formula). The definitions make sense for any set R, but are usually used only when R is a relation.

f is a *function* if f is a relation such that

$$\forall x \in \mathbf{dom}(f)\, \exists! y \in \mathbf{ran}(f)\, (\langle x, y\rangle \in f).$$

$f : A \to B$ means that f is a function with $\mathbf{dom}(f) = A$ and $\mathbf{ran}(f) \subseteq B$. As usual, when $x \in \mathbf{dom}(f)$ we write $f(x)$ for the unique y such that $\langle x, y\rangle \in f$.

Lemma: 3.2 (**ECST**) *If $\forall x \in a\, \exists! y\, \phi(x, y)$ then there exists a unique function f with $\mathbf{dom}(f) = a$ such that $\forall x \in a\, \phi(x, f(x))$.*

Proof: Suppose $\forall x \in a\, \exists! y\, \phi(x, y)$. Then

$$\forall x \in a\, \exists! z\, \theta(x, z),$$

where $\theta(x, z)$ is $\exists y\, [z = \langle x, y\rangle \ \wedge\ \phi(x, y)]$. By Replacement there exists a set f such that

$$\forall z\, [z \in f \ \leftrightarrow\ \exists x \in a\, \theta(x, z)].$$

Hence f is a set of ordered pairs. From the above it follows also that f is a function and that $\forall x \in a\, \phi(x, f(x))$. The uniqueness of f is obvious. $\square$

The Union-Replacement Scheme

This is a natural scheme that combines the Union axiom with the Replacement scheme.

$$\forall x \in a\, \exists b \forall y\, [y \in b \ \leftrightarrow\ \phi(x, y)] \ \to\ \exists c\, \forall y\, [y \in c \ \leftrightarrow\ \exists x \in a\, \phi(x, y)].$$

Proposition: 3.3 *Given the Extensionality and Pairing axioms the Union-Replacement axiom scheme is equivalent to the combination of the Union axiom and the Replacement axiom scheme.*

Proof: Assume Union-Replacement and let $\forall x \in a \exists! y\ \phi(x, y)$. Then, as singleton classes are sets,

$$\forall x \in a\, \exists b \forall y [y \in b \ \leftrightarrow\ \phi(x, y)]$$

so that by Union-Replacement

$$\exists c \forall y\, [y \in c \ \leftrightarrow \ \exists x \in a \phi(x, y)].$$

So we have proved Replacement. The Union axiom follows from the instance of Union-replacement where $\phi(x, y)$ is $y \in x$.

Conversely, given the Union axiom and the Replacement scheme, suppose that $\forall x \in a\, \exists b\, \forall y[y \in b \ \leftrightarrow \ \phi(x, y)]$. Then

$$\forall x \in a \exists! b \forall y[y \in b \ \leftrightarrow \ \phi(x, y)].$$

So, by Replacement we may form the set

$$\{z \mid \exists x \in a \forall y[y \in z \ \leftrightarrow \ \phi(x, y)]\}.$$

By the Union axiom we may form the union set of this set, which is

$$\{y \mid \exists x \in a \phi(x, y)\}.$$

Thus we have proved the Union-Replacement axiom scheme. □

So the axiom system **ECST** can be considered to consist of the three axioms of Extensionality, Pairing and Strong Infinity and the two schemes of Bounded Separation and Union-Replacement.

3.3.2 Constructive Zermelo Fraenkel, CZF

For the sake of reference we shall introduce two further axiom schemes which complete the description of the axioms of Constructive Zermelo-Fraenkel Set Theory, **CZF**. **CZF** is obtained from **ECST** as follows.

1. Add the Set Induction scheme,
2. Add the Subset Collection scheme,
3. Use the Strong Collection scheme instead of the Replacement scheme.

Strong Collection

$$\forall x{\in}a\, \exists y\, \phi(x, y) \ \rightarrow \ \exists b\, [\forall x{\in}a\, \exists y{\in}b\, \phi(x, y) \ \wedge \ \forall y{\in}b\, \exists x{\in}a\, \phi(x, y)]$$

for every formula $\phi(x, y)$.

Subset Collection

$$\begin{aligned} &\exists c \forall u\, [\forall x{\in}a\, \exists y{\in}b\, \psi(x, y, u) \ \rightarrow \\ &\qquad \exists d{\in}c\, (\forall x{\in}a\, \exists y{\in}d\, \psi(x, y, u) \ \wedge \ \forall y{\in}d\, \exists x{\in}a\, \psi(x, y, u))] \end{aligned}$$

for every formula $\psi(x, y, u)$.

Note that the respective formulae $\phi(x, y)$ and $\psi(x, y, u)$ in the above schemas may have any number of other variables free.

For the record, let's state that Strong Collection implies Collection as well as Replacement. Note that, on the basis of **ECST** minus Replacement, it does not seem to be possible to obtain Replacement from Collection since this system does not have full Separation.

Lemma: 3.4 *Without any further axioms, Strong Collection implies Collection and Replacement.*

Proof: Obvious. $\square$

While Strong Collection is a well-known theorem of **ZF**, Subset Collection may strike the reader as mysterious. We will later discuss the Subset Collection scheme and show that its instances follow from the Powerset axiom of **ZF** and, moreover, that it can be replaced by a single axiom in the presence of Strong Collection. It will also be shown that Subset Collection implies the important Exponentiation Axiom which postulates that for sets a, b the class of all functions from a to b forms a set.

Exponentiation

$$\forall a \forall b \exists c \forall f \, [f \in c \;\; \leftrightarrow \;\; (f : a \to b)].$$

On notations. In this monograph, special attention is given to know that some of the results we prove from **CZF** do not in fact require all the axioms of **CZF**. We have already singled out the subsystem **ECST**. We list here some abbreviations for commonly used subtheories of a given theory **T**. If P is an axiom, **T**-P consists of the theory with P deleted. By $\mathbf{T}^-$, we mean the the theory with the Set Induction scheme removed. If **T** contains the Collection or Strong Collection scheme, we denote by $\mathbf{T}_R$ the theory resulting from deleting that scheme and then adding Replacement. Likewise, when **T** contains the Subset Collection scheme we mean by $\mathbf{T}_E$ the theory with Subset Collection deleted and then Exponentiation added.

4 Operations on Sets and Classes

We show how to develop some of the standard apparatus for representing mathematical ideas in **ECST**.

4.1 Class Notation

In doing mathematics in Constructive Set Theory we shall exploit the use of class notation and terminology, just as in Classical Set Theory. Given a formula $\phi(x)$ there may not exist a set of the form $\{x \mid \phi(x)\}$. But there is nothing wrong with thinking about such collection. So, if $\phi(x)$ is a formula in the language of set theory we may form a class $\{x \mid \phi(x)\}$. We allow $\phi(x)$ to have free variables other than x, which are considered parameters upon which the class depends. Informally, we call any collection of the form $\{x \mid \phi(x)\}$ a *class*. However formally, classes do not exist, and expressions involving them must be thought of as abbreviations for expressions not involving them.

Classes A, B are defined to be equal if

$$\forall x[x \in A \ \leftrightarrow \ x \in B].$$

We may also consider an augmentation of the language of set theory wherein we allow atomic formulas of the form $y \in A$ and $A = B$ with A, B being classes. There is no harm in taking such liberties as any such formula can be translated back into the official language of set theory by re-writing $y \in \{x \mid \phi(x)\}$ and $\{x \mid \phi(x)\} = \{y \mid \psi(y)\}$ as $\phi(y)$ and $\forall z\,[\phi(z) \ \leftrightarrow \ \psi(z)]$, respectively (with z not in $\phi(x)$ and $\psi(y)$).

In particular each set a is identified with the class $\{x \mid x \in a\}$. Also, A is a subclass of B, written $A \subseteq B$, if $\forall x \in A\ x \in B$. So, without assuming any non-logical axioms we may form the following classes, where A, B, C are classes and $a, a_1, \ldots, a_n$ are sets.

Definition: 4.1

1. $\{a_1, \ldots, a_n\} = \{x \mid x = a_1 \vee \cdots \vee x = a_n\}$. When $n = 0$ this is the empty class $\emptyset$.
2. $\bigcup A = \{x \mid \exists y \in A\ x \in y\}$.
3. $A \cup B = \{x \mid x \in A \vee x \in B\}$.
4. $a^+ = a \cup \{a\}$.
5. $\mathcal{P}(A) = \{x \mid x \subseteq A\}$.
6. $V = \{x \mid x = x\}$.

The Union Axiom asserts that the class $\bigcup A$ is a set for each set A. So, using the Pairing axiom we get that the class $A \cup B$ is a set whenever A, B are sets and hence that $\{a_1, \ldots, a_n\}$ is a set whenever $a_1, \ldots, a_n$ are sets for $n > 0$.

If A is a class and $\theta(x, y)$ is a formula in the language of set theory, then we may form a *family of classes* $(B_a)_{a \in A}$ over A, where for each $a \in A$

$$B_a = \{y \mid \theta(a, y)\}.$$

If $(B_a)_{a \in A}$ is a family of classes then we may form the classes

$$\begin{aligned} \bigcup_{a \in A} B_a &= \{y \mid \exists a \in A\ y \in B_a\}, \\ \bigcap_{a \in A} B_a &= \{y \mid \forall a \in A\ y \in B_a\}. \end{aligned}$$

4.2 Class Relations and Functions

If R is a class of ordered pairs then we use aRb for $\langle a, b\rangle \in R$. If A, B are classes and $R \subseteq A \times B$ such that

$$\forall x \in A\, \exists y \in B\ xRy$$

then we will write

$$R : A \succ\!\!- B$$

and if also

$$\forall y \in B \exists x \in A\ xRy$$

then we write

$$R : A \succ\!\!-\!\!\prec B.$$

If

$$\forall x \in A \exists! y \in B\ xRy$$

then we use the standard notation

$$R : A \to B,$$

and for each $a \in A$ we write $R(a)$ for the unique $b \in B$ such that aRb. If $R : A \to B$ we will say that R is a *class function* or *map*.

dom(R) and **ran**(R) are the classes $\{x \mid \exists y\ xRy\}$ and $\{y \mid \exists x\ xRy\}$, respectively.

Lemma: 4.2 (**ECST**) *If A is a set and $F : A \to B$ then F is a set.*

Proof: Since $\forall x \in A\, \exists! y\, (\langle x, y\rangle \in F)$ it follows from Lemma 3.2 that there is a function f with $\mathbf{dom}(f) = A$ and $\forall x \in A\, (\langle x, f(x)\rangle \in F)$. Hence $F = f$, so F is a set. $\square$

4.3 Some Consequences of Union-Replacement

We now consider a few consequences of Union-Replacement.

Lemma: 4.3 (**ECST**) *Let A be a set and $(B_a)_{a\in A}$ be a family of sets over A. Then, $\bigcup_{a\in A} B_a$ is a set and if A is inhabited, $\bigcap_{a\in A} B_a$ is a set also.*

Proof: $\bigcup_{a\in A} B_a$ is a set by Union-Replacement. Now suppose that A is inhabited. Let $a_0 \in A$. By Lemma 4.2, there is a function f with domain A such that $\forall a \in A\, f(a) = B_a$. Then

$$\bigcap_{a\in A} B_a = \{u \in a_0 \mid \forall x \in A\, u \in f(x)\},$$

so it is a set by Bounded Separation. $\square$

Cartesian Products of Classes

For classes A, B let $A \times B$ be the class given by

$$A \times B = \{z \mid \exists a \in A \exists b \in B\ z = \langle a, b\rangle\}.$$

For r a natural number greater than 0, the r-fold **cartesian product** of a class A, A^r, is defined by $A^1 = A$ and $A^{k+1} = A^k \times A$.

If $F : A \times B \to C$ is a class function we will write $F(a, b)$ rather than $F(\langle a, b\rangle)$ for $\langle a, b\rangle \in A \times B$. Similarly, if $G : A^r \to B$ is a class function defined on the r-fold cartesian product of a class A, we will write $F(a_1, \ldots, a_r)$ for $F(\langle a_1, \ldots, a_r\rangle)$ whenever $\langle a_1, \ldots, a_r\rangle \in A^r$.

Proposition: 4.4 (**ECST**) *If A, B are sets then so is the class $A \times B$.*

Proof: Let A, B be sets. Then, as

$$\{a\} \times B = \{\langle a, b\rangle \mid b \in B\}$$

is a set, by Replacement, so is

$$A \times B = \bigcup_{a\in A} (\{a\} \times B)$$

by Union-Replacement. $\square$

Definition: 4.5 Let I be a class and $(A_i)_{i\in I}$ be a family of classes over I. The **disjoint union** or **sum** of $(A_i)_{i\in I}$ is the class

$$\sum_{i\in I} A_i \quad = \quad \{\langle i, a\rangle \mid a \in A_i \ \wedge \ i \in I\}.$$

Note that the cartesian product $A \times B$ is a special case of disjoint union as $A \times B = \sum_{i\in A} B_i$, where $B_i = B$ for all $i \in A$.

Proposition: 4.6 (**ECST**) *If I is a set and $(A_i)_{i\in I}$ be a family of sets over I, then $\sum_{i\in I} A_i$ is a set.*

Proof: We know that $\{i\} \times A_i$ is a set for every $i \in I$. As

$$\sum_{i\in I} A_i = \bigcup_{i\in I} \{i\} \times A_i$$

it follows by Union-Replacement that $\sum_{i\in I} A_i$ is a set. $\square$

Quotients

Let A be a class and R be a subclass of $A\times$A. R is said to be an **equivalence relation on** A if the following hold for all $a, b, c \in A$:

1. aRa (R is **reflexive**),
2. if aRb then bRa (R is **symmetric**),
3. if aRb and bRc then aRc (R is **transitive**).

Then for each $a \in A$ we may form its *equivalence class*

$$[a]_R = \{x \in A \mid xRa\}.$$

Lemma: 4.7 (**ECST**) *If A and R are sets, where $R \subseteq A \times A$, then for each $a \in A$, $[a]_R$ is a set and, moreover, the* **quotient of A with respect to R**,

$$A/R = \{[a]_R \mid a \in A\},$$

is a set.

Proof: This is an immediate consequence of Bounded Separation and Union-Replacement. $\square$

4.4 Russell's paradox

That one had to distinguish between proper classes and sets was an important insight of early set theory. In its "naive" phase, set theory was developed on the basis of Cantor's definition of set:

> *By a set we are to understand any collection into a whole of definite and separate objects of our intuition or our thought.*

This definition of set led to the following principle.

Definition: 4.8 (**General Comprehension Principle**) For each definite property P of sets, there is a set

$$A = \{x \mid P(x)\}.$$

As is well known, this principle was refuted by Russell in 1901.

Lemma: 4.9 Russell's paradox (**ECST**) *The General Comprehension Principle is not valid.*

Proof: By the General Comprehension Principle,

$$R = \{x \mid x \text{ is a set and } x \notin x\}$$

is a set. The assumption $R \in R$ yields $R \notin R$ by the very definition of R, which is a contradiction. As a result, $R \notin R$. However, in view of the definition of R, the latter implies $R \in R$ and thus we have reached a contradiction. Consequently, R is not a set, and thus the General Comprehension Principle does not hold. □

Russell's paradox can also be conceived of as a positive result.

Lemma: 4.10 (**ECST**) *For every set A there is a set A_R such that $A_R \notin A$.*

Proof: Let $A_R = \{x \in A \mid x \notin x\}$. From $A_R \in A_R$ we get the contradiction $A_R \notin A_R$, whence $A_R \notin A_R$. Thus, $A_R \in A$ leads to the contradiction $A_R \in A_R$, and therefore $A_R \notin A$. □

4.5 Subset Collection and Exponentiation

An important construction in mathematics is to form function spaces, that is if A, B are sets one forms the collection of all functions from A to B. There is no problem in talking about function spaces as classes when working in **ECST**. However, in general, if we want to ensure that this class is a set we have to appeal to the Exponentiation Axiom. This axiom will be mathematically important in showing that the class of constructive Cauchy reals constitutes a set. For other notions of reals, as for example the constructive Dedekind reals, the Exponentiation axiom appears to be too weak, while with the aid of Subset Collection they can be shown to form a set.

In this section we study some of the consequences of the Subset Collection scheme as well as equivalent axioms. We also investigate the deductive relationships between the Subset Collection Scheme, Exponentiation Axiom, and Powerset Axiom. The Subset Collection scheme easily qualifies for the most intricate axiom of **CZF**. To explain this axiom in different terms, we introduce the notion of **Fullness**.

Definition: 4.11 For sets A, B let ${}^{A}B$ be the class of all functions with domain A and with range contained in B. Let $\mathbf{mv}({}^{A}B)$ be the class of all sets $R \subseteq A \times B$ satisfying $\forall u \in A\, \exists v \in B\, \langle u, v\rangle \in R$. A set C is said to be **full in** $\mathbf{mv}({}^{A}B)$ if $C \subseteq \mathbf{mv}({}^{A}B)$ and

$$\forall R \in \mathbf{mv}({}^{A}B)\, \exists S \in C\; S \subseteq R.$$

The expression $\mathbf{mv}({}^{A}B)$ should be read as the class of **multi-valued functions** (or **multi functions**) from the set A to the set B.

An additional axiom we consider is:

Fullness: For all sets A, B there exists a set C such that C is full in $\mathbf{mv}({}^{A}B)$.

Theorem: 4.12 (i) (**ECST**) Subset Collection implies Fullness.

(ii) (**ECST** + Strong Collection) Fullness implies Subset Collection.

(iii) (**ECST**) Fullness implies Exponentiation.

Proof: (i): Suppose A, B are sets. Let $\phi(x, y, u)$ be the formula $y \in u \wedge \exists z \in B\, (y = \langle x, z\rangle)$. Using the relevant instance of Subset Collection and noticing that for all $R \in \mathbf{mv}({}^{A}B)$ we have

$$\forall x \in A\, \exists y \in A \times B\; \phi(x, y, R),$$

there exists a set C such that $\forall R\in\mathbf{mv}(^AB)\,\exists S\in C\, S\subseteq R$.

For (ii), let A, B be sets. Pick a set C which is full in $\mathbf{mv}(^AB)$. Assume $\forall x\in A\exists y\in B\phi(x,y,u)$. Define $\psi(x,w,u) := \exists y\in B\,[w=\langle x,y\rangle\wedge\phi(x,y,u)]$. Then $\forall x\in A\exists w\psi(x,w,u)$. Thus, by Strong Collection, there exists $v\subseteq A\times B$ such that

$$\forall x\in A\,\exists y\in B\,[\langle x,y\rangle\in v\wedge\phi(x,y,u)]\ \wedge\ \forall x\in A\,\forall y\in B\,[\langle x,y\rangle\in v\ \rightarrow\ \phi(x,y,u)].$$

As C is full, we find $w\in C$ with $w\subseteq v$. Consequently, $\forall x\in A\exists y\in\mathbf{ran}(w)\phi(x,y,u)$ and $\forall y\in\mathbf{ran}(w)\exists x\in A\,\phi(x,y,u)$, where $\mathbf{ran}(w) := \{v\mid\exists z\,\langle z,v\rangle\in w\}$.

Whence $D := \{\mathbf{ran}(w) : w\in C\}$ witnesses the truth of the instance of Subset Collection pertaining to ϕ.

(iii) Let C be full in $\mathbf{mv}(^AB)$. If now $f\in{}^AB$, then $\exists R\in C\,R\subseteq f$. But then $R=f$. Therefore $^AB\ =\ \{f\in C:\ f \text{ is a function}\}$. □

An important infinitary operation in set theory is the dependent product or function spaces construction.

Definition: 4.13 Let I be a set and $(A_i)_{i\in I}$ be a family of classes over I. The **dependent product** of $(A_i)_{i\in I}$ is the class

$$\prod_{i\in I}A_i\ \ =\ \ \{f\mid f:I\to\bigcup_{i\in I}A_i\ \wedge\ (\forall i\in I)f(i)\in A_i\}.$$

Proposition: 4.14 (**ECST** + Exponentiation) *If I is a set and $(A_i)_{i\in I}$ is a family of sets over I, then $\prod_{i\in I}A_i$ is a set.*

Proof: $\bigcup_{i\in I}A_i$ is a set by Lemma 4.3, and hence, by Exponentiation, $\{f\mid f:I\to\bigcup_{i\in I}A_i\}$ is a set. Thus, Bounded Separation ensures that $\prod_{i\in I}A_i$ is a set. □

Corollary: 4.15 (**ECST**) *Strong Collection plus Powerset implies Subset Collection.*

Proof: Arguing in **ECST**, one easily shows that Powerset implies Fullness. Thus the assertion follows from Theorem 4.11 (ii). □

As the next result will show, Fullness does not entail that, for sets A and B, $\mathbf{mv}(^AB)$ is always a set.

Proposition: 4.16 *(i)* (**ECST**) $\forall A \forall B\, (\mathbf{mv}(^A B)$ is a set$)\ \leftrightarrow$ Powerset.

(ii) **CZF** *does not prove* $\forall A \forall B\, (\mathbf{mv}(^A B)$ is set$)$.

Proof: (i): We argue in **ECST**. It is obvious that Powerset implies that $\mathbf{mv}(^A B)$ is a set for all sets A, B. Henceforth assume the latter. Let C be an arbitrary set and $D = \mathbf{mv}(^C\{0,1\})$. By our assumption D is a set. To every subset X of C we assign the set $X^* := \{\langle u, 0\rangle |\ u \in X\} \cup \{\langle z, 1\rangle |\ z \in C\}$. As a result, $X^* \in D$. For every $S \in D$ let $pr(S)$ be the set $\{u \in C|\ \langle u, 0\rangle \in S\}$. We then have $X = pr(X^*)$ for every $X \subseteq C$, and thus

$$\mathcal{P}(C) \quad = \quad \{pr(S)|\ S \in D\}.$$

Since $\{pr(S)|\ S \in D\}$ is a set by Replacement, $\mathcal{P}(S)$ is a set as well.

(ii): As will be explained in the final chapter, the strength of **CZF** + Powerset exceeds that of second order arithmetic whereas **CZF** has only the strength of a small fragment of second order arithmetic. $\square$

Remark: 4.17 On page 623 of[75], a different rendering of Fullness is introduced:

$$\text{Fullness}^{TvD} \qquad \forall A \forall B \exists C\, \forall r \in \mathbf{mv}(^A B)\ \mathbf{ran}(r) \in C.$$

Proposition 8.9, page 623 of [75] claims that Subset Collection implies Fullness^{tvd} on the basis of **CZF**. That this is not correct can be seen as follows. Let A, B be arbitrary sets. For $R \in \mathbf{mv}(^A B)$ let R^d be the set $\{\langle u, \langle u, v\rangle\rangle |\ \langle u, v\rangle \in R\}$. Then $R^d \in \mathbf{mv}(^A(A \times B))$ and $\mathbf{ran}(R^d) = R$. By Fullness^{TvD} there exists a set C such that $\mathbf{ran}(S) \in C$ for all $S \in \mathbf{mv}(^A(A \times B))$. Consequently $\mathbf{mv}(^A B) \subseteq C$ and thus $\mathbf{mv}(^A B)$ is a set by Δ_0 Separation. The latter collides with Proposition 4.16 (ii).

4.6 Binary Refinement

This is a possible subsection 4.6 on Binary Refinement, which will be used in showing that the Dedekind reals form a set.

We formulate a weak consequence of the Fullness axiom that will play a role in showing that the class of Dedekind reals form a set.

Definition: 4.18 *For each set A, a set $D \subseteq Pow(A)$ is a* binary refinement set for A *if, whenever sets X_0, X_1 are sets such that $X_0 \cup X_1 = A$ then there are sets Y_0, Y_1 such that $Y_0 \subseteq X_0$, $Y_1 \subseteq X_1$ and $Y_0 \cup Y_1 = A$.*

Exercise: 4.19 *Show that a set D of subsets of a set A is a binary refinement set for A iff, for each set $X \subseteq A$, if Y is a set such that $X \cup Y = A$ then there is a set $X' \in D$ such that $X' \subseteq X$ and $X' \cup Y = A$.*

Binary Refinement Axiom (BRA) *Every set has a binary refinement set.*

Theorem: 4.20 (ECST) *Fullnes implies* **BRA**.

Proof: Let C be a set that is full in $\mathbf{mv}({}^A2)$ and let

$$D = \{\{x \in A \mid (x, i) \in R\} \mid R \in C, i \in 2\}.$$

Given sets X_0, X_1 such that $X_0 \cup X_1 = A$ let

$$R = \{(x, i) \in A \times 2 \mid x \in X_i\}.$$

Then $R \in \mathbf{mv}({}^A2)$ so that there is $S \in C$ such that $S \subseteq R$. If $Y_i = \{x \in A \mid (x, i) \in S\}$ for $i = 0, 1$ then $Y_0, Y_1 \in D$, $Y_0 \subseteq X_0, Y \subseteq X_1$ and $Y_0 \cup Y_1 = A$, as required. $\square$

Exercise: 4.21 *Show that if A has a binary refinement set and $A \sim A'$ then A' has a binary refinement set.*

Proposition: 4.22

1. *If A has a binary refinement set then the class $Dec(A)$ of decidable subsets of A is a set and hence so is ${}^A2 \sim Dec(A)$.*

2. *If A, B are sets such that $A \times B$ has a binary refinement set and B is discrete then the class ${}^AB$ is a set.*

3. *If $\mathbb{N}$ has a binary refinement set then ${}^{\mathbb{N}}\mathbb{N}$ is a set.*

The following result will be useful in showing that the Dedekind reals form a set, assuming only that $\mathbb{N}$ has a binary refinement set.

Proposition: 4.23 *Let $f : A \to B$, where A, B are sets, and let P be the class of sets $X \subseteq B$ such that there is a set $Y \subseteq A$ such that*

1. *$X \subseteq f(A - Y)$,*

2. *$A \subseteq f^{-1}X \cup Y$.*

If A has a binary refinement set then P is a set.

Proof: Let D be a binary refinement set for A. We will show that P is a subclass of the set $D^f = \{fU \mid U \in D\}$ and then conclude that P is a set.

Let $X \subseteq B, Y \subseteq A$ such that 1,2 hold. By 2, there are sets $U, V \in D$ such that $U \subseteq f^{-1}X$, $V \subseteq Y$ and $U \cup V = A$. Observe that $fU \subseteq f(f^{-1}X) \subseteq X$ and, by 1, $X \subseteq f(A - Y) \subseteq fU$. So $X = fU \in D^f$. Also observe that $X \subseteq f(A - Y) \subseteq f(A - V)$ and $A \subseteq U \cup V \subseteq f^{-1}X \cup V$. It follows that $X \in P$ iff $X \in D^f$ such that there is a set $V \in D$ such that $X \subseteq f(A - V)$ and $A \subseteq f^{-1}X \cup V$. So, by Restricted Separation, P is a set. $\square$

5 On Bounded Separation

The Δ_0 Separation Scheme has infinitely many instances and is the only axiom scheme of **CZF** that makes reference to the syntactic form of formulas. We show that in a weak subtheory, $\mathbf{ECST}_0$, each instance is a consequence of the Binary Intersection Axiom which just expresses that the intersection class $a \cap b = \{x \mid x \in a \ \wedge \ x \in b\}$ of two sets a, b is a set. Of course this axiom is itself an instance of the scheme.

Definition: 5.1 The theory $\mathbf{ECST}_0$ consists of the Extensionality, Pairing and Union Axioms, the Replacement axiom Scheme and the Emptyset Axiom: $\exists a \forall x \in a \bot$ which asserts that the empty class $\emptyset = \{x \mid \bot\}$ is a set.

For the remainder of this subsection we mostly argue in $\mathbf{ECST}_0$.

5.1 Truth Values

Definition: 5.2 (The class Ω of Truth values.) Let $0 = \emptyset$, $1 = \{0\}$ and $\Omega = \mathbf{Pow}(1) = \{x : \ x \subseteq 1\}$. We think of the elements of Ω as truth values, with 0 representing falsity and 1 representing truth. In constructive mathematics we cannot assert that those are the only truth values. Moreover in constructive set theory we cannot even assert that the class of truth values forms a set.

For each class $A \subseteq \Omega$ let

- $\bigvee A = \{x \mid x \in 1 \ \wedge \ \exists y \in A \ x \in y\} = \bigcup A$,
- $\bigwedge A = \{x \mid x \in 1 \ \wedge \ \forall y \in A \ x \in y\}$.

For each set $a \in Pow(\Omega)$ the class $\bigvee a$ is a set in Ω by the Union axiom and assuming Δ_0 Separation, we would get that $\bigwedge a$ is a set in Ω.

If θ is a formula and $c \in \Omega$ such that $[\theta \ \leftrightarrow \ 0 \in c]$ then, by Extensionality, c is unique and we call c the *truth value* of θ. For any formula θ we use $!\theta$ to abbreviate

$$\exists c \in \Omega \ [\theta \ \leftrightarrow \ 0 \in c]$$

Proposition: 5.3 ($\mathbf{ECST}_0$) *Let θ be a formula in which z does not occur free. Then, for each set a,*

$$!\theta \quad \textit{iff} \quad \{z \in \{a\} \mid \theta\} \textit{ is a set.}$$

Proof: Note that we do have this equivalence when $a = 0$. So it suffices to show that A is a set iff B is a set where $A = \{z \in \{0\} \mid \theta\}$ and $B = \{z \in \{a\} \mid \theta\}$. Let $F = \{(0, a)\}$. Then $F : \{0\} \to \{a\}$ and $B = \{F(x) \mid x \in A\}$. So, by Replacement, if A is a set then so is B. For the converse just use the inverse function $F^{-1} : \{a\} \to \{0\}$. □

Proposition: 5.4 (ECST$_0$) *Let $\phi(x)$ be a formula. For each set a, if $\forall x \in a\ !\phi(x)$ then*

1. *$!\ \exists x \in a\ \phi(x)$,*
2. *$\{x \in a \mid \phi(x)\}$ is a set.*

Proof:

1. By the assumption, using Union-Replacement we get that

$$b = \{c \in \Omega \mid\ \exists x \in a\ [\phi(x)\ \leftrightarrow\ 0 \in c]\}$$

   is a set. This is in $Pow(\Omega)$ so that $\bigvee b \in \Omega$ and

$$\exists x \in a\ \phi(x)\ \leftrightarrow\ 0 \in \bigvee b.$$

2. By the assumption and Proposition 5.3 , for each $x \in a$ the class

$$b_x = \{y \in \{x\} \mid \phi(x)\}$$

   is a set. Hence, by Union-Replacement, $\{x \in a \mid \phi(x)\} = \bigcup_{x \in a} b_x$ is a set.

□

5.2 The Infimum Axiom

We let *Infimum* be the assertion that for every set $a \subseteq \Omega$, the class $\bigwedge a$ is a set.

Proposition: 5.5 (ECST$_0$ + *Infimum*)

1. *If $\forall x \in a\ !\phi(x)$ then $!\ \exists x \in a\ \phi(x)$, and $!\ \forall x \in a\ \phi(x)$.*
2. *If $!\phi_1$ and $!\phi_2$ then $!(\phi_1 \vee \phi_2)$, $!(\phi_1 \wedge \phi_2)$ and $!(\phi_1 \to \phi_2)$.*

3. If $!\phi$ then $!\neg\phi$.

Proof:

1. As in the proof of part 1 of Proposition 5.4, by the assumption we may use Union-Replacement to get that

$$b = \{c \in \Omega \mid \ \exists x \in a\ [\phi(x) \ \leftrightarrow \ 0 \in c]\}$$

is a set. This is in $Pow(\Omega)$ so that $\bigvee b \in \Omega$ and

$$\exists x \in a\ \phi(x) \ \leftrightarrow \ 0 \in \bigvee b.$$

Also, using Infimum, $\bigwedge b \in \Omega$ and

$$\forall x \in a\ \phi(x) \ \leftrightarrow \ 0 \in \bigwedge b.$$

2. Let $c_1, c_2 \in \Omega$ such that

$$\phi_i \ \leftrightarrow \ 0 \in c_i$$

for $i = 1, 2$. Then $c_\wedge = \bigwedge\{c_1, c_2\} \in \Omega$ and

$$[\phi_1 \wedge \phi_2] \ \leftrightarrow \ 0 \in c_\wedge.$$

Similarily $c_\vee = \bigvee\{c_1, c_2\} \in \Omega$ and

$$[\phi_1 \vee \phi_2] \ \leftrightarrow \ 0 \in c_\vee.$$

Finally if $c_\rightarrow = \bigwedge\{c_2 \mid 0 \in c_1\} \in \Omega$ then

$$[\phi_1 \rightarrow \phi_2] \ \leftrightarrow \ 0 \in c_\rightarrow.$$

3. As $0 \in \Omega$ and $0 = 1 \ \leftrightarrow \ 0 \in 0$ and $\neg\phi \ \leftrightarrow \ [\phi \rightarrow 0 = 1]$.

□

5.3 The Binary Intersection Axiom

The Binary Intersection Axiom states that the class $a \cap b$ is a set for all sets a, b. In $\mathbf{ECST}_0$, the axiom has several equivalents.

Theorem: 5.6 ($\mathbf{ECST}_0$) *The following are equivalent.*

1. *$\cap a$ is a set for every inhabited set a.*
2. *$a \cap b$ is a set for all sets a, b.*
3. *$\{a\} \cap \{b\}$ is a set for all sets a, b.*
4. *$!(a = b)$ for all sets a, b.*
5. *$!(a \subseteq b)$ for all sets a, b.*
6. *Infimum and $!(a \in b)$ for all sets a, b.*

Proof: The implications $1 \Rightarrow 2$ and $2 \Rightarrow 3$ are trivial. For $3 \Leftrightarrow 4$ it is enough to observe that, by Proposition 5.3,

$$\{a\} \cap \{b\} \text{ is a set } \iff !(a = b).$$

For $4 \Rightarrow 5$ observe that $a \subseteq b$ iff $a \cup b = b$.

To prove $5 \Rightarrow 6$ assume 5. As $a \in b$ iff $\{a\} \subseteq b$ we immediately get that $!(a \in b)$. To prove Infimum let $a \subseteq \Omega$. Then, as $(\forall y \in a)!(0 \in y)$, by Proposition 5.4,

$$b = \{y \in a \mid 0 \in y\}$$

is a set. Now $\bigwedge a = \{x \in \{0\} \mid a \subseteq b\}$ is a set using 5 again.

It only remains to show that $6 \Rightarrow 1$. So let a be an inhabited set. Let $b \in a$. Then, assuming $\forall x \forall y \, !(\in y)$,

$$\forall x \in b \forall y \in a \, !(x \in y)$$

so that, using part 1 of Proposition 5.4 and assuming Infimum,

$$\forall x \in b \, ! \, \forall y \in a \, (x \in y)$$

so that, by part 2 of proposition 5.4,

$$\cap a = \{x \in b \mid \forall y \in a \, (x \in y)\}$$

is a set. □

Corollary: 5.7 ($\mathbf{ECST_0}$) *The Δ_0 Separation Scheme is equivalent to its single instance, the Binary Intersection Axiom.*

Proof: If a, b are sets then, as $a \cap b = \{x \in a \mid x \in b\}$ the assertion that $a \cap b$ is a set is an instance of Δ_0 Separation.

Conversely, let us assume the Binary Intersection Axiom. Then, by the Theorem, $!\theta$ for every atomic formula θ. Also Infimum holds so that, by repeated application of Proposition 5.5 we get that $!\phi$ for every bounded formula ϕ. We can now apply part 2 of Proposition 5.4 to get that $\{x \in a \mid \phi(x)\}$ is a set for every set a and every bounded formula ϕ; i.e. we have proved each instance of the bounded separation scheme. $\square$

6 The Natural Numbers

6.1 The smallest inductive set

The set of natural numbers will be obtained from the Strong Infinity axiom. The role of the number zero is played by the empty set which is obtained as follows. By Restricted Separation there is a set $\emptyset = \{u \in b : u \neq u\}$, where b is an arbitrary set. Since $\forall u\,(u = u)$, one has $\forall u \in \emptyset, (u \notin \emptyset)$. If z is another set such that $\forall u \in z\,(u \notin z)$ then $\forall u\,(u \in \emptyset \leftrightarrow u \in z)$, and hence $\emptyset = z$ by Extensionality. Thus there is exactly one set z such that $\forall u \in z\,(u \notin z)$. This set will be denoted by $\emptyset$ or 0.

Next we show that the infinite set of the Strong Infinity axiom is uniquely determined by its properties. Most of the results of this subsection can be proved in **ECST**.

Lemma: 6.1 (**ECST**) *Let $\theta(a)$ be the formula*

$$Ind(a) \wedge \forall y[Ind(y) \to a \subseteq y].$$

If $\theta(a)$ and $\theta(b)$ then $a = b$.

Proof: $Ind(a)$ and $Ind(b)$ yield $a \subseteq b$ and $b \subseteq a$, hence $a = b$ by Extensionality. $\square$

Definition: 6.2 The unique set a such that $Ind(a) \wedge \forall y[Ind(y) \to a \subseteq y]$ will be denoted by ω. We use a^+ to mean $a \cup \{a\}$.

Theorem: 6.3 (**ECST**)

1. $\forall n \in \omega\,[n = 0 \ \vee\ (\exists m \in \omega)\, n = m^+]$.
2. $\forall n \in \omega\,(0 \neq n^+)$.
3. $\phi(0) \ \wedge\ \forall n \in \omega[\phi(n) \to \phi(n^+)] \ \to\ (\forall n \in \omega)\, \phi(n)$ *for every bounded formula $\phi(n)$.*
4. $\forall n \in \omega\,(n$ *is transitive*$)$.
5. $\forall n \in \omega\,(n \notin n)$.
6. $\forall n, m \in \omega\,[n \in m \to n^+ \in m \ \vee\ n^+ = m]$.
7. $\forall n, m \in \omega\,[n^+ = m^+ \to n = m]$.

8. $\forall n \in \omega\, (0 \in n^+)$

9. $\forall n, m \in \omega\, [n \in m \ \vee\ n = m \ \vee\ m \in n]$.

10. *$m \in n \ \vee\ m \notin n$ and $m = n \ \vee\ m \neq n$ for all $n, m \in \omega$.*

11. *If $\phi(x_1, \ldots, x_r)$ is a bounded formula with all free variables among those shown, then*

$$\forall n_1, \ldots, n_r \in \omega\, [\phi(n_1, \ldots, n_r) \ \vee\ \neg\phi(n_1, \ldots, n_r)].$$

Proof: For (1), let $a = \{n \in \omega : n = 0 \vee (\exists m \in \omega) n = m^+\}$. Then $0 \in a$ and $(\forall x \in a)(x + 1 \in a)$, thus $Ind(a)$. So $\omega \subseteq a$ which implies (1).

(2): Since $n \in n^+$ and $n \notin 0$ it follows $0 \neq n^+$.

(3): Assume $\phi(0) \ \wedge\ (\forall n \in \omega)[\phi(n) \to \phi(n^+)]$ By Restricted Separation $b = \{n \in \omega : \phi(n)\}$ is a set. Since $0 \in b$ and $(\forall n \in b) n^+ \in b$, we get $Ind(b)$, so $\omega \subset b$, and hence $(\forall n \in \omega)\phi(n)$.

(4): Here we use the induction principle (3). Obviously 0 is transitive. Suppose n is transitive. If $k \in m \in n^+$ then $m = n$ or $m \in n$, thus $k \in n$ or $k \in n \in m$, so $k \in n$ as n is transitive, and hence $k \in n^+$. So n^+ is transitive, too. By (3) we get that all $n \in \omega$ are transitive.

(5): $0 \notin 0$ is obvious. $n^+ \in n^+$ implies $n^+ \in n \ \vee\ n^+ = n$, and thus $n \in n$. Hence $n \notin n$ implies $n^+ \notin n^+$. So (5) follows by the induction principle (3).

(6): Let $\phi(n)$ be the bounded formula $(\forall m \in \omega)[m \in n \to m^+ \in n \vee m^+ = n]$. Obviously $\phi(0)$. Suppose $\phi(n)$. If $k \in n^+$, then $k = n$ or $k \in n$, so $k^+ = n^+$ or $k^+ \in n$ or $k^+ = n$ using $\phi(n)$. Whence $k^+ = n^+$ or $k^+ \in n^+$, confirming $\phi(n^+)$. Using (2), it follows $(\forall n \in \omega)\phi(n)$.

(7): $n^+ = m^+$ yields $n = m \ \vee\ n \in m$, thus $n = m \ \vee\ n^+ \in m \ \vee\ n^+ = m$ by (6). So $n^+ = m^+ \to n = m \ \vee m \in m$ by transitivity of m. Using (5) this yields $n^+ = m^+ \to n = m$.

(8): We have $0 \in 0 + 1$ and if $0 \in n$, so is $0 \in n^+$. Thus $(\forall n \in \omega) 0 \in n^+$ by (3).

(9): Let $\psi(n)$ be the formula $\forall m \in \omega[n \in m \ \vee\ n = m \ \vee\ m \in n]$. Then $\psi(0)$ by (8) and (1). Suppose $\psi(n)$ and $m \in \omega$. Then $m \in n \vee n = m \vee n \in m$, so $m \in n^+ \ \vee\ n^+ \in m \ \vee\ n = m$ by (6), whence $\psi(n^+)$ as m was arbitrary. By (3), (9) follows.

(10): $m = n \ \vee\ n \in m$ implies $m \notin n$ by (4) and (5). Thus, by (9), $m \in n \vee, m \notin n$. Likewise, by (5), $m \in n \ \vee\ n \in m$ implies $n \neq m$. Thus (9) yields $m = n \ \vee\ m \neq n$.

(11): We use meta-induction on the build up of $\phi(\vec{n})$ If $\phi(\vec{n})$ is atomic then the assertion follows from (10). If $\phi(\vec{n})$ is of either form $\neg\phi_0$, $\phi_0 \wedge \phi_1$, $\phi_0 \vee \phi_1$, or $\phi_0 \to \phi_1$, then the assertion is an immediate consequence of the inductive hypotheses. Suppose $\phi(\vec{n})$ is of the form $(\forall k \in n_j)\theta(\vec{n}, k)$, where $1 \leq j \leq r$. Let $\psi(m)$ be the formula $(\forall k \in m)\theta(\vec{n}, k)$. We will use (3) to show $(\forall m \in \omega)[\psi(m) \vee \neg\psi(m)]$. Obviously, $\psi(0)$, so $\psi(0) \vee \neg\psi(0)$. Suppose $\psi(m) \vee \neg\psi(m)$. By induction hypothesis we have $\theta(\vec{n}, m) \vee \neg\theta(\vec{n}, m)$. Moreover, $k \in m^+ \rightarrow k \in m \vee k = m$. Thus from $\psi(m) \wedge \theta(\vec{n}, m)$ it follows $\psi(m^+)$ whereas $\psi(m) \wedge \neg\theta(\vec{n}, m)$ as well as $\neg\psi(m)$ imply $\neg\psi(m^+)$. Hence $\psi(m^+) \vee \neg\psi(m^+)$. So, by (3), $(\forall m \in \omega)[\psi(m) \vee \neg\psi(m)]$. The latter yields $\phi(\vec{n}) \vee \neg\phi(\vec{n})$.

Finally, when $\phi(\vec{n})$ is of the form $(\exists k \in n_j)\theta(\vec{n}, k)$ let $\chi(m)$ be the formula $(\exists k \in m)\theta(\vec{n}, k)$ and use (3) to show $(\forall m \in \omega)[\chi(m) \vee \neg\chi(m)]$. Since $\neg\chi(0)$, $\chi(0) \vee \neg\chi(0)$ follows. Suppose $\chi(m) \vee \neg\chi(m)$. $\chi(m)$ implies $\chi(m^+)$. $\theta(\vec{n}, m) \vee \neg\theta(\vec{n}, m)$ holds by induction hypothesis. $\theta(\vec{n}, m)$ implies $\chi(m^+)$, whereas $\neg\chi(m) \wedge \neg\theta(\vec{n}, m)$ implies $\neg\chi(m^+)$. Therefore, $\chi(m^+) \vee \neg\chi(m^+)$. $\square$

6.2 The Dedekind-Peano axioms

In classical set theory all one needs to know about the set $\mathbb{N}$ of natural numbers can be derived from the Dedekind-Peano axioms for the structure $(\mathbb{N}, 0, S)$. These axioms can be given as follows.

1. $0 \in \mathbb{N}$.
2. $S : \mathbb{N} \rightarrow \mathbb{N}$.
3. $0 \neq S(n)$ for all $n \in \mathbb{N}$.
4. $S(n) = S(m)$ implies $n = m$ for all $n, m \in \mathbb{N}$.
5. For each subset X of $\mathbb{N}$, if $0 \in X$ and $S(n) \in X$ for all $n \in X$ then $n \in X$ for all $n \in \mathbb{N}$.

Let us call any structure $(\mathbb{N}, 0, S)$ satisfying the Dedekind-Peano axioms a Dedekind-Peano structure.

Proposition: 6.4 (ECST) $(\omega, 0, S)$ *satisfies the Dedekind-Peano axioms, where* ω *is the smallest inductive set given by the Strong Infinity axiom,* 0 *is the empty set and* $S(n) = n^+ = n \cup \{n\}$ *for* $n \in \omega$.

Proof: As ω is the smallest inductive set we get the first two axioms and the last axiom, which just states that ω is included in every inductive subset of ω. The remaining two axioms are parts 2 and 7 of Theorem 6.3. $\square$

Dedekind showed that from his axioms one could derive the following method for defining functions on $\mathbb{N}$ by iteration.

Definition: 6.5 (Small Iteration) *For each set A, each $F : A \to A$ and each $a_0 \in A$ there is a unique function $H : \mathbb{N} \to A$ such that*

$$\begin{array}{ll} H(0) & = a_0, \\ H(S(n)) & = F(H(n)). \end{array}$$

We call this Small Iteration because we require A to be a set. We get full Iteration by allowing A and F to be classes. An easy application of Small Iteration is the following result.

Theorem: 6.6 (ECST) *Assuming Small Iteration, any structure (A, a_0, F) satisfying the Dedekind-Peano axioms is isomorphic to $(\omega, 0, S)$.*

Proof: By Small Iteration there is a unique structure preserving map $\omega \to A$. That the map is injective can be proved using the fifth axiom for ω. That it is surjective uses the fifth axiom for A. $\square$

Thus, assuming Small Iteration, the Dedekind-Peano axioms give a categorical axiomatisation of the natural numbers.

Exercise: 6.7 *Show that the last three Dedekind-Peano axioms can be derived from the first two using Small Iteration. [Hint: To prove the third and fourth axioms choose $* \notin \mathbb{N}$ and let $\mathbb{N}_* = \mathbb{N} \cup \{*\}$. Define $\alpha : \mathbb{N}_* \to \mathbb{N}$ by*

$$\begin{array}{ll} \alpha(*) & = 0, \\ \alpha(n) & = S(n)) \textit{ for all } n \in \mathbb{N}. \end{array}$$

As $\alpha : \mathbb{N}_* \to \mathbb{N}_*$ we can use Small Iteration to define $\beta : \mathbb{N} \to \mathbb{N}_*$ such that

$$\begin{array}{ll} \beta(0) & = *, \\ \beta(S(n)) & = \alpha(\beta(n)) \textit{ for all } n \in \mathbb{N}. \end{array}$$

Now show that β is the inverse of α. The third and fourth axioms follow from the injectivity of α.]

6.3 The Iteration Lemma

Small Iteration can **not** be proved in **ECST** (see ?). But we can extract the following fundamental construction from the classical proof.

Let A, F be classes with $F : A \to A$ and let $a_0 \in A$. We will call a function $X : m^+ \to A$ *good* if $m \in \omega$, $X(0) = a_0$ and $X(n^+) = F(X(n))$ for all $n \in m$. Let G be the class of all good functions, let $H = \cup G$ and let

$$Q = \{n \in \omega \mid (\exists a \in A)\ (n, a) \in H\}.$$

Lemma: 6.8 (ECST) *Q is an inductive subclass of ω and $H : Q \to A$ such that*

$$\begin{array}{ll} H(0) & = a_0 \\ H(n^+) & = F(H(n)) \end{array}$$

for all $n \in Q$.

Proof: We first show that Q is inductive. Clearly $(0, a_0) \in \{(0, a_0)\} \in G$ so that $(0, a_0) \in H$ and hence $0 \in Q$. If $n \in Q$ then $(n, a) \in X \in G$ for some X and some a. Then $X : m^+ \to A$ for some $m \in \omega$. so $n \in m^+$ and hence $n \in m$ or $n = m$. If $n \in m$ then $(n^+, F(a)) \in X$. If $n = m$ then $X' = X \cup \{(n^+, F(a)\} \in G$ so that $(n^+, F(a)) \in X' \in G$. In either case $n^+ \in Q$.

To show that $H : Q \to A$ it suffices to show that, for good X_1, X_2, the set Q' is an inductive Δ_0 class, where Q' is the set of $n \in \omega$ such that for all $a_1, a_2 \in \mathbf{ran}(X_1) \cup \mathbf{ran}(X_2)$,

$$(n, a_1) \in X_1 \ \&\ (n, a_2) \in X_2 \Rightarrow a_1 = a_2.$$

For then $Q' = \omega$ so that for all $a_1, a_2 \in A$

$$(n, a_1), (n, a_2) \in H \Rightarrow a_1 = a_2.$$

To see that Q' is inductive note that $(0, a) \in X_i$ implies $a = a_0$ for $i = 1, 2$. So

$$(0, a_1) \in X_1 \ \&\ (0, a_2) \in X_2 \Rightarrow a_1 = a_0 = a_2$$

and so $0 \in Q'$. To show that if $n \in Q'$ then $n^+ \in Q'$ let $n \in Q'$ and let $(n^+, a_1) \in X_1, (n^+, a_2) \in X_2$ to show that $a_1 = a_2$. There must be b_1, b_2 such that $a_1 = F(b_1)$, $a_2 = F(b_2)$, $(n, b_1) \in X_1$ and $(n, b_2) \in X_2$. As $n \in Q'$, $b_1 = b_2$ so that

$$a_1 = F(b_1) = F(b_2) = a_2.$$

$\square$

6.4 The Finite Powers Axiom

To prove small iteration using the above construction we make use of the following axiom.

Definition: 6.9 (Finite Powers Axiom, FPA) *For each set A the class ${}^nA$ of functions from n to A is a set for all $n \in \omega$.*

Note that this axiom is an immediate consequence of the Exponentiation Axiom and so is a theorem of **CZF**.

From now on we assume that $\mathbb{N} = \omega$ and we write s-$\mathbf{ITER}_\omega$ for the Small Iteration axiom.

Lemma: 6.10 (ECST+FPA) *For each set A, the class $\bigcup_{m\in\omega}\ {}^{m^+}\!A$ is a set.*

Proof: Obvious. $\square$

Theorem: 6.11 (ECST) *The Finite Powers Axiom implies s-$\mathbf{ITER}_\omega$.*

Proof: Let A be a set, $F : A \to A$ and $a_0 \in A$. By Lemma 6.8 we have $H : Q \to A$ satisfying the desired equations where Q is an inductive class. As the Finite Powers Axiom entails that $\bigcup_{m\in\omega}\ {}^{m^+}\!A$ is a set it follows that the class G of all good functions is a set so that $H = \cup G$ is a set and finally Q is an inductive subset of ω and hence must be equal to ω.

It only remains to observe, using Δ_0-$\mathbf{IND}_\omega$, that if $H' : \omega \to A$ such that $H'(0) = a_0$ and $H'(n^+) = F(H'(n))$ for all $n \in \omega$ then $H'(n) = H(n)$ for all $n \in \omega$ $\square$

6.5 Induction and Iteration Schemes

In the following we will always assume that Γ is a standard definability notion such as Δ_0, Σ_1 or Σ_ω, and also that Γ comprises the Δ_0-formulas. For example a Σ_1 formula is a formula of the form $\exists y\, \phi(y, \vec{x})$ with ϕ bounded. A Γ-class is a class defined by a Γ-formula.

It is sometimes convenient to allow for an induction principle on ω stronger than Theorem 6.3 (3).

Definition: 6.12 In future, the induction principle of Theorem 6.3 (3) will be referred to as Δ_0 Induction on ω, abbreviated Δ_0-$\mathbf{IND}_\omega$.

$$\Gamma\text{-}\mathbf{IND}_\omega \quad \phi(0) \wedge (\forall n{\in}\omega)(\phi(n) \to \phi(n^+)) \ \to\ (\forall n{\in}\omega)\phi(n)$$

for all Γ formulae ϕ.

We shall consider the full scheme of induction on ω, too.

$$\mathbf{IND}_\omega \quad \psi(0) \wedge (\forall n{\in}\omega)(\psi(n) \to \psi(n^+)) \ \to\ (\forall n{\in}\omega)\psi(n)$$

for all formulae ψ.

The Iteration axiom s-$\mathbf{ITER}_\omega$ concerns the iteration of a function F on a set A. If we allow A, F to be classes then we get the axiom scheme of full Iteration, which we will refer to as $\mathbf{ITER}_\omega$. If we restrict the classes A and F to be Γ classes then we get the Γ-$\mathbf{ITER}_\omega$ scheme.

Theorem: 6.13 (ECST) *If Γ is closed under $\exists$ and bounded universal quantification $\forall x \in n$ for $n \in \mathbb{N}$ then Γ Induction, Γ-$\mathbf{IND}_\omega$, implies Γ Iteration, Γ-$\mathbf{ITER}_\omega$.*

Proof: It is only necessary to check that given Γ classes A, F with $F : A \to A$ and $a_0 \in A$ the inductive class Q constructed before Lemma 6.8 are both Γ classes. Observe that the notion of a good function involves quantifications of the form $\forall x \in n$. So, by Γ Induction, $Q = \omega$ and the proof of the uniqueness of H is the easy Δ_0-$\mathbf{IND}_\omega$ that we have already used. $\square$

6.6 The Function Reflection Scheme

The following Γ-scheme will be useful.

Definition: 6.14 (Γ Function Reflection, Γ-FRS) *If $F : A \to A$, with A, F Γ classes and $a_0 \in A$ then there is a set $A_0 \subseteq A$ with $a_0 \in A_0$ such that $F(a) \in A_0$ for all $a \in A_0$.*

Proposition: 6.15 (ECST)

1. Γ-$\mathbf{ITER}_\omega$ *implies* Γ-**FRS**.

2. Γ-**FRS** *implies* Γ-$\mathbf{IND}_\omega$.

3. Δ_0-**FRS** *implies* **FPA**.

4. Γ-**FRS** *implies* Γ-$\mathbf{ITER}_\omega$.

Proof:

1. Let $F : A \to A$, where A, F are Γ classes and let $a_0 \in A$. Then, assuming Γ-$\mathbf{ITER}_\omega$, there is $h : \omega \to A$ such that $H(0) = a_0$ and $h(S(n)) = F(h(n))$. Then, by Replacement, $A_0 = \{h(n) \mid n \in \omega\}$ is a set which is closed under F and $a_0 \in A_0 \subseteq A$.

2. Let A be an inductive Γ subclass of ω. We must show that $\omega \subseteq A$. As A is inductive $0 \in A$ and A is closed under S. So, by Γ-**FRS**, there is an inductive subset A_0 of A and hence $\omega \subseteq A_0 \subseteq A$.

3. Let A be a set and let $F : \omega \times V \to V$ be the Δ_0 class function defined by
$$F(n, X) \quad = \quad \{f \cup \{\langle n, u\rangle\} \mid f \in X \wedge u \in A\}.$$
For each $(n, X) \in \omega \times V$ let
$$F'(n, X) = (n^+, F(n, X)).$$
As $\omega \times V$ and F' are Δ_0 we may use Δ_0-**FRS** to get a set $B \subseteq \omega \times V$ such that $\{\langle 0, \emptyset\rangle\} \in B$ and for all $(n, X) \in B$, $F'(n, X) \in B$. Then $C = \bigcup\{X \mid (\exists n \in \omega)\ (n, X) \in B\}$ is a set.

Now let $n \in \omega$ and $f \in {}^nA$. Observe that we can show that
$$i \in n^+ \Rightarrow f \cap (i \times V) \in C$$
by Δ_0-$\mathbf{IND}_\omega$ on i. So if $n \in \omega$ then ${}^nA \subseteq C$ so that
$${}^nA = \{f \in C \mid f \in {}^nA\}$$
is a set by Restricted Separation as ${}^nA$ is Δ_0.

4. By Γ-**FRS** we have Δ_0-**FRS** so that by part 3 we have **FPA** and hence, by Theorem 6.11, we have s-$\mathbf{ITER}_\omega$.

Let $F : A \to A$, where A, F are Γ classes and let $a_0 \in A$. Then we may apply the Γ Function Reflection Scheme to get that there is a subset A_0 of the class A that is closed under F and has a_0 as an element. It follows that we may apply s-$\mathbf{ITER}_\omega$ to get a unique $h : \omega \to A_0$ such that $h(0) = a_0$ and $h(S(n)) = F(h(n))$ for all $n \in \omega$. Then $h : \omega \to A$ and an easy induction shows that it is a unique such function satisfying the equations.

□

Corollary: 6.16 (ECST)

1. $\mathbf{IND}_\omega$, **FRS** *and* $\mathbf{ITER}_\omega$ *are equivalent schemes.*

2. Γ-$\mathbf{ITER}_\omega$ *is equivalent to* Γ-**FRS**.

Proof:

1. Use the two previous results, the second result with Γ being Σ_ω, the full definability notion where all formulae are Σ_ω formulae.

2. Use parts 1 and 4 of the previous proposition.

□

6.7 Primitive Recursion

A familar generalisation of Iteration is Primitive Recursion. The set version is the following scheme.

Definition: 6.17 (Small Primitive recursion) *For sets A, B, if $F_0 : B \to A$ and $F : B \times \omega \times A \to A$ then there is a (necessarily unique) $H : B \times \omega \to A$ such that for all $b \in B$*

$$\left\{ \begin{array}{ll} H(b, 0) & = F_0(b) \\ H(b, n^+) & = F(b, n, H(b, n)) \text{ for all } n \in \omega \end{array} \right.$$

We refer to this scheme as s-$\mathbf{PRIM}_\omega$.

Note that s-$\mathbf{ITER}_\omega$ is essentially a restricted version of s-$\mathbf{PRIM}_\omega$ where B is a singleton set and F does not depend on its first argment.

Theorem: 6.18 (ECST) *Assuming s-$\mathbf{ITER}_\omega$ the axiom s-$\mathbf{PRIM}_\omega$ holds.*

Proof: Let A, B be sets and let $F_0 : B \to A$ and $F : B \times \omega \times A \to A$.

Claim: For each $b \in B$ there is a unique $h : \omega \to A$ such that $h(0) = F_0(b)$ and $F(n^+) = F(b, n, h(n))$.

Proof: Let $A' = \omega \times A$ and let $F' : A' \to A'$ be given by

$$F'(n, a) = (n^+, F(b, n, a))$$

for all $(n, a) \in A'$. By small iteration there is a unique $h' : \omega \to A'$ such that $h'(0) = (0, F_0(b))$ and $h'(n^+) = F'(h'(n))$ for all $n \in \omega$. Let $p_1 : A' \to \omega$ and $p_2 : A' \to A$ be the two projections on A' and let $h : \omega \to A$ be given by $h(n) = p_2(h'(n))$ for all $n \in \omega$. An easy Δ_0 induction shows that $h'(n) = (n, h(n))$ for all $n \in \omega$. It follows that $h(0) = F_0(b)$ and $h(n^+) = p_2(h'(n^+)) = p_2(n, F(b, n, h(n))) = F(b, n, h(n))$ for all $n \in \omega$. It remains to show that h is the unique function satisfying these equations. So let $g : \omega \to A$ such that $g(0) = F_0(b)$ and $g(n^+) = F(b, n, g(n))$ for all $n \in \omega$. Then an easy Δ_0 induction on $n \in \omega$ shows that $g(n) = h(n)$ for all $n \in \omega$ so that $g = h$. $\square$

By the claim there is $G : B \to {}^\omega A$ such that for all $b \in B$ the function $G(b)$ is the unique h such that $h(0) = F_0(b)$ and $h(n^+) = F(b, n, h(n))$ for all $n \in \omega$. Now let $H : B \times \omega \to A$ be given by

$$H(b, n) = G(b)(n)$$

for all $(b, n) \in B \times \omega$. Then H is the unique function desired. $\square$

The proof of the previous result carries over to the class version, where A, B, F_0, F are only assumed to be classes. More generally we get the following result for any standard definability notion Γ.

Theorem: 6.19 (ECST) *Assuming* Γ-$\mathbf{ITER}_\omega$*, the scheme* Γ-$\mathbf{PRIM}_\omega$ *holds.*

Theorem: 6.20 *Heyting arithmetic,* **HA***, can be interpreted in* $\mathbf{ECST} + s$-$\mathbf{ITER}_\omega$.

Proof: Using s-$\mathbf{PRIM}_\omega$ we see that the primitive recursive functions on ω can all be defined. Hence the fact that **HA** can be interpreted in $\mathbf{ECST} + s$-$\mathbf{ITER}_\omega$ follows from Theorem 6.3 and Theorem 6.18. $\square$

6.8 Summary

We can summarise the relationships between the schemes considered here as follows

Theorem: 6.21 (ECST)

1. $\mathbf{IND}_\omega$, $\mathbf{ITER}_\omega$, **FRS**, $\mathbf{PRIM}_\omega$ *are all equivalent schemes.*
2. Γ-$\mathbf{ITER}_\omega$, Γ-**FRS** *and* Γ-$\mathbf{PRIM}_\omega$ *are all equivalent schemes and imply* Γ-$\mathbf{IND}_\omega$.
3. Γ-$\mathbf{IND}_\omega$ *is equivalent to* Γ-$\mathbf{ITER}_\omega$ *if* Γ *is closed under* $\exists$.
4. *The following sequence of implications hold.*

$$\Sigma_1\text{-}\mathbf{ITER}_\omega \Rightarrow \Delta_0\text{-}\mathbf{ITER}_\omega \Rightarrow \mathbf{FPA} \Rightarrow s\text{-}\mathbf{ITER}_\omega.$$

5. s-$\mathbf{ITER}_\omega$ *is equivalent to* s-$\mathbf{PRIM}_\omega$.

Remark: 6.22 It is known that the implication Δ_0-$\mathbf{ITER}_\omega \Rightarrow \mathbf{FPA}$ cannot be made into an equivalence. This is because it is known that **FPA** cannot be used to prove the existence of the ordinal $\omega + \omega$, but it is easy to do this using Δ_0-$\mathbf{ITER}_\omega$. There remain some open problems. Can any of the other implications stated in the previous theorem be made into equivalences? We conjecture that none of them can.

It is worth noting that in the presence of Collection, Σ_1-$\mathbf{IND}_\omega$ actually implies a stronger form of induction on $\mathbb{N}$.

Lemma: 6.23 ($\mathbf{ECST}$ + Collection) Σ_1-$\mathbf{IND}_\omega$ *implies*

$$\Sigma\text{-}\mathbf{IND}_\omega \quad \theta(0) \wedge (\forall n{\in}\omega)(\theta(n) \rightarrow \theta(n+1)) \;\rightarrow\; (\forall n{\in}\omega)\theta(n)$$

for all Σ *formulae* θ*, where the* Σ **formulae** *are the smallest collection of formulae comprising the bounded formulae which is closed under* $\wedge, \vee$*, bounded quantification, and (unbounded) existential quantification.*

Proof: This is due to the fact that every Σ formula is equivalent to a Σ_1 formula provably in **ECST** plus Collection. This equivalence principle is called the Σ **Reflection Principle**. The proof proceeds by induction on the build up of Σ formulae (Exercise!). Details can be found in the proof of Theorem 18.4. □

6.9 Transitive Closures

The principles of the existence of the transitive closure of a (set) relation and of the transitive closure of a set are immediate consequences of the existence of $\mathbb{N}$, assuming a sufficient amount of induction on $\mathbb{N}$.

Definition: 6.24 Let R be a binary relation. A relation R^* is said to be the **transitive closure of** R if $R \subseteq R^*$ and R^* is a transitive relation and for all transitive relations P, whenever $R \subseteq P$, then $R^* \subseteq P$.

Lemma: 6.25 ($\mathbf{ECST}$+$\mathbf{FPA}$) *For every binary relation, the transitive closure exists.*

Proof: Let R be a binary relation. Let

$$A \;=\; \{x \mid \exists y\,[(x,y) \in R \,\vee\, (y,x) \in R]\}.$$

A is a set by Bounded Separation. Let $F = \bigcup_{n\in\mathbb{N}} {}^nA$. By **FPA** and Union-Replacement, F is a set. Let F^* be the subset of F consisting of those $f \in F$ that are R-descending, i.e., whenever $k, k+1 \in \mathbf{dom}(f)$ then $f(k+1)Rf(k)$. Now, put

$$R^* \;=\; \{(f(i), f(j)) \mid f \in F^* \,\wedge\, i,j \in \mathbf{dom}(f) \,\wedge\, i > j\}.$$

R^* is a set, and one easily checks that $R \subseteq R^*$ and that R^* is transitive. To show that R^* is the smallest such relation suppose $R \subseteq P$ and P is transitive. Let aR^*b. Then there exist $n \in \mathbb{N}$, $f \in F^*$, $n > i_0 > j_0$ such that $a = f(i_0)$ and $b = f(j_0)$. By induction on n one readily ensures that for all $i < j < n$, $f(j)Pf(i)$; whereby aPb. $\square$

Another important construction in set theory is the transitive closure of a set.

Definition: 6.26 A set A is said to be **transitive** if elements of elements of A are elements of A, in symbols: $\forall x \in A\, \forall y \in x\; y \in A$.

Given a set B, a set C is said to be the **transitive closure of** B if $B \subseteq C$, C is transitive, and whenever X is transitive set with $B \subseteq X$, then $C \subseteq X$.

Lemma: 6.27 ($\mathbf{ECST} + \Delta_0$-$\mathbf{ITER}_\omega$) *Every set has a transitive closure.*

Proof: Let $F : V \to V$ be the class function defined by $F(x) = x \cup \bigcup x$. V, F are Δ_0 classes. Let b be any set. By Δ_0-$\mathbf{ITER}_\omega$, there exists a function $h : \mathbb{N} \to V$ such that $h(0) = b$ and $h(n+1) = F(h(n))$ for all $n \in \mathbb{N}$. Let $c = \bigcup_{n \in \mathbb{N}} h(n)$. As $b = h(0)$ we have $b \subseteq c$. Let $x \in y \in c$. Then $y \in h(n)$ for some n. Thus $x \in \bigcup h(n) \subseteq h(n+1) \subseteq c$, and hence $x \in c$. This shows that c is transitive. Finally, suppose that $b \subseteq d$, where d is a transitive set. By induction on n one readily establishes that $h(n) \subseteq d$, whence $c \subseteq d$. $\square$

7 The Size of Sets

Here we look at the fundamental definitions of Cantor about the size or cardinality of sets. Frequently, classically equivalent notions of size turn out to be genuinely different when one refrains from using the law of excluded middle.

7.1 Notions of size

To begin with, we review some standard notions and notations pertaining to functions.

We write $f : A \to B$ to indicate that f is a function from A to B. We say that $f : A \to B$ is an **injection** or **one-to-one** (notated $f : A \rightarrowtail B$) if for all $x, y \in A$, whenever $f(x) = f(y)$ then $x = y$; f is a **surjection** or **onto** (notated $f : A \twoheadrightarrow B$) if for all $z \in B$ there exists $x \in A$ such that $f(x) = z$; f is a **bijection** if f is both an injection and a surjection, and the sets A and B are said to be in **one-to-one correspondence** with each other.

If the values of a function are given by an explicit expression $t(x)$ for x in the domain and the domain of the function is understood from the context, we sometimes simply notate the the function by $(x \mapsto t(x))$.

For every $f : A \to B$ and $C \subseteq A$, the set

$$f[C] = \{f(x) \mid x \in C\}$$

is the **image** of C under f, and if $D \subseteq B$, then

$$f^{-1}[D] = \{x \in A \mid f(x) \in D\}$$

is the **pre-image** of D by f.

If $f : A \to B$ is a bijection, then we can define the **inverse function** $f^{-1} : B \to A$ by the condition

$$f^{-1}(y) = x \quad \text{iff} \quad f(x) = y.$$

Exercise: 7.1 *Show that f^{-1} is a bijection.*

The **composition**

$$g \circ f : A \to C$$

of two functions

$$f : A \to B, \qquad g : B \to C$$

is defined by

$$g \circ f(x) = g(f(x)) \qquad (x \in A).$$

Composition is associative:

$$h \circ (g \circ f) \quad = \quad (h \circ g) \circ f.$$

Definition: 7.2 Two sets A, B are **equinumerous** or **equal in cardinality** if there exists a bijection $f : A \to B$. If A and B are equinumerous, we write $A =_c B$, and if $f : A \to B$ is a bijection, we write $f : A =_c B$.

A set A is **less than or equal to** a set B **in size** if it is equinumerous with some subset of B, in symbols:

$$A \leq_c B \quad \text{iff} \quad \exists C \, [C \subseteq B \ \wedge \ A =_c C].$$

The definition of equinumerosity stems from our intuitions about finite sets. The radical element in Cantor's definition is the proposal to accept the existence of such a correspondence as a definition of the notion of same size for arbitrary sets, despite the fact that its application to infinite sets leads to conclusions which had been viewed as counterintuitive. Infinite sets as opposed to finite sets (see Corollary 7.38) can be equinumerous with one of their proper subsets. In "Ein Beitrag zur Mannigfaltigkeitslehre", published in 1878, Cantor established a one-to-one correspondence between the real numbers in the unit interval and the pairs thereof in the unit square $[0, 1] \times [0, 1]$, thereby raising for the first time the problem of dimension.

Lemma: 7.3 (**ECST**) *The relation $=_c$ is reflexive, symmetric and transitive. The relation $\leq_c$ is reflexive and transitive.*

Proof: Obvious. □

Lemma: 7.4 (**ECST**) $A \leq_c B$ *if and only if* $\exists f \, [f : A \rightarrowtail B]$.

Proof: If $A \leq_c B$, then $f : A =_c C$ for some function f and set $C \subseteq B$, and thus $f : A \rightarrowtail B$.

Conversely, if $f : A \rightarrowtail B$, then $A =_c C$, where $C = \{f(u) \mid u \in A\} \subseteq B$. □

Definition: 7.5 Let A be a set. A is **finite** if there exists $n \in \omega$ and a bijection $f : n \to A$. A is **infinite** if $\exists f \, [f : \omega \rightarrowtail A]$. A is **finitely enumerable** if $\exists n \in \omega \, \exists f \, [f : n \twoheadrightarrow A]$. A is **countable** if $\exists f \, [f : \omega \twoheadrightarrow A]$. A is **countably infinite** if $\exists f \, [f : \omega =_c A]$.

Definition: 7.6 For a class A we denote by $\mathcal{P}_{fin}(A)$, $\mathcal{P}_{finEnum}(A)$, and $\mathcal{P}_{\omega}(A)$ the classes of finite subsets of A, finitely enumerable subsets of A, and countable subsets of A, respectively.

Theorem: 7.7 (ECST + FPA) *If A is a set then $\mathcal{P}_{fin}(A)$ and $\mathcal{P}_{finEnum}(A)$ are sets.*

Proof: Exercise. □

Theorem: 7.8 (ECST + EXP) *If A is a set then $\mathcal{P}_{\omega}(A)$ is a set.*

Proof: Exercise. □

In the next definition we consider weaker versions of the foregoing notions.

Definition: 7.9 Let A be a set. A is **subfinite** if A is the surjective image of a subset of a finite set. A is **subcountable** if A is the surjective image of a subset of ω.

A set A is said to be **discrete** if $\forall x, y \in A\,[x = y \lor x \neq y]$.

Clearly, every finitely enumerable set is subfinite, and every subfinite set is subcountable. Also, countable sets are subcountable.

Proposition: 7.10 (**ECST**) *A set is subfinite iff it is a subset of a finitely enumerable set. In other words, "subfinite" is precisely the closure of "finitely enumerable" under subsets.*

Proof: The implication from right to left is trivial. For the converse, assume that A is subfinite. By definition, there exist $n \in \mathbb{N}$, $B \subseteq n$ and $f : B \twoheadrightarrow A$. Take f^* to be the function defined on n such that, for $m < n$,

$$f^*(m) \;=\; \bigcup\{f(k) \mid k \in B \;\wedge\; k = m\}.$$

If $m \in B$, then $f^*(m) = \bigcup\{f(m)\} = f(m)$, so f^* extends f, thus $A \subseteq \mathbf{ran}(f^*)$ and therefore A is a subset of the finitely enumerable set $\mathbf{ran}(f^*)$. □

Proposition: 7.11 (**ECST**) *A set is subcountable iff it is a subset of a countable set. In other words, "subcountable" is precisely the closure of "countable" under subsets.*

Proof: Just as for the foregoing result. $\square$

The next result characterizes the finite sets as special finitely enumerable sets.

Proposition: 7.12 (**ECST** + **FPA**) *A set is finite iff it is finitely enumerable and discrete.*

Proof: Let A be finite. Then there exists $n \in \omega$ and an injection $g : A \rightarrowtail n$. Thus, for $x, y \in A$ we have $g(x) = g(y) \lor g(x) \neq g(y)$ by Theorem 6.3,(10); whence $x = y \lor x \neq y$.

For the converse, suppose $f : n \twoheadrightarrow A$ with A discrete. For $k \leq n$ let f_k be the restriction of f to k. By induction on $k \leq n$ we shall show that

$$\forall x \in A\,[x \in \mathbf{ran}(f_k) \lor x \notin \mathbf{ran}(f_k)]. \tag{2}$$

Clearly, the claim is true for $k = 0$. Now assume that the claim has been established for k_0 and that $k_0 + 1 = k \leq n$. Let $y \in A$. As A is discrete, we have $y = f(k_0) \lor y \neq f(k_0)$. $y = f(k_0)$ implies $y \in \mathbf{ran}(f_k)$. Assume $y \neq f(k_0)$. We then consider the two cases that obtain on account of the inductive assumption. If $y \in \mathbf{ran}(f_{k_0})$ then $y \in \mathbf{ran}(f_k)$. If $y \notin \mathbf{ran}(f_{k_0})$ then $y \notin \mathbf{ran}(f_k)$ as $y \neq f(k_0)$. Therefore, we conclude that $y \in \mathbf{ran}(f_k) \lor y \notin \mathbf{ran}(f_k)$, showing (2).

Next, we employ an induction on $k \leq n$ to show that $\mathbf{ran}(f_k)$ is finite. Since $A = \mathbf{ran}(f_n)$, this entails the desired assertion. We will actually construct a sequence of functions $g_0, \ldots, g_n$ with domains $m_0, \ldots, m_n$, respectively, such that, for all $k \leq n$, $\mathbf{ran}(g_k) = \mathbf{ran}(f_k)$ and $g_k : m_k \rightarrowtail \mathbf{ran}(f_k)$. Moreover, the construction will ensure that for all $i < j \leq n$, $m_i \leq m_j$ and $g_i \subseteq g_j$.

As $\mathbf{ran}(f_0) = \emptyset$, we let $g_0 = \emptyset$ and $m_0 = 0$. Now assume that $k = k_0 + 1$ and that a bijection $g_{k_0} : m_{k_0} \to \mathbf{ran}(f_{k_0})$ has been defined. According to (2), we have $f(k_0) \in \mathbf{ran}(f_{k_0})$ or $f(k_0) \notin \mathbf{ran}(f_{k_0})$. In the former case we have $\mathbf{ran}(f_k) = \mathbf{ran}(f_{k_0})$, and we let $m_k = m_{k_0}$ and $g_k = g_{k_0}$. In the latter case we define the function g_k with domain $n_k = n_{k_0} + 1$ by

$$g_k(i) \quad = \quad \begin{cases} g_{k_0}(i) & \text{if } i < n_{k_0} \\ f(k_0) & \text{if } i = n_{k_0}. \end{cases} \tag{3}$$

Then g_k is 1-1 and sends the numbers $< n_k$ onto $\mathbf{ran}(f_k)$, as desired.

We need **FPA** in the above proof to find a bounding set for the functions g_k. $\square$

Corollary: 7.13 (**ECST** + **FPA**) *Finitely enumerable subsets of* $\mathbb{N}$ *are finite.*

Proof: Subsets of $\mathbb{N}$ are discrete. □

With the help of Proposition 7.12 one also gets a characterization of the countably infinite sets, i.e., the sets in one-to-one correspondence with $\mathbb{N}$.

Corollary: 7.14 (**ECST** + **FPA**) *A set A is in one-to-one correspondence with* $\mathbb{N}$ *iff A is discrete and there exists a surjection $f : \mathbb{N} \twoheadrightarrow A$ such that*

$$\forall n \in \mathbb{N}\, \exists k \in \mathbb{N}\, f(k) \notin \{f(0), \ldots, f(n)\}. \tag{4}$$

Proof: The direction from left to right is trivial. For the converse, assume that A is discrete and that $f : \mathbb{N} \twoheadrightarrow A$ satisfies (4). For $k \in \mathbb{N}$, let f_k be the restriction of f to k. Note that every subset of A is discrete, too. Thus, by the same construction as in the proof of Proposition 7.12 we obtain a non-decreasing sequence of natural numbers $n_0 \leq n_1 \leq \ldots \leq n_k \leq \ldots$ and bijections $g_k : n_k \to \mathbf{ran}(f_k)$ such that $g_k \subseteq g_{k+1}$ holds for all $k \in \mathbb{N}$. Now, let $g = \bigcup_{k\in\mathbb{N}} g_k$. Then g is a 1-1 function with range A since $\mathbf{ran}(g) = \bigcup_{k\in\mathbb{N}} \mathbf{ran}(g_k) = \bigcup_{k\in\mathbb{N}} \mathbf{ran}(f_k) = A$. Let $X = \mathbf{dom}(g)$. It remains to show that $X = \mathbb{N}$. Note first that for $m \in \mathbb{N}$,

$$m \subseteq X \;\to\; (\exists i \in \mathbb{N})\, m \subseteq \mathbf{dom}(g_i). \tag{5}$$

We prove (5) by induction on m. This is trivial for $m = 0$. So let $m > 0$. If the assertion holds for $m-1$ and $m-1 \subseteq X$ then $m-1 \subseteq g_i$ for some $i \in \mathbb{N}$. If $m \subseteq X$, then $m-1 \in \mathbf{dom}(g_j)$ for some $j \in \mathbb{N}$, so that $m \subseteq \mathbf{dom}(g_{\max(i,j)})$.

Next, we prove that

$$(\forall m \in \mathbb{N})\, m \subseteq X. \tag{6}$$

This is obvious for $m = 0$. So let $m > 0$ and assume that $m-1 \subseteq X$. By (5), there exists $l \in N$ such that $m-1 \subseteq \mathbf{dom}(g_l)$. As $\mathbf{ran}(g_l) = \mathbf{ran}(f_l)$, we can employ (4) in selecting a k such that $f(k) \notin \mathbf{ran}(g_l)$. As $f(k) \in \mathbf{ran}(g_{k+1})$ we must have $k+1 > l$ and $n_l < n_{k+1}$, so that $m-1 \leq n_l < n_{k+1}$, yielding $m \subseteq \mathbf{dom}(g_{k+1}) \subseteq X$. Thus, by induction on m, $m \subseteq X$, and hence $g : \mathbb{N} =_c A$. □

Lemma: 7.15 (**ECST**) *If A is an inhabited finitely enumerable set, then A is countable.*

Proof: Let $f : n \twoheadrightarrow A$. Since A is inhabited we must have $n > 0$. Now define $g : \mathbb{N} \twoheadrightarrow A$ by $g(k) = f(k)$ if $k < n$ and $g(k) = f(0)$ if $k \geq n$. $\square$

Lemma: 7.16 (**ECST**+s-**ITER**$_\omega$) *Quotients of finitely enumerable sets are finitely enumerable, i.e., if A is a finitely enumerable set and R is an equivalence relation on C, which is a set, then C/R is finitely enumerable. The union and Cartesian product of two finitely enumerable subsets are finitely enumerable, i.e., if A, B are finitely enumerable sets, then $A \cup B$ and $A \times B$ are finitely enumerable.*

Proof: If $h : k \twoheadrightarrow C$ then $(i \mapsto [h(i)]_R)$ maps k onto C/R.

Let $g : n \twoheadrightarrow A$ and $h : m \twoheadrightarrow B$. Define $f : n+m \to A \cup B$ by $f(k) = g(k)$ if $k < n$ and $f(k) = h(i)$ if $k = n + i$ for some $i < m$. Likewise, as $n \times m$ is in one-to-one correspondence with $n \cdot m$ via $(i, j) \mapsto i \cdot m + j$ and $((i, j) \mapsto (g(i), h(j))$ maps $n \times m$ onto $A \times B$, we see that $A \times B$ is finitely enumerable, too. $\square$

Lemma: 7.17 (**ECST**+s-**ITER**$_\omega$) *The Cartesian product of two finite sets is finite.*

Proof: See the previous proof. $\square$

Remark: 7.18 In general, it is not possible to demonstrate intuitionistically that the union of two finite sets is finite or that the intersection of two finitely enumerable sets is finite also.

Lemma: 7.19 (**ECST** + s-**ITER**$_\omega$) *Subsets, quotients and Cartesian products of subfinite (subcountable) sets are subfinite (subcountable).*

Proof: Exercise. $\square$

Theorem: 7.20 (Cantor) (**ECST** + s-**ITER**$_\omega$) *For each sequence of pairs $(A_i, f_i)_{i\in\mathbb{N}}$, where f_i witnesses the countability of A_i, i.e. $f_i : \omega \twoheadrightarrow A_i$, it holds that*

$$A = \bigcup_{i\in\mathbb{N}} A_i$$

is countable, too.

Proof: If we let

$$a_n^i = f_i(n),$$

then for each i,

$$A_i = \{a_0^i, a_1^i, a_2^i, \ldots\}, \tag{7}$$

and thus

$$A = \{a_0^0, a_0^1, a_1^0, a_0^2, a_1^1, \ldots\}.$$

This is called Cantor's *first diagonal method*. In more detail, the proof uses the *Cantor pairing function* $\pi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by

$$\pi(n, m) = \frac{1}{2}((n+m)^2 + 3n + m).$$

π establishes a one-to-one correspondence between $\mathbb{N} \times \mathbb{N}$ and $\mathbb{N}$ (Exercise). π gives rise to two inverse functions $\sigma, \tau : \mathbb{N} \to \mathbb{N}$ satisfying the equation $\pi(\sigma(k), \tau(k)) = k$ for all numbers k. The enumeration of A in (7) amounts to the same as

$$A \quad = \quad \{f_{\sigma(0)}(\tau(0)), f_{\sigma(1)}(\tau(1)), f_{\sigma(2)}(\tau(2)), \ldots\},$$

and thus the function $n \mapsto f_{\sigma(n)}(\tau(n))$ maps $\mathbb{N}$ onto A. $\square$

Corollary: 7.21 (**ECST**+s-**ITER**$_\omega$) *If B, C are countable sets so is $B \cup C$.*

Proof: Let $g : \mathbb{N} \twoheadrightarrow A$ and $h : \mathbb{N} \twoheadrightarrow B$. Put $A_0 = B$, $f_0 = g$ and for $i > 0$ let $A_i = C$ and $f_i = h$. Then $B \cup C = \bigcup_{i \in \mathbb{N}} A_i$ is countable by Theorem 7.20. $\square$

Corollary: 7.22 (**ECST** + s-**ITER**$_\omega$) *The set of positive and negative integers*

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

is countable.

Proof: $\mathbb{Z} = \mathbb{N} \cup \{-1, -2, \ldots\}$ and the set of negative integers is countable via the correspondence $(n \mapsto -(n+1))$. $\square$

Corollary: 7.23 (**ECST** + s-**ITER**$_\omega$) *The set $\mathbb{Q}$ of rational numbers is countable.*

Proof: Let $\mathbb{N}^+ = \{1, 2, \ldots\}$. The set $\mathbb{Q}^+$ of ≥ 0 rationals is countable because

$$\mathbb{Q}^+ = \bigcup_{n \in \mathbb{N}^+} \{\frac{m}{n} \mid m \in \mathbb{N}\}$$

and each set $\{\frac{m}{n} \mid m \in \mathbb{N}\}$ is countable with the enumeration $(m \mapsto \frac{m}{n})$. The set $\mathbb{Q}^-$ of rationals < 0 is countable by the same method, and therefore the union $\mathbb{Q}^+ \cup \mathbb{Q}^-$ is countable. □

Corollary: 7.24 (**ECST + FPA**) *The sets $\mathbb{Z}$ and $\mathbb{Q}$ are both in one-to-one correspondence with $\mathbb{N}$.*

Proof: Note that $\mathbb{Z}$ and $\mathbb{Q}$ are discrete sets and satisfy (4). Therefore the assertion follows by Corollary 7.22, Corollary 7.23 and Corollary 7.14. □

Corollary: 7.25 (**ECST + FPA**) *For every countable set A, each ${}^nA$ and the union*

$$\bigcup_{n=0}^{\infty} {}^nA$$

are all countable.

Proof: The existence of the sets ${}^nA$ is ensured by the Finite Powers axiom, and thus $\bigcup_{n=1}^{\infty} {}^nA$ is a set by Union-Replacement. Let $g : \mathbb{N} \twoheadrightarrow A$. We construct a sequence of surjections $f_n : \mathbb{N} \twoheadrightarrow {}^nA$ from g by induction on n. Since we find these functions in the set $\bigcup_{n=0}^{\infty} {}^nA$, this induction is justified by Theorem 6.3(3). As ${}^0A = \{0\}$, $(n \mapsto 0)$ maps $\mathbb{N}$ onto ${}^0A$. Next, assume that we have built $f_n : \mathbb{N} \twoheadrightarrow {}^nA$. There is a one-to-one correspondence $F : {}^{n+1}A \to {}^nA \times A$, namely $F(g) = \langle g{\restriction}n, g(n)\rangle$, where $g{\restriction}n$ denotes the restriction of g to the set n. Moreover,

$${}^nA \times A = \bigcup_{i \in \mathbb{N}} ({}^nA \times \{g(i)\}),$$

and each ${}^nA \times \{g(i)\}$ is equinumerous with $\mathbb{N}$ via the correspondence $(i \mapsto \langle f_n(i), g(i)\rangle)$. Hence, by Theorem 7.20 one can explicitly define a map $h : \mathbb{N} \to \bigcup_{i \in \mathbb{N}} ({}^nA \times \{g(i)\})$. Now put $f_{n+1} = F^{-1} \circ h$.

Finally, by means of the functions $f_n : \mathbb{N} \twoheadrightarrow {}^nA$ we find a function

$$f^* : \mathbb{N} \twoheadrightarrow \bigcup_{n=1}^{\infty} {}^nA,$$

again by Theorem 7.20. $\square$

Definition: 7.26 For numbers $n \geq 1$ and sets $A, A_1, \ldots, A_n$,

$$\begin{aligned} A_1 \times \cdots \times A_n &= \{\langle x_1, \ldots, x_n \rangle \mid x_1 \in A_1, \ldots, x_n \in A_n\}, \\ A^n &= \{\langle x_1, \ldots, x_n \rangle \mid x_1, \ldots, x_n \in A\}. \end{aligned}$$

Corollary: 7.27 (**ECST** + Σ_1-$\mathbf{IND}_\omega$)

(i) If $n \in \mathbb{N}$ and $A_1, \ldots, A_n$ are countable (finite, finitely enumerable, subcountable), then their Cartesian product $A_1 \times \cdots \times A_n$ is countable (finite, finitely enumerable, subcountable) also.

(ii) For every countable set A, each A^n ($n \geq 1$) is countable and the union

$$\bigcup_{n=1}^{\infty} A^n = \{(x_1, \ldots, x_n) \mid n \geq 1, x_1, \ldots, x_n \in A\}$$

is countable also.

Proof: (i): First, one needs Σ_1-$\mathbf{IND}_\omega$ to show the existence of the sets $A_1 \times \cdots \times A_n$ by induction on n.

In the case of two sets A, B with enumerations $f : \mathbb{N} \to A$ and $g : \mathbb{N} \to B$ one has

$$A \times B = \bigcup_{i \in \mathbb{N}} (A \times \{g(i)\})$$

and each $A \times \{g(i)\}$ is equinumerous with $\mathbb{N}$ via the correspondence $(n \mapsto (f(n), g(i)))$, so that $A \times B$ is countable by Theorem 7.20. The latter provides the inductive step in proving the countability of $A_1 \times \cdots \times A_n$ by induction on n.

The corresponding results for finite, finitely enumerable, and subcountable sets are left as an exercise.

(ii): Given $f : \mathbb{N} \twoheadrightarrow A$, (i) shows that functions $f_n : \mathbb{N} \twoheadrightarrow A^n$ can be effectively constructed from f by recursion on n. This (of course) requires Σ_1-$\mathbf{IND}_\omega$. Therefore, by Theorem 7.20, it follows that $\bigcup_{n=1}^{\infty} A^n$ is countable, too. $\square$

Theorem: 7.28 (Cantor) (**ECST** + s-$\mathbf{ITER}_\omega$ + $\mathbf{AC}_\omega$) *For each sequence $(A_i)_{i \in \mathbb{N}}$ of countable sets, $A = \bigcup_{i \in \mathbb{N}} A_i$ is countable also.*

Proof: $\mathbf{AC}_\omega$ provides a sequence $(f_i)_{i\in\mathbb{N}}$ of functions $f_i : \omega \twoheadrightarrow A_i$, so that the countability of A follows by Theorem 7.20. $\square$

The classes of subfinite and subcountable sets have further nice closure properties, assuming a little more than **ECST**.

Lemma: 7.29 ($\mathbf{ECST}+\Sigma_1\text{-}\mathbf{IND}_\omega$ or $\mathbf{ECST}+s\text{-}\mathbf{ITER}_\omega+\mathbf{AC}_\omega$) *The class of subfinite (subcountable) sets is closed under finitely enumerable unions: if I is a finitely enumerable set and $(A_i)_{i\in I}$ is a family of subfinite (subcountable) sets, then $\bigcup_{i\in I} A_i$ is subfinite (subcountable).*

Proof: Exercise. $\square$

Lemma: 7.30 ($\mathbf{ECST}+s\text{-}\mathbf{ITER}_\omega+\mathbf{AC}_\omega$) *The class of subcountable sets is closed under countable unions: if I is a countable set and $(A_i)_{i\in I}$ is a family of subcountable sets, then $\bigcup_{i\in I} A_i$ is subcountable.*

Proof: Exercise. $\square$

Definition: 7.31 The **powerclass** $\mathcal{P}(A)$ of a set A is the class of all its subsets,

$$\mathcal{P}(A) \quad = \quad \{X \mid X \text{ is a set and } X \subseteq A\}.$$

Theorem: 7.32 (Cantor) (**ECST**) *For every set A there is no surjection $f : A \twoheadrightarrow \mathcal{P}(A)$.*

Proof: Towards a contradiction, assume that $f : A \twoheadrightarrow \mathcal{P}(A)$. We then define

$$B = \{x \in A \mid x \notin f(x)\}.$$

Note that B is a set by Bounded Separation and that $B \in \mathcal{P}(A)$. Whence, by our assumption, there exists $a_0 \in A$ such that $f(a_0) = B$.

Now, if $a_0 \in B$, then, by definition of B, $a_0 \notin f(a_0)$, so that $a_0 \notin B$, which is a contradiction. So we have shown that $a_0 \notin B$, and thus $a_0 \notin f(a_0)$. But the latter entails that $a_0 \in B$, contradicting $a_0 \notin B$. Having reached a contradiction, we conclude that there can't be an f satisfying $f : A \twoheadrightarrow \mathcal{P}(A)$. $\square$

Theorem: 7.33 (**ECST**) *For every function* $F : \mathbb{N} \to {}^{\mathbb{N}}\mathbb{N}$ *there exists* $g \in {}^{\mathbb{N}}\mathbb{N}$ *such that* g *is not in the range of* F*.*

As a result, there is no surjection $G : \mathbb{N} \twoheadrightarrow {}^{\mathbb{N}}\mathbb{N}$*.*

Proof: Assume that we have a function $F : \mathbb{N} \to {}^{\mathbb{N}}\mathbb{N}$. Define f_n to be $F(n)$ and let $f_\Delta : \mathbb{N} \to \mathbb{N}$ be defined by

$$f_\Delta(n) = f_n(n) + 1.$$

As f_Δ takes a different value than f_n at n, we conclude that $f_\Delta \notin F[\mathbb{N}]$, and hence F is not surjective. $\square$

Theorem: 7.34 (**ECST**) $\mathcal{P}(\mathbb{N})$ *is not subcountable.*

Proof: Exercise. $\square$

Remark: 7.35 It is consistent with **CZF** (even with **IZF** if that theory is consistent) that ${}^{\mathbb{N}}\mathbb{N}$ is subcountable.

7.2 The Pigeonhole principle

Finite sets have the pivotal property that they are not equinumerous with any of their proper subsets. We show that this result, known as the *Pigeonhole Principle*, can be established on the basis of **ECST** + **FPA**.

Variables $k, m, n, n_0, \ldots$ range over elements of ω.

Lemma: 7.36 (**ECST**) *Let* $n_0 < m$*. Then* $m = m_0 + 1$ *for some* m_0 *and*

$$\{k \,:\, k < m \wedge k \neq n_0\} \quad =_c \quad m_0.$$

Proof: By Theorem 6.3(1), since $m \neq 0$ there exists m_0 such that $m = m_0 + 1$. Now, define $g : m_0 \to \{k \,:\, k < m \wedge k \neq n_0\}$ by

$$g(k) \quad = \quad \begin{cases} k & \text{if } k < n_0 \\ k+1 & \text{if } k \geq n_0 \end{cases} \tag{8}$$

That g is a function and, moreover, is 1-1 and onto follows from Theorem 6.3 (Exercise). $\square$

Theorem: 7.37 (**ECST** + **FPA**) **Pigeonhole Principle**: *Every injection $f : A \rightarrowtail A$ on a finite set into itself is also a surjection, i.e. $f[A] = A$.*

Proof: It is enough to prove that for every natural number m and each $g \in \bigcup_{n \in \mathbb{N}} {}^n\mathbb{N}$, whenever $g : m \rightarrowtail m$, then $g : m \twoheadrightarrow m$. The proof is (naturally) by induction on m. $\bigcup_{n \in \mathbb{N}} {}^n\mathbb{N}$ being a set by the Finite Powers Axiom, **FPA**, it follows from Theorem 6.3(3) that this induction can be carried out in the given background theory.

The assertion is trivial when $m = 0$. So assume inductively that the assertion holds for m_0. Suppose that $f : m_0 + 1 \rightarrowtail m_0 + 1$. Now, let f^* be the restriction of f to m_0. Then $f^* : m_0 \rightarrowtail X$, where $X = \{k : k < m_0 + 1 \wedge k \neq f(m_0)\}$. By Lemma 7.36, there is a bijection $h : X \to m_0$. As a result, $h \circ f^* : m_0 \rightarrowtail m_0$. And hence, by the inductive assumption, $h \circ f^*$ is a surjection. This implies that f^* must be a surjection, too, and therefore f has to be surjective as well. $\square$

Corollary: 7.38 (**ECST** + **FPA**) *A finite set cannot be equinumerous with one of its proper subsets.*

Corollary: 7.39 (**ECST** + **FPA**) *For each finite set A, there exists exactly one natural number n such that $A =_c n$. (This justifies that we call this number n the number of elements of A and denote it by $\sharp(A)$.)*

Proof: If $A =_c n$ and $A =_c m$ with $n < m$, then m would be equinumerous with its proper subset n. $\square$

Definition: 7.40 A set A has **at most n elements** if whenever $a_0, \ldots, a_n \in A$, then there exist $0 \leq i < j \leq n$ such that $a_i = a_j$.

We introduce a further notion of finiteness. A set is **bounded in number**, or **bounded**, if it has at most n elements for some n.

Lemma: 7.41 (**ECST**) *Every subfinite set is bounded.*

Proof: Exercise. $\square$

The pigeonhole principle can also be established for finitely enumerable sets, as was observed by Klaus Thiel. Before we prove this result we shall list several useful facts about finite and finitely enumerable sets.

Lemma: 7.42 (**ECST** + **FPA**) *If E is a finitely enumerable set and B is an arbitrary set then ${}^E B$ is a set.*

Proof: Let $f : n \twoheadrightarrow E$. By **FPA**, ${}^n B$ is set. Let

$$X \quad = \quad \{g \in {}^n B \mid \forall k, k' < n \, [f(k) = f(k') \to g(k) = g(k')]\}$$

and define $F : X \to {}^E B$ by

$$F(g) \quad = \quad \{\langle f(k), g(k) \rangle \mid k < n\}.$$

One easily checks that $F(g)$ is a function from E to B for every $g \in X$. Given $h : E \to B$ define $g : n \to B$ by $g(k) = h(f(k))$ for $k < n$. Then $g \in X$ and $F(g) = h$. Thus F surjects the set X onto ${}^E B$ and therefore ${}^E B$ is a set using Replacement. $\square$

The next lemma states a provable "choice" principle for finite sets.

Lemma: 7.43 (**ECST** + **FPA**) *Let A be a finite set, B be an arbitrary set and $R \subseteq A \times B$ be a relation from A to B such that $\forall x \in A \, \exists y \in B \; xRy$. Then there exists a function $f : A \to B$ such that $\forall x \in A \; xRf(x)$.*

Proof: Without loss of generality we may assume that $A = n$ for some $n \in \mathbb{N}$. We proceed by induction on $m \leq n$ to show that there exists a function $f_m : m \to B$ such that $\forall k < m \, kRf_m(k)$. This is trivial for $m = 0$. So suppose the claim holds for $m < n$. By assumption there exists $y_0 \in B$ such that mRy_0. Now let $f_{m+1} = f_m \cup \{\langle m, y_0 \rangle\}$.

Note that **FPA** ensures that $C := \bigcup_{m \leq n} {}^n B$ is a set. Hence as $f_m \in C$ holds for all $m \leq n$, the above induction formula is of complexity Δ_0. $\square$

Lemma: 7.44 (**ECST**) *Let A be a finite set and B be a discrete set. If $f : A \to B$ then f is one-to-one or $\exists x, y \in A \, [x \neq y \, \wedge \, f(x) = f(y)]$.*

Proof: Again, we may assume that $A = n$ for some $n \in \mathbb{N}$. For $k \leq n$ let f_k be the restriction of f to k. As in the proof of Proposition 7.12 (2) we then have

$$\forall y \in B \, [y \in \mathbf{ran}(f_k) \; \vee \; y \notin \mathbf{ran}(f_k)]. \tag{9}$$

By induction on $k \leq n$ we shall prove that

$$f_k : k \rightarrowtail B \; \vee \; \exists i, j < k \, [i \neq j \; \wedge \; f(i) = f(j)]. \tag{10}$$

As $f_0 : 0 \rightarrowtail B$ the claim holds for $k = 0$. Now suppose $k = k_0 + 1$ and by the inductive assumption that

$$f_{k_0} : k_0 \rightarrowtail B \ \vee \ \exists i, j < k_0 \, [i \neq j \ \wedge \ f(i) = f(j)]. \tag{11}$$

Case 1 $f(k_0) \in \mathbf{ran}(f_{k_0})$: Then $f(k_0) = f(i)$ for some $i < k_0$ and thus (10) holds.

Case 2 $f(k_0) \notin \mathbf{ran}(f_{k_0})$: If $f_{k_0} : k_0 \rightarrowtail B$ holds we also have $f_k : k \rightarrowtail B$. On the other hand, if $\exists j, i < k_0 \, [i \neq j \ \wedge \ f(i) = f(j)]$ then also $\exists j, i < k \, [i \neq j \ \wedge \ f(i) = f(j)]$.

Since one of these possibilities must obtain according to (11), we get (10). $\square$

Theorem: 7.45 (Klaus Thiel) (**ECST+FPA**) **Pigeonhole Principle for finitely enumerable sets**: *Every injection $f : E \rightarrowtail E$ of a finitely enumerable set into itself is also a surjection, i.e. $f[E] = E$.*

Proof: Let E be finitely enumerable and $f : E \rightarrowtail E$. We say that E is n-enumerable if $g : n \twoheadrightarrow E$ holds for some g and $n \in \mathbb{N}$. By induction on n we shall show that if E is n-enumerable then $f : E \twoheadrightarrow E$.

Suppose $g : n \twoheadrightarrow E$. Since $f : E \rightarrow E$ we have

$$\forall k < n \, \exists l < n \; f(g(k)) = g(l),$$

so that by Lemma 7.43 there exists a function $h : n \rightarrow n$ such that

$$\forall k < n \; f(g(k)) \;\; = \;\; g(h(k)). \tag{12}$$

By Lemma 7.44, $h : n \rightarrowtail n$ or $\exists i, j < n \, [i \neq j \ \wedge \ h(i) = h(j)]$.

If $h : n \rightarrowtail n$ then $h : n \twoheadrightarrow n$ by the pigeonhole principle for finite sets, i.e., Theorem 7.37. Thus $g \circ h : n \twoheadrightarrow E$, and hence f must be surjective owing to (12).

Next, suppose that there are $i, j < n$ with $i \neq j$ and $h(i) = h(j)$. Let $i < j$ and $n = n_0 + 1$. Hence

$$f(g(i)) = g(h(i)) = g(h(j)) = f(g(j))$$

by (12), and thus $g(i) = g(j)$ as f is one-to-one.

Define

$$g'(k) \;\; = \;\; \begin{cases} g(k) & \text{if } k < j \\ g'(k+1) & \text{if } j \leq k < n_0 \end{cases} \tag{13}$$

Then $\mathbf{ran}(g') = \mathbf{ran}(g)$ as $g(j) = g'(i)$ and thus $g' : n_0 \twoheadrightarrow E$. As a result, E is n_0-enumerable and the inductive assumption yields that f is surjective.

It remains to show that the above induction is feasible in our background theory. This follows from the fact that $\bigcup_{n \in N} {}^{n}E$ is a set due to **FPA**, making the notion of n-enumerability Δ_0. $\square$

Problems

- (**ECST**) Prove that for all sets A, B, C,

$$((A \times B) \to C) \quad =_c \quad (A \to (B \to C)).$$

- (**ECST**) The Wiener pair is defined as follows:

$$(x, y)_w \quad = \quad \{\{0, \{x\}\}, \{\{y\}\}\}.$$

  Show that for all sets x, y, x', y',

$$(x, y)_w = (x', y')_w \quad \text{iff} \quad x = x' \ \wedge \ y = y'.$$

- (**ECST**$+\Sigma_1$-**IND**$_\omega$) or (**ECST**$+$**FPA**$+$**AC**$_\omega$) If E is a finitely enumerable set and every member of E is finitely enumerable, then the unionset $\bigcup E$ is also finitely enumerable.

- (**ECST** $+$ **FPA**) The Cartesian product of two finite sets A, B is finite and such that

$$\sharp(A \times B) = \sharp(A) \cdot \sharp(B).$$

- (**ECST** $+$ **FPA**) Assume the existence of the set of real numbers, $\mathbb{R}$. Let $x < y$ where x, y are reals, ∞ or $-\infty$ and let $(x, y) = \{u \in \mathbb{R} \mid x < u < y\}$. Construct bijections which prove the equinumerosities

$$(x, y) =_c (0, 1) =_c \mathbb{R}.$$

- (**ECST** $+$ **FPA**) Show that if A is a set in one-to-one correspondence with $\mathbb{N}$ then $\bigcup_{n=0}^{\infty} {}^{n}A$ is in one-to-one correspondence with $\mathbb{N}$.

- (**ECST**) Show that the function $g : m_0 \to \{k \ : \ k < m \wedge k \neq n_0\}$ of the proof of Lemma 7.36 is 1-1 and onto.

8 The Continuum

8.1 The Classical Continuum

In classical mathematics the continuum, viewed as a field, can be characterised, up to a rigid isomorphism, as a complete totally ordered field. Many constructions of a complete totally ordered field have been given, usually as a completion of the rationals. Perhaps the two most well known are the Dedekind cuts construction and the Cauchy sequence construction. In practise, whatever construction is used, the process is a somewhat tedious matter when carried out in full detail. For that reason most textbooks on Analysis avoid the details by taking an axiomatic approach in which the existence of the set of real numbers satisfying the axioms for a complete totally ordered field is assumed, or a sketch of a proof of existence is left to an appendix.

8.2 Some Algebra

In this chapter we will usually assume only the axioms of **ECST**. So we do not assume Subset Collection or even Exponentiation. For this reason we will need to work with algebraic structures having a class of elements that need not be a set. We will call a structure *small* when the elements form a set.

The standard classical definitions of the notions of group, abelian group, ring (commutative with 1) carry over to constructive mathematics without problems, as do the notions of partial and total orders. Starting from the structure $(\mathbb{N}, 0, S)$ of the natural numbers satisfying the Dedekind-Peano axioms, the classical set theoretic constructions of the totally ordered rings $\mathbb{N}$, $\mathbb{Q}$ of integers and rationals also carry over easily. We do not stop to review the details, which can be found in many textbooks. It is important to note that the equality and inequality relations on $\mathbb{Q}$ are decidable. This will not be the case for these relations on $\mathbb{R}$. Nor will the partial order relation on $\mathbb{R}$ be total. We next formulate the notions we will need to characterise the real numbers in Constructive Set Theory.

Definition: 8.1 *Let $<$ be a class relation on a class R. We consider the following posible properties.*

$P1$: $[x < y \ \wedge\ y < z] \Rightarrow x < z$,

$P2$: $\neg[x < y \ \wedge\ y < x]$,

$P3$: $x < y \Rightarrow [x < z \ \vee\ z < y]$,

$P4$**:** $\neg[x < y \ \vee \ y < x] \Rightarrow x = y$,

$P5$**:** $[x < y \ \vee \ x = y \ \vee \ y < x]$,

$P6$**:** $[x < y] \ \vee \ \neg[x < y]$.

1. *$<$ is a* strict partial ordering of R *if $P1, P2, P3$, for all $x, y, z \in R$,*
2. *$<$ is a* pseudo-ordering of R *if $P2, P3, P4$, for all $x, y, z \in R$,*
3. *$<$ is a* strict total ordering of R *if $P1, P2, P5$, for all $x, y, z \in R$,*

Exercise: 8.2 *Show that every pseudo-ordering is a strict partial ordering and a relation $<$ is a strict total ordering iff it is a decidable pseudo-ordering. So classically the notions of pseudo-order and strict total order are equivalent.*

Definition: 8.3 *A class relation $\leq$ on a class R is a* partial order *if, for all $x, y, z \in R$,*

1. *$x \leq x$,*
2. *$[x \leq y \ \wedge \ y \leq z] \Rightarrow [x \leq z]$,*
3. *$[x \leq y \ \wedge \ y \leq x] \Rightarrow [x = y]$.*

Exercise: 8.4 *Show that if $<$ is a pseudo-order then $\leq$ is a partial order, where, for $x, y \in R$,*

$$[x \leq y] \iff \neg[y < x].$$

Definition: 8.5 *Let $<$ be a pseudo-ordering of a class R and let X be a subclass of R. Let*

$$X^{<} = \{u \in R \mid (\exists x \in X)\ u < x\}.$$

An element $a \in R$ is an upper bound of X *if $a \notin X^{<}$; i.e. $x \leq a$ for all $x \in X$. It is a* least upper bound (lub) of X *if also $a \leq b$ for every upper bound b of X. The class X is* bounded above *if it has an upper bound. An element $a \in R$ is a* supremum (sup) *of X if $X^{<} = \{a\}^{<}$. The class X is* upper-located *if, for $x, y \in R$,*

$$x < y \Rightarrow [x \in X^{<} \vee y \notin X^{<}].$$

The pseudo-ordered class R is defined to be upper Dedekind complete *if every inhabited, bounded above, upper-located subset has a supremum.*

Note that if $<$ is a pseudo-ordering of R and we define

$$x > y \;\Leftrightarrow\; y < x$$

then $>$ is also a pseudo-ordering of R and using it we can define $\geq$ and, for each subclass X of R, $X^{>}$, lower bounds, greatest lower bounds and infimums of X, etc.

Exercise: 8.6 *Let R be a class with a pseudo-ordering $<$. Show the following.*

1. *Any lub of a set is unique if it exists.*
2. *If a is a sup of a class X then a is the lub of X and X is upper-located.*

Definition: 8.7 *A* pseudo-ordered abelian group *consists of an abelian group with a pseudo-ordering $<$ of its class R of elements, such that, for all $x, y, z \in R$,*

$$x < y \Rightarrow x + z < y + z.$$

It is Archimedean *if, for all $x, y \in R$ with $0 < y$, there is $n \in \mathbb{N}$ such that*

$$x < \overbrace{y + \cdots + y}^{n}.$$

Definition: 8.8 *A* pseudo-ordered ring *is a (commutative with 1) ring together with a pseudo-ordering that makes the underlying abelian group a pseudo-ordered abelian group and such that if $0 < z$ then*

$$x < y \Rightarrow xz < yz.$$

It is a pseudo-ordered field *if $0 < x$ implies that $xy = 1$ for some y.*

8.3 The Dedekind Reals

We assume that the small totally ordered field $(\mathbb{Q}, <, +, -, \cdot, 0, 1)$ of rational numbers has been introduced in one of the standard ways.

Since the time of the ancient Greeks we know that the rationals do not adequately represent the continuum of points on the real line. For example there is a gap between the rationals r such that $r^2 < 2$ and the rationals r such that $r^2 > 2$. The real numbers are introduced to extend the rationals so that there are no longer such gaps.

The Classical Dedekind reals is the order completion of the rationals. It can be defined to consist of the inhabited, bounded above sets X of rationals such that $X = X^<$. We call these sets the *weak left cuts* and call a weak left cut a *left cut* if it is located. As $X = X^<$ when X is a weak left cut, X is located iff for all $r, s \in \mathbb{Q}$

$$r < s \Rightarrow r \in X \text{ or } s \notin X.$$

In classical mathematics the notion of a weak left cut is good enough , as classically every weak left cut is located and so is a left cut. A crucial property of the reals is that every real can be aproximated arbitrarily closely by a rational number. The locatedness property is needed in order to achieve this.

Proposition: 8.9 *Every left cut X can be approximated arbitrarily closely by a rational; i.e. for every positive rational ϵ there is $r \in X$ such that $r + \epsilon \notin X$. We write that X is* convergent *when it has this property.*

Proof: Let X be a left cut and let $\epsilon > 0$ be in $\mathbb{Q}$. Choose rationals s, s' such that $s \in X$ and $s' \notin X$. Then $s < s'$ and we may choose an integer $n > 0$ such that $(s' - s)/(\epsilon/2) < n$. Then $s' < s + n\epsilon/2$. For each $i \in \mathbb{N}$ let

$$r_i = (s - \epsilon/2) + i\epsilon/2.$$

So $r_0, r_1 \in X$ and $r_{n+1} \notin X$. For each i, as $r_i < r_{i+1}$ and X is upper-located we have

$$r_i \in X \text{ or } r_{i+1} \notin X.$$

So,

$$(\forall i \leq n)(\exists j \in \{0, 1\})[(j = 0 \wedge r_i \in X) \vee (j = 1 \wedge r_{i+1} \notin X)].$$

By Lemma 7.43 there is a function $f : \mathbb{N}_{n+2} \to \{0, 1\}$ such that, for all $i \in \mathbb{N}_{n+2}$

$$(f(i) = 0 \wedge r_i \in X) \vee (f(i) = 1 \wedge r_{i+1} \notin X).$$

Note that the Lemma uses **FPA**. Then $f(0) = 0$, as $r_1 \in X$, and $f(n+1) = 1$, as $r_{n+1} \notin X$. Let n' be the least $i \leq n + 1$ such that $f(i) = 1$. Then $n' > 0$ and

$$r_{n'-1} \in X \text{ and } r_{n'+1} \notin X.$$

So, putting $r = r_{n'-1}$, we get that $r \in X$ and $r + \epsilon = r_{n'+1} \notin X$. □

Corollary: 8.10 *A set of rationals is a left cut iff it is a convergent set X such that $X = X^<$.*

Definition: 8.11 *We define the class* $\mathbb{R}$ *of real numbers to be the class of all left cuts. We define the relation* $<$ *on* $\mathbb{R}$ *as follows. For* $X, Y \in \mathbb{R}$ *let* $X < Y$ *if some rational is in* Y *that is not in* X*.*

Exercise: 8.12 *Show that the relation* $<$ *on* $\mathbb{R}$ *is a pseudo-ordering of* $\mathbb{R}$ *and, for* $X, Y \in \mathbb{R}$*,*

$$X \leq Y \quad \Leftrightarrow \quad X \subseteq Y.$$

If R is a class with a pseudo-ordering, a function $f : \mathbb{Q} \to R$ is defined to be a *fully dense embedding*, $f : (\mathbb{Q}, <) \to (R, <)$ if it is order preserving; i.e. $r < s$ in $\mathbb{Q}$ implies $f(r) < f(s)$ in R and, whenever $a < b$ in R, there are $r_1, r_2, r_3 \in \mathbb{Q}$ such that $f(r_1) < a < f(r_2) < b < f(r_3)$.

Exercise: 8.13 *Show that the function that assigns to each* $r \in \mathbb{Q}$ *the set* $r^* = \{s \in \mathbb{Q} \mid s < r\}$ *of rationals defines a fully dense embedding* $(\mathbb{Q}, <) \to (\mathbb{R}, <)$*.*

Theorem: 8.14 *The structure* $(\mathbb{R}, <)$ *is an upper Dedekind complete pseudo-ordered class.*

Proof: Let $\mathcal{Y} \subseteq \mathbb{R}$ be a an inhabited, bounded above and upper-located set. Let $\overline{Y} = \bigcup \mathcal{Y}$. We will show that $\overline{Y} \in \mathbb{R}$ and is the supremum of $\mathcal{Y}$.

As $\mathcal{Y}$ is inhabited there is some $Y \in \mathcal{Y}$. As Y is inhabited there is $r \in Y$. Hence $r \in \overline{Y}$. Thus $\overline{Y}$ is inhabited.

As $\mathcal{Y}$ is bounded above there is $Z \in \mathbb{R}$ such that $Y \subseteq Z$ for all $Y \in \mathcal{Y}$. It follows that $\overline{Y} \subseteq Z$ so that, as Z is bounded above, $\overline{Y}$ is bounded above. Observe that

$$\begin{array}{rcl} r \in \overline{Y}^< & \Leftrightarrow & \exists s \in \overline{Y}\; r < s \\ & \Leftrightarrow & \exists Y \in \mathcal{Y}\; \exists s \in Y\; r < s \\ & \Leftrightarrow & \exists Y \in \mathcal{Y}\; r \in Y^< \\ & \Leftrightarrow & \exists Y \in \mathcal{Y}\; r \in Y, \text{ as } Y = Y^< \text{ for } Y \in \mathcal{Y}, \\ & \Leftrightarrow & r \in \overline{Y} \end{array}$$

Thus $\overline{Y}^< = \overline{Y}$.

To complete the proof that $\overline{Y} \in \mathbb{R}$ it remains to show that $\overline{Y}$ is upper-located. So let $r < s$ in $\mathbb{Q}$. We must show that $r \in \overline{Y}$ or $s \notin \overline{Y}$. As $\mathcal{Y}$ is upper-located in $\mathbb{R}$ and $r^* < s^*$ we get that $r^* \in \mathcal{Y}^<$ or $s^* \notin \mathcal{Y}^<$. Observe that, for any $t \in \mathbb{Q}$,

$$\begin{array}{rcl} t^* \in \mathcal{Y}^< & \Leftrightarrow & t^* < Y, \text{ some } Y \in \mathcal{Y} \\ & \Leftrightarrow & \exists Y \in \mathcal{Y}\; \exists t' \in Y\; t' \notin t^* \\ & \Leftrightarrow & \exists Y \in \mathcal{Y}\; \exists t' \in Y\; t' \geq t \\ & \Leftrightarrow & \exists t' \in \overline{Y}\; t' \geq t \\ & \Leftrightarrow & t \in \overline{Y} \end{array}$$

So $r \in \overline{Y}$ or $s \notin \overline{Y}$, as desired. It only remains to show that $\overline{Y}$ is the sup of $\mathcal{Y}$. Observe that, for $X \in \mathbb{R}$,

$$\begin{aligned} \exists Y \in \mathcal{Y}\, X < Y \quad &\Leftrightarrow\ \exists Y \in \mathcal{Y}\, \exists r \in Y\ r \notin X \\ &\Leftrightarrow\ \exists r \in \overline{Y}\ r \notin X \\ &\Leftrightarrow\ X < \overline{Y} \end{aligned}$$

as required. □

We have the following categorical characterisation of the structure $(\mathbb{R}, <)$.

Theorem: 8.15 *The structure $(\mathbb{R}, <)$ is the unique, up to isomorphism, structure $(R, <)$ such that the relation $<$ on R is an upper Dedekind complete pseudo-ordering of R having a fully dense embedding $f : \mathbb{Q} \to R$ such that $\{r \in \mathbb{Q} \mid f(r) < a\}$ is a set for all $a \in R$.*

Proof: It is clear from our previous work that the structure $(\mathbb{R}, <)$ has the properties stated in the theorem. Now let $(R, <)$ be a structure with $f : \mathbb{Q} \to R$ having the stated properties.

Claim: $fX = \{fr \mid r \in X\}$ *is an inhabited, bounded above, upper-located subset of R.*

Proof: As X is inhabited so is fX. As X is bounded above there is $r \in \mathbb{Q}$ such that, for $s \in X$, $s \leq r$ and hence $fs \leq fr$. So

$$\begin{aligned} a \in fX \quad &\Rightarrow a = fs,\ \text{some } s \in X \\ &\Rightarrow a \leq fr \end{aligned}$$

Thus fX is bounded above.

To show that fX is upper-located let $x < y$ in R. As f is a fully dense embedding there is $r \in \mathbb{Q}$ such that $x < fr < y$ and so there is $s \in \mathbb{Q}$ such that $fr < fs < y$. Then, as $r < s$, either $r \in X$ or $s \notin X$. If $r \in X$ then $fr \in fX$ so that $x \in (fX)^<$, as $x < fr$. Also

$$\begin{aligned} y \in (fX)^< \quad &\Rightarrow y < ft,\ \text{some } t \in X \\ &\Rightarrow fs < ft,\ \text{some } t \in X,\ \text{as } fs < y, \\ &\Rightarrow s < t,\ \text{some } t \in X, \\ &\Rightarrow s \in X \text{ as } X^< \subseteq X \end{aligned}$$

So $s \notin X \Rightarrow y \notin (fX)^<$. Thus $x \in (fX)^<$ or $y \notin (fX)^<$. □

By the claim we may define $g : \mathbb{R} \to R$ by

$$gX = \text{ the sup of } (fX),$$

for $X \in \mathbb{R}$. We show that g is a strictly order-preserving surjection and hence an isomorphism $(\mathbb{R}, <) \sim (R, <)$. So let $X < Y$ in $\mathbb{R}$. We may find $r, s \in \mathbb{Q}$ such that $X < r^* < s^* < Y$. As $X < r^*$, $r \notin X$. But if $fr < gX$ then $fr < fr'$ and hence $r < r'$ for some $r' \in X$ so that $r \in X$. So $fr \not< gX$. Also, as $fr < fs$, either $fr < gX$ or $gX < fs$, so that $gX < fs$. As $s \in Y$, $gX < gY$. Thus g is strictly order-preserving.

To show that g is surjective let $x \in R$ and let $X = \{r \in \mathbb{Q} \mid fr < x\}$. We show that $X \in \mathbb{R}$ and $gX = x$. As $fr < x$ for some $r \in \mathbb{Q}$, X is inhabited. As $x < fs$ for some $s \in \mathbb{Q}$, X is upper-bounded. Also $X^< = X$, as

$$\begin{aligned} r \in X^< \quad & \Leftrightarrow \exists s \in X\ r < s \\ & \Leftrightarrow \exists s \in \mathbb{Q}\ [fs < x \wedge fr < fs] \\ & \Leftrightarrow fr < x \\ & \Leftrightarrow r \in X. \end{aligned}$$

X is upper-located as

$$\begin{aligned} r < s \ & \Rightarrow fr < fs \\ & \Rightarrow [fr < x \vee x < fs] \\ & \Rightarrow [r \in X \vee s \notin X]. \end{aligned}$$

Thus $X \in \mathbb{R}$. Finally, $x = gX$; i.e. x is the sup of fX as, for $y \in R$,

$$\begin{aligned} y < x \quad & \Leftrightarrow y < fr < x, \text{ some } r \in \mathbb{Q} \\ & \Leftrightarrow y < fr, \text{ some } r \in X \\ & y \in (fX)^<. \end{aligned}$$

□

The additive and multiplicative structure on $\mathbb{R}$

It is easy to define addition on $\mathbb{R}$. For $X, Y \in \mathbb{R}$ let

$$X + Y = \{a + b \mid a \in X \text{ and } b \in Y\}.$$

It is easy to check that this forms an abelian group with zero 0^* and inverse given by $-X = \{-r \mid r \notin X\}^<$. In fact we have the following result.

Proposition: 8.16 *The structure* $(\mathbb{R}, <, +, -, 0^*)$ *forms an Archimedean pseudo-ordered abelian group.*

Proof: Exercise.

It is less easy to define multiplication on $\mathbb{R}$. A standard classical approach is to define $X \cdot Y$ by cases depending on the four cases whether X is positive or not combined with whether Y is positive or not. In constructive mathematics we cannot generally decide which cases hold. In the case when both X and Y are positive we can define

$$X \cdot Y = \{a.b \mid a \in X \ \& \ b \in Y\}^{<}.$$

We can also define X^{-1} for positive X as follows.

$$X^{-1} = \{a^{-1} \mid a \notin X\}^{<}.$$

With these definitions it is easy to see that the class $\mathbb{R}^{>0}$ of positive reals forms an abelian group under multiplication, with unit 1^* and inverse operation $(\ )^{-1}$. Moreover, on this class multiplication distributes over addition. In this situation there is a fairly standard method that will extend multiplication to the whole of $\mathbb{R}$ so as to get a pseudo-ordered commutative ring with unit. It will be a field in the sense that each positive or negative element has an inverse. We do not go into the tedious details. The key idea is that each real X can be represented as $X_+ - X_-$, where X_+, X_- are positive reals. If Y is also given such a representation then we can define

$$X \cdot Y = [X_+ \cdot Y_+ + X_- \cdot Y_-] - [X_+ \cdot Y_- + X_- \cdot Y_+].$$

Of course these representations of X and Y are not unique and it is necessary to prove that this definition is independent of the choice of representatives. But this can be done. We also need to define X^{-1} when X is negative. In that case $-X$ is positive and we define

$$X^{-1} = (-X)^{-1}.$$

Also, it is straightforward to check that the fully dense embedding $(\ )^* : (\mathbb{Q}, <) \to (\mathbb{R}, <)$ defined in Exercise 8.13 also preserves the field structure. In summary we have the following result.

Proposition: 8.17 *The reals $\mathbb{R}$ forms an Archimedean, upper-located complete, pseudo-ordered field $(\mathbb{R}, <, +, -, 0^*, 1^*)$ such that every element is the sup of some subset. Moreover $(\ )^*$ is a pseudo-ordered field embedding $(\mathbb{Q}, <, ...) \to (\mathbb{R}, <, ...)$.*

In fact, by the following exercise we have a rigidly categorical characterisation of the reals. Recall that the rationals form an Archimedean ordered field $(\mathbb{Q}, <, +, -, ., 0, 1)$.

Exercise: 8.18 *Show that if $(R, <, ...)$ is any Archimedean pseudo-ordered field then there is a unique fully dense embedding $g : (\mathbb{Q}, <) \to (R, <)$ that also preserves the field structure. Moreover, if $(R, <, ...)$ is also upper-located complete such that every element is the sup of some subset then g determines a unique pseudo-ordered field isomorphism*

$$f : (\mathbb{R}, <, ...) \cong (R, <, ...)$$

such that $f(r^*) = g(r)$ for all $r \in \mathbb{Q}$.

If $(R, <, ...)$ is an Archimedean pseudo-ordered field and $g : (\mathbb{Q}, <) \to (R, <)$ is the unique fully dense embedding then we will write r^* for $g(r)$. This agrees with the notation we have been using when $R = \mathbb{R}$.

Classically the real numbers is Cauchy complete; i.e. every Cauchy sequence converges. We can show that this is still true in constructive set theory. As is usual in constructive mathematics we will use strong notions of Cauchy sequence and convergent sequence which require that the sequence has an explicit modulus function of the appropriate kind.

Definition: 8.19 *Let $(R, <, ...)$ be an Archimedean pseudo-ordered field. Let $\{x_n\}_{n\in\mathbb{N}}$ be a sequence of elements $x_n \in R$*

- *It is a* Cauchy sequence *if there is a modulus function $h : \mathbb{Q}^{>0} \to \mathbb{N}^{>0}$ such that for all $\epsilon \in \mathbb{Q}^{>0}$, if $n, m \geq h(\epsilon)$ then*

$$-\epsilon^* \leq x_n - x_m \leq \epsilon^*.$$

- *It* converges to *$x \in R$ if there is a modulus function $h : \mathbb{Q}^{>0} \to \mathbb{N}^{>0}$ such that for all $\epsilon \in \mathbb{Q}^{>0}$, if $n \geq h(\epsilon)$ then*

$$-\epsilon^* \leq x - x_n \leq \epsilon^*.$$

Note that when a Cauchy sequence $\{x_n\}_{n\in\mathbb{N}}$ converges then it converges to a uniquely determined element of R which we call the limit *of the sequence, written $lim_{n\to\infty}x_n$.*

The field is Cauchy complete *if every Cauchy sequence converges.*

Exercise: 8.20 *Show that the pseudo-ordered field of real numbers is Cauchy complete.*

8.4 The Cauchy Reals

The traditional constructive approach to defining the real numbers is to use Cauchy sequences of rational numbers. For example the Bishop approach is to define a a real to be sequence $x = \{x_n\}_{n>0}$ of rationals x_n for integers $n > 0$ such that

$$|x_n - x_m| \leq 1/n + 1/m$$

for all $n, m > 0$. We call such a sequence a *regular sequence* and define R_c to be the class of such sequences. Of course different regular sequences can be equal as real numbers and for $x = \{x_n\}_{n>0}, y = \{y_n\}_{n>0} \in R_c$ we can define

$$x =_{R_c} y \quad \Leftrightarrow \quad |x_n - y_n| \leq 2/n \quad \text{for all } n > 0.$$

This relation on R_c is easily seen to be an equivalence relation. Classically the next step would be to form a quotient by taking equivalence classes. The Bishop style approach to constructive mathematics does not take this step as the approach prefers to work concretely with the elements of R_c while ensuring that the notions and results are worked out 'up to the equivalence relation'. In set theory it is more natural to take a quotient. Rather than using equivalence classes we can use the following association of a left cut $X_x \in \mathbb{R}$ to each $x \in R_c$. If $x = \{x_n\}_{n>0} \in R_c$ let $X_x = \{r_n \mid n > 0\}^<$, where

$$r_n = max_{1\leq m\leq n}(x_m - 1/m).$$

for each $m > 0$.

Proposition: 8.21

1. *$X_x \in \mathbb{R}$ for all $x \in R_c$.*
2. *$X_x = X'_x \quad \Leftrightarrow \quad x =_{R_c} x'$ for all $x, x' \in R_c$.*

Proof: Let $x = \{x_n\}_{n>0} \in R_c$. So for all $n, m > 0$,

$$x_m - 1/m \leq x_n + 1/n \leq r_n + 2/n$$

so that for all $n, m > 0$

$$(*) \quad r_m \leq x_n + 1/n \leq r_n + 2/n.$$

1. Trivially X_x is inhabited, as any $r < r_1$ is in X_x, and $X_x = X_x^<$. Also, by $(*)$, X_x is bounded above by $x_1 + 1$. It remains to show that if $r < s$ in $\mathbb{Q}$ then either $r \in X_x$ or $s \notin X_x$.

   So let $r < s$ in $\mathbb{Q}$. Choose an integer $n > (s-r)/2$ so that $r + 2/n < s$. Either $r < r_n$ or $r \geq r_n$. In the first case $r \in X_x$. In the second case, by $(*)$, $s > r_n + 2/n \geq r_m$ for all $m > 0$ so that $s \notin X_x$.

2. Let $x = \{x_n\}_{n>0} \in R_c$ and $x' = \{x'_n\}_{n>0} \in R_c$. Then $X_x = \{r_n \mid n > 0\}^<$ and $X_{x'} = \{r'_n \mid n > 0\}^<$, where $r_n = max_{1\leq m\leq n}(x_m - 1/m)$ and $r'_n = max_{1\leq m\leq n}(x'_m - 1/m)$ for all $n > 0$.

$\Rightarrow$ Let $X_x = X_{x'}$. So

$$(\exists n > 0)\; r < r_n \;\;\Leftrightarrow\;\; (\exists n' > 0)\; r < r'_{n'}.$$

We must show that $|x_n - x'_n| \leq 2/n$ for all $n > 0$.
Given $n > 0$, we must show that if $r = (|x_n - x'_n| - 2/n)$ then $r \leq 0$. Observe that for any $m > 0$,

$$\begin{aligned} |x_n - x'_n| &\leq |x_n - x_m| + |x_m - x'_m| + |x'_m - x'_n| \\ &\leq 1/n + 1/m + |x_m - x'_m| + 1/n + 1/m \\ &\leq 2/n + [2/m + |x_m - x'_m|] \end{aligned}$$

so that

$$(**) \qquad r \leq 2/m + |x_m - x'_m|.$$

If $r > 0$ choose an integer $m > 5/r$. By (*) for x, $x_m \leq r_m + 1/m$ so that $x_m - 2/m < r_m$ and so $x_m - 2/m < r'_{m'}$ for some $m' > 0$. By (*) for x', $r'_{m'} \leq x'_m + 1/m$. So $x_m - 2/m \leq x'_m + 1/m$ and hence $x_m - x'_m \leq 3/m$. Similarily we get that $x'_m - x_m \leq 3/m$ so that $|x_m - x'_m| \leq 3/m$. So

$$2/m + |x_m - x'_m| \leq 5/m < r$$

which contradicts $(**)$. So the assumption that $r > 0$ has been contradicted. So $r \leq 0$ as wanted.

$\Leftarrow$ Let $x =_{R_c} x'$; i.e. $|x_n - x'_n| \leq 2/n$ for all $n > 0$. To show that $X_x \subseteq X_{x'}$ let $r \in X_x$ so that $r < r_m$ for some $m > 0$. By (*) for x and x' we have, for all $n > 0$,

$$r_m \leq x_n + 1/n \leq x'_n + 3/n \leq r'_n + 4/n.$$

As $r < r_m$ we may choose $n > 0$ such that $r + 4/n < r_m$. It follows that $r + 4/n < r'_n + 4/n$, so that $r < r'_n$ and hence $r \in X_{x'}$. Thus $X_x \subseteq X_{x'}$. Similarily we get $X_{x'} \subseteq X_x$ so that $X_x = X_{x'}$.

$\square$

Exercise: 8.22 *Show that if $x \in R_c$ then there are $s = \{s_n\}_{n>o} \in R_c$ and $t = \{t_n\}_{n>0} \in R_c$ such that*

1. $s =_{R_c} t =_{R_c} x$,

2. $s_n < s_{n+1} < t_{n+1} < t_n$ *for all* $n > 0$,

3. $t_n - s_n < 1/n$ *for all* $n > 0$.

Solution: Let $x = \{x_n\}_{n>0} \in R_c$ and for $n > 0$ let

$$r_n = max_{1 \leq m \leq n}(x_m - 1/m).$$

Recall that, for all $n, m > 0$,

$$(*) \quad r_m \leq x_n + 1/n \leq r_n + 2/n.$$

Also note that $r_n \leq r_{n+1}$ for all $n > 0$. Let $s_n = r_{4n} - 1/(2n)$ for $n > 0$. We will show that

Claim:

1. $s_n < s_{n+1}$ for all $n > 0$,
2. $s \in R_c$,
3. $s =_{R_c} x$.

For 1: $s_{n+1} - s_n = (r_{4n+4} - r_{4n}) + (1/(2n) - 1/(2n+2)) > 0$ as $r_{4n+4} \geq r_{4n}$ and $1/(2n) > 1/(2n+2)$.

For 2: Given $n, m > 0$ we show that $s_m \leq s_n + 1/n + 1/m$. By (*)

$$\begin{aligned} s_m = r_{4m} - 1/(2m) &\leq r_{4n} + 2/(4n) - 1/(2m) \\ &= s_n + 1/(2n) + 2/(4n) - 1/(2m) \end{aligned}$$

so that $s_m < s_n + 1/n < s_n + 1/n + 1/m$. Interchanging m, n we get $|s_m - s_n| \leq 1/n + 1/m$ for all $n, m > 0$.

For 3: Let $n > 0$. By (*)

$$s_n = r_{4n} - 1/(2n) \leq x_n + 1/n - 1/(2n) = x_n + 1/(2n)$$

so that $s_n - x_n \leq 2/n$. Also, as $x_n - 1/n \leq r_{4n} = s_n + 1/(2n)$, we get $x_n - s_n \leq 3/(2n) < 2/n$. Thus $|s_n - x_n| \leq 2/n$ for all $n > 0$; i.e. $s =_{R_c} x$.

Now let $t_n = q_{4n} + 1/(2n)$ for all $n > 0$, where $q_n = min_{1 \leq m \leq n}(x_m + 1/m)$. Then, Interchanging $>$ and $<$ and using q_n and t_n instead of r_n and s_n we get that, if $t = \{t_n\}_{n>0}$,

1. $t_n > t_{n+1}$ for all $n > 0$,
2. $t \in R_c$,
3. $t =_{R_c} x$.

Also, as $x_m - 1/m \leq x_{m'} + 1/m'$ for all $m, m' > 0$ we get

$$r_n \leq q_n$$

for all $n > 0$, so that $s_n = r_{4n} - 1/(2n) \leq q_{4n} - 1/(2n) = t_n - 1/n$. Thus $s_n < t_n$. Finally, as $q_n \leq x_n + 1/n \leq r_n + 2/n$,

$$\begin{array}{ll} t_n = q_{4n} + 1/(2n) & \leq r_{4n} + 2/(4n) + 1/(2n) \\ & = s_n + 1/(2n) + 2/(4n) + 1/(2n) = s_n + 1/n. \end{array}$$

Thus $t_n - s_n \leq 1/n$ and the solution to the exercise is completed.

Definition: 8.23 *We define the* Cauchy Reals *to be the elements of the class*

$$\mathbb{R}_c = \{X_x \mid x \in R_c\}.$$

Which reals are in $\mathbb{R}_c$?

Proposition: 8.24 *The following are equivalent for $X \in \mathbb{R}$, where $X^R = \{r \in \mathbb{Q} \mid \exists s \in \mathbb{Q} - X \; r > s\}$.*

1. *$X \in \mathbb{R}_c$.*
2. *For some $f : \mathbb{Q} \times \mathbb{Q}^{>0} \to \{0, 1\}$, if $(r, \epsilon) \in \mathbb{Q} \times \mathbb{Q}^{>0}$ then*

   $$[f(r, \epsilon) = 0 \;\&\; r \in X] \text{ or } [f(r, \epsilon) = 1 \;\&\; r + \epsilon \notin X]$$

3. *For some $f : \mathbb{Q}^{>0} \to X$, if $\epsilon \in \mathbb{Q}^{>0}$ then $f(\epsilon) + \epsilon \notin X$.*
4. *there is a strictly increasing sequence of rationals $s_1 < s_2 < \cdots$ such that $X = \{r \in \mathbb{Q} \mid r < s_n$ for some $n > 0\}$ and a strictly decreasing sequence of rationals $t_1 > t_2 > \cdots$ such that $X^R = \{r \in \mathbb{Q} \mid r > t_n$ for some $n > 0\}$.*
5. *Both X and $X^R X$ are infinitely countable; i.e. each is in one-one correspondence with $\mathbb{N}$.*
6. *Both X and X^R are $\sigma -$ decidable; i.e. each is a countable union of decidable sets.*

Proof: leave as an exercise??? □

For sets X, Y the assertion $\mathbf{AC}(X, Y)$ is the restricted form of AC that asserts that for every $R \in \mathbf{mv}({}^X Y)$ there is $f \in {}^X Y$ such that $f \subseteq R$.

Corollary: 8.25

1. *$\mathbb{R}_c$ is a subfield of $\mathbb{R}$.*

2. *Assuming $\mathbf{AC}(\mathbb{N}, 2)$, $\mathbb{R}_c = \mathbb{R}$.*

Proof: Exercise.

We might expect that the Cauchy reals is Cauchy complete. Martin Escardo and Alex Simpson have made the, at first, surprising observation that if one takes a quotient, such as $\mathbb{R}_c$, of the class R_c of regular sequences of rationals by the equivalence relation $=_{R_c}$ the resulting field is not known to be Cauchy complete unless the Contable Axiom of Choice is assumed. This is because the natural way to find the limit of a Cauchy sequence of elements of the quotient is to extract from the Cauchy sequence a sequence of elements of R_c that represent in an obvious sense the Cauchy sequence. This may be surprising for those used to the Bishop style approach to dealing with the quotient construction, where sets come equiped with an equivalence relation and a quotient is obtained by just changing the equivalence relation without changing the objects in the set. In Bishop style constructive mathematics the Cauchy reals do indeed form a Cauchy complete field because the terms of a Cauchy sequence of Cauchy reals are already elements of R_c.

8.5 When is the Continuum a Set?

We will work informally in $\mathbf{CZF}^-$ which is $\mathbf{CZF}$ without Subset Collection. We will be interested to know under what conditions the real numbers form a set for any given notion of real number. In $\mathbf{CZF}^-$ each notion of real determines a class of reals which cannot be shown to be a set. We will consider three notions.

- The class R_c of regular sequences; i.e. Bishop style reals.
- The class $\mathbb{R}$ of constructive Dedekind reals.
- The class $\mathbb{R}_c$ of Cauchy reals in $\mathbb{R}$ with modulus function.

Theorem: 8.26 (ECST)

1. *If the class $\mathbb{N}^{\mathbb{N}}$ is a set then so is the class R_c and its quotient $\mathbb{R}_c$.*

2. If $\mathbb{N}$ has a binary refinement set then $\mathbb{R}$ is a set.

Proof:

1. Observe that if $\mathbb{N}^{\mathbb{N}}$ is a set then so is the class A of all functions $\mathbb{N}^{>0} \to \mathbb{Q}$, and so the class $R_c \subseteq A$ is a set, by Restricted Separation, as it can be defined by a resticted formula. As $\mathbb{R}_c = \{X_x \mid x \in R_c\}$, the class $\mathbb{R}_c$ is a set by Replacement.

2. Let $A = \{(r,s) \in \mathbb{Q} \times \mathbb{Q} \mid r < s\}$. Then $\mathbb{N} \sim A$ so that if $\mathbb{N}$ has a binary refinement set then so does A. So let D be a refinement set for A and let $f : A \to \mathbb{Q}$ be given by $f(r,s) = r$ for $(r,s) \in A$. Let P be the class of sets $X \subseteq \mathbb{Q}$ such that there is a set $Y \subseteq A$ such that

   (a) $X \subseteq f(A - Y)$,

   (b) $A \subseteq f^{-1}X \cup Y$.

   By Theorem 4.23 P is a set. It suffices to show that $\mathbb{R} \subseteq P$, as $\mathbb{R}$ is a class defined by a restricted formula so that we can use Restricted Separation. So let $X \in \mathbb{R}$. Then we will need that $X \subseteq \mathbb{Q}$ is both open; i.e. $r \in X \Rightarrow r < s$ for some $s \in X$, and upper-located; i.e. if $r < s$ then $r \in X$ or $s \notin X$. If $X \in \mathbb{R}$ let $Y = \{(r,s) \in A \mid s \notin X\}$.

   For (a):

   $$\begin{array}{ll} r \in X & \Rightarrow r < s \text{ for some } s \in X, \text{ as } X \text{ is open} \\ & \Rightarrow (r,s) \in A \text{ and } s \in X \text{ for some } s \\ & r = f(a) \text{ and } a \notin Y \text{ for some } a \in A \\ & \Rightarrow r \in f(A - Y) \end{array}$$

   For (b):

   $$\begin{array}{ll} (r,s) \in A & \Rightarrow r < s \\ & \Rightarrow [r \in X \text{ or } s \notin X], \text{ as } X \text{ is located} \\ & \Rightarrow f(r,s) \in X \text{ or } (r,s) \in Y \\ & (r,s) \in f^{-1}x \cup Y. \end{array}$$

□

8.6 Another notion of real

We have seen that, without using some form of the Countable Axiom of Choice it does not seem possible to prove that the field $\mathbb{R}_c$ of Cauchy reals is Cauchy complete. What we can do is prove the following somewhat limited result.

Proposition: 8.27 *Every Cauchy sequence in* $\mathbb{R}_c$ *of elements of* $\{r^* \mid r \in \mathbb{Q}\}$ *has a limit in* $\mathbb{R}_c$.

Proof: Exercise $\square$

As $\mathbb{R}$ is Cauchy complete it is natural, as suggested by Escardo and Simpson, to consider the Cauchy completion of the rationals, which can be carried out inside the Constructive Dedekind reals, the latter being itself Cauchy complete. This can be characterised, when it exists, as the smallest Cauchy complete (class) subfield $\mathbb{R}_{cc}$ of $\mathbb{R}_c$. Then $\mathbb{R}_c \subseteq \mathbb{R}_{cc} \subseteq \mathbb{R}$ and all are equal when the Axiom of Countable Choice is assumed. We have the following result.

Theorem: 8.28 (CZF$^-$) *The class* $\mathbb{R}_{cc}$ *exists and, assuming* **REA***, is a set.*

We want to define $\mathbb{R}_{cc}$ as the smallest subclass $\mathcal{X}$ of $\mathbb{R}$ closed under taking limits of Cauchy sequences. Fortunately this kind of inductive definition of a class can be carried out in **CZF$^-$** and moreover is the kind of inductive definition that defines a set in **CZF** + **REA**. Clearly we have

$$\mathbb{R}_c \subseteq \mathbb{R}_{cc} \subseteq \mathbb{R}.$$

Although we know that it is consistent to have that $\mathbb{R}_c$ is a proper subset of $\mathbb{R}$ we do not know whether $\mathbb{R}_c$ can be a proper subset of $\mathbb{R}_{cc}$ and we do not know whether $\mathbb{R}_{cc}$ can be a proper subset of $\mathbb{R}$.

9 Foundations of Set Theory

This section addresses the important set-theoretic tool of definition by transfinite recursion and studies the basic set-theoretic notion of ordinal from a constructive point of view. Moreover, it is shown that the common practice of enriching the language of set theory by function symbols for provably total class functions does not change the stock of provable theorems of the basic language.

9.1 Well-founded relations

In classical set theory, the notion of well-foundedness of a binary relation $<_A$ on a set A is expressed either by saying that there are no infinite $<_A$-descending sequences or via the least element principle, which asserts that every non-empty subset of A has a $<_A$-least element. The least element principle is far too strong a condition to be useful in intuitionistic set theory in that it implies undesirable instances of excluded middle, whereas the non-existence of infinite descending sequences is too weak a condition to guarantee the induction principle for $<_A$. Since proofs by induction and definitions by recursion are what one really wants from a notion of "well-founded" relation, the natural choice of definition is that the relation be "inductive".

Definition: 9.1 Let A be a set and $<_A$ be a binary relation on A, that is $<_A \subseteq A \times A$. An **infinite descending $<_A$-sequence** is a function $f : \mathbb{N} \to A$ such that for all $n \in \mathbb{N}$, $f(n+1) <_A f(n)$. A subset X of A is said to be **$<_A$-inductive** if

$$\forall u \in A\,[(\forall v \in A)(v <_A u \to v \in X) \;\to\; u \in X].$$

$<_A$ is **well-founded** if each $<_A$-inductive subset of A equals A.

Note that notion of well-founded relation assumes that a set and a relation on it are given, so being well-founded is actually a property of the pair $(A, <_A)$.

Lemma: 9.2 (**ECST**) *If $<_A$ is a well-founded relation on a set A, then there are no infinite descending $<_A$-sequences.*

Proof: For contradiction's sake, suppose that we have a a function $f : \mathbb{N} \to A$ such that for all $n \in \mathbb{N}$, $f(n+1) <_A f(n)$. Let $B = \{u \in A \mid u \notin f[\mathbb{N}]\}$. Clearly, $f(0) \notin B$. We show that B is $<_A$-inductive. To this end, suppose $u \in A$ and that for all $v \in A$, whenever $v <_A u$ then $v \in B$. If $u \in f[\mathbb{N}]$ then $u = f(n)$ for some n, and hence with $v_0 = f(n+1)$ we get $v_0 <_A u$, which leads to the absurdity that $f(n+1) \in B$. As a result, $u \notin f[\mathbb{N}]$, and whence $u \in B$, showing that B is $<_A$-inductive, so that $B = A$. But this collides with $f(0) \notin B$. So we have reached a contradiction. $\square$

Corollary: 9.3 (**ECST**) *If $<_A$ is a well-founded relation on a set A, then $\neg\, a <_R a$ holds for all $a \in A$.*

Proof: Immediate by Lemma 9.2. $\square$

Recall that if R is a binary relation on a set A, for $a \in A$ we denote by R_a the segment $\{u \in A \mid uRa\}$.

Lemma: 9.4 (**ECST + FPA**) *If (A, R) is a well-founded set and R^* is the transitive closure of R, then (A, R^*) is a well-founded set.*

Proof: Note that owing to Lemma 6.25, **FPA** ensures the existence of the transitive closure of R. Let X be an R^*-inductive subset of A. Put $Y = \{u \in A \mid (\forall z \in R^*_u) z \in X\}$. We shall show that Y is R-inductive. So suppose that $u \in Y$ for all uRa. Then $(\forall y \in R_a)(\forall z \in R^*_y) z \in X$; whence, because X is R^*-inductive, we also get $(\forall y \in R_a) y \in X$. This implies $(\forall y \in R^*_a) y \in X$, so that $a \in Y$. Hence Y is R-inductive.

As a result, $Y = A$. This means that for all $a \in A$, $(\forall z \in R^*_a) z \in X$, and therefore, as X is R^*-inductive, $a \in X$. Hence, $X = A$. $\square$

Lemma: 9.5 (**ECST**) *Let A, B be sets each with a binary relation $<_A$ and $<_B$, respectively, such that $<_B$ is well-founded. Let $f : A \to B$ be a map such that $f(u) <_B f(v)$ whenever $u <_A v$. Then $<_A$ is well-founded.*

Proof: Let X be an inductive subset of A, and let $Y = \{v \in B \mid f^{-1}[\{v\}] \subseteq X\}$. We shall show that Y is $<_B$-inductive, so $Y = B$ and thus $X = A$.

Suppose $v \in Y$ whenever $v <_B u$. If $x \in f^{-1}[\{u\}]$ and $y <_A x$, then $f(y) <_B u$ so $f(y) \in Y$, hence $y \in X$. Since X is inductive, this implies that $x \in X$ for each $x \in f^{-1}[\{u\}]$, so $u \in Y$. Whence Y is $<_B$-inductive. $\square$

Corollary: 9.6 (**ECST**) *If R is well-founded on a set B, then for every subset A of B, the restriction of R to A,*

$$R\restriction_A = \{\langle x, y\rangle \in R \mid x, y \in A\},$$

is well-founded on A.

Proof: This follows as the map $(x \mapsto x)$ from A to B satisfies the requirements of Lemma 9.5. $\square$

One way of constructing new well-founded sets from given ones is by adding them together as disjoint unions.

Lemma: 9.7 (**ECST**) *Let $(I, <_I)$ be a well-founded set, and $(A_i, <_{A_i})_{i \in I}$ be a family of well-founded sets. The disjoint union*

$$\sum_{i \in I} A_i \quad = \quad \{\langle i, a\rangle \mid a \in A_i \ \wedge \ i \in I\}$$

admits a relation:

$$\langle i, x\rangle \lhd \langle j, y\rangle \quad \textit{iff} \quad i <_I j \ \vee \ (i = j \ \wedge \ x <_{A_i} y).$$

$\lhd$ is a well-founded relation on $\sum_{i \in I} A_i$.

Proof: Suppose X is an $\lhd$-inductive subset of $\sum_{i \in I} A_i$. For each $i \in I$ let $A_i^* = \{u \in A_i \mid \langle i, u\rangle \in X\}$, and let $I^* = \{i \in I \mid A_i^* = A_i\}$. We claim that I^* is $<_I$-inductive, so that $I = I^*$, which yields $X = \sum_{i \in I} A_i$. Now, suppose $j \in I^*$ holds for each $j <_I i$. We shall show that $A_i^* = A_i$ by showing that A_i^* is $<_{A_i}$-inductive. Suppose $x \in A_i^*$ for each $x <_{A_i} a$. Then $w \in X$ for each $w \lhd \langle i, a\rangle$, thus $(a, i) \in X$, whence $a \in A_i^*$. Therefore $A_i^* = A_i$ as $<_{A_i}$ is well-founded, so that $i \in I$. $\square$

In **ZF** one can show that every well-founded set $(A, <_A)$ has a rank function ρ with domain A and ordinal range, such that for each $x \in A$

$$\rho(x) \quad = \quad \bigcup \{\rho(y) + 1 \mid y <_A x\}, \tag{14}$$

where $\rho(y) + 1 = \rho(y) \cup \{\rho(y)\}$.

As a rule, the existence of a rank function is not provable in **CZF**, but it is provable with the aid of a principle that asserts the existence of enough functionally regular sets, **fREA**. This result will be proved in Proposition 11.8.

Remark: 9.8 Note that the uniqueness of a function satisfying (14) is an immediate consequence of the well-foundedness of the relation.

9.2 Some consequences of Set Induction

If we have Set Induction then we can obtain, already in $\mathbf{ECST}_0$, the bounded separation scheme from the apparently weaker Infimum axiom. In point of fact, a restricted form of Set Induction suffices.

Definition: 9.9 Δ_0 or *Bounded Set Induction* is the scheme

$$\forall a\,[\forall x\in a\phi(x) \;\rightarrow\; \phi(a)] \;\rightarrow\; \forall a\phi(a)$$

for all bounded formulae $\phi(a)$.

Proposition: 9.10 ($\mathbf{ECST}_0$+Set Induction) *The Δ_0 Separation Scheme is equivalent to its single instance, the Infimum Axiom.*

Proof: It suffices to show that $\forall a\forall b\; !\;(a=b)$, as then we can apply Theorem 5.6 to get Binary Intersection and hence, by the Corollary 5.7, Δ_0 Separation. We can prove $!\;(a=b)$ by a double set induction on a,b using the equivalence

$$a=b \iff \forall x\in a\exists y\in b\;(x=y)\;\wedge\;\forall y\in b\exists x\in a\;(x=y)$$

and, using Infimum, Proposition 5.4. □

Assuming Bounded Set Induction, ω has a categorical definition via a bounded formula.

Lemma: 9.11 ($\mathbf{ECST}+\Delta_0$ Set Induction) ω *is the unique set a such that $\theta(a)$, where $\theta(a)$ is the formula*

$$\forall x\,[x\in a\leftrightarrow x=0\,\vee\,(\exists u\in a)\,x=u+1].$$

Proof: By Theorem 6.3, (1), $\theta(\omega)$. Now suppose $\theta(a)$ and $\theta(b)$ for some sets a and b. Let $\psi(x)$ be the Δ_0 formula $x\in a\rightarrow x\in b$. Suppose $\forall u\in x\,\psi(u)$. If $x\in a$, then $x=0$ or $x=v+1$ for some $v\in a$, so $\psi(v)$ as $v\in x$, thus $v\in b$, and hence $x=v+1\in v$ since $\theta(b)$. The latter shows $(\forall u\in x)\,\psi(u)\rightarrow\psi(x)$, yielding $\psi(x)$ for all x by Δ_0 Set Induction. Hence $a\subseteq b$. By the same argument one gets $b\subseteq a$, and hence $a=b$ by Extensionality. □

$\mathbf{IND}_\omega$ is a theorem of $\mathbf{CZF}$, in fact the following obtains:

Lemma: 9.12 $\mathbf{ECST}+\text{Set Induction}\vdash\mathbf{IND}_\omega$.

Proof: Assume $\phi(0) \ \wedge \ (\forall n \in \omega)[\phi(n) \rightarrow \phi(n+1)]$. Let $\theta(x)$ be the formula $x{\in}\omega \rightarrow \phi(x)$. Suppose $\forall x{\in}a\, \theta(x)$. We want to show $\theta(a)$. So assume $a{\in}\omega$. By Theorem 6.3 (1), $a = 0$ or $a = n+1$ for some $n{\in}\omega$. In the first case we get $\phi(a)$, thus $\theta(a)$. In the second case we have $n{\in}a$, thus $\theta(n)$, and hence $\phi(n)$. The latter yields $\phi(n+1)$, and so $\theta(a)$. As a result, we have shown $\forall a\, [\forall x{\in}a\, \theta(x) \ \rightarrow \ \theta(a)]$. Hence Set Induction yields $\forall a\, \theta(a)$, and consequently $\forall n{\in}\omega\, \phi(n)$. $\square$

9.3 Transfinite Recursion

A mathematically powerful tool of set theory is the possibility of defining (class) functions by $\in$-recursion or recursion on ordinals. Many interesting functions in set theory are definable by recursion.

For this subsection, the background theory will be **ECST** augmented by Set Induction.

Proposition: 9.13 (Definition by Recursion.) *If G is a total $(n+2)$–ary class function, i.e.*

$$\forall \vec{x} y z \exists! u\, G(\vec{x}, y, z) = u$$

then there is a total $(n+1)$–ary class function F such that[4]

$$\forall \vec{x} y [F(\vec{x}, y) = G(\vec{x}, y, (F(\vec{x}, z) | z \in y))].$$

Proof: Let $\Phi(f, \vec{x})$ be the formula

$[f$ is a function$] \wedge [\mathbf{dom}(f)$ is transitive$] \wedge [\forall y \in \mathbf{dom}(f)\, (f(y) = G(\vec{x}, y, f \restriction y))]$.

Set

$$\psi(\vec{x}, y, f) = [\Phi(f, \vec{x}) \wedge y \in \mathbf{dom}(f)].$$

Claim $\quad \forall \vec{x}, y \exists! f \psi(\vec{x}, y, f)$.

Proof of Claim: By $\in$ induction on y. Suppose $\forall u \in y\, \exists! g\, \psi(\vec{x}, u, g)$. By Replacement we find a set A such that $\forall u \in y\, \exists g \in A\, \psi(\vec{x}, u, g)$ and $\forall g \in A \exists u \in y\, \psi(\vec{x}, u, g)$. Let $f_0 = \bigcup\{g : g \in A\}$. By our general assumption there exists a u_0 such that $G(\vec{x}, y, (f_0(u) | u \in y)) = u_0$. Set $f = f_0 \cup \{\langle y, u_0 \rangle\}$. Since for all $g \in A$, $\mathrm{dom}(g)$ is transitive we have that $\mathrm{dom}(f_0)$ is transitive. If $u \in y$, then $u \in \mathbf{dom}(f_0)$. Thus $\mathbf{dom}(f)$ is transitive and $y \in \mathbf{dom}(f)$. We have to show that f is a function. But it is readily shown that if $g_0, g_1 \in A$, then $\forall x \in \mathbf{dom}(g_0) \cap \mathbf{dom}(g_1)[g_0(x) = g_1(x)]$. Therefore f is a function. This

[4] $(F(\vec{x}, z) | z \in y) \ := \ \{\langle z, F(\vec{x}, z) \rangle : z \in y\}$

also shows that $\forall w \in \mathbf{dom}(f)[f(w) = G(\vec{x}, w, f \restriction w)]$, confirming the claim (using Set Induction).

Now define F by

$$F(\vec{x}, y) = w \;\; := \;\; \exists f[\psi(\vec{x}, y, f) \wedge f(y) = w].$$

$\square$

Corollary: 9.14 *There is a class function* **TC** *such that*

$$\forall a[\mathbf{TC}(a) = a \cup \bigcup\{\mathbf{TC}(x) : x \in a\}].$$

Proposition: 9.15 (Definition by **TC**–Recursion) *Under the assumptions of Proposition 9.13 there is an* $(n+1)$*–ary class function* F *such that*

$$\forall \vec{x} y[F(\vec{x}, y) = G(\vec{x}, y, (F(\vec{x}, z) | z \in \mathbf{TC}(y)))].$$

Proof: Let $\theta(f, \vec{x}, y)$ be the formula

$[f \text{ is a function}] \wedge [\mathbf{dom}(f) = \mathbf{TC}(y)] \wedge [\forall u \in \mathbf{dom}(f)[f(u) = G(\vec{x}, u, f \restriction \mathbf{TC}(u))]]$.

Prove by $\in$–induction that $\forall y \exists! f\, \theta(f, \vec{x}, y)$. Suppose $\forall v \in y\, \exists! g\, \theta(g, \vec{x}, v)$. We then have

$$\forall v \in y \exists! a \exists g[\theta(g, \vec{x}, v) \wedge G(\vec{x}, v, g) = a].$$

By Replacement or rather Lemma 3.2, there is a function h such that $\mathbf{dom}(h) = y$ and

$$\forall v \in y\, \exists g\, [\theta(g, \vec{x}, v) \wedge G(\vec{x}, v, g) = h(v)]\,.$$

Applying Replacement to $\forall v \in y\, \exists! g\; \theta(g, \vec{x}, v)$ also provides us with a set A such that $\forall v \in y\, \exists g \in A\; \theta(g, \vec{x}, v)$ and $\forall g \in A\, \exists v \in y\; \theta(g, \vec{x}, v)$. Now let $f = (\bigcup\{g : g \in A\}) \cup h$. Then $\theta(f, \vec{x}, y)$. $\square$

9.4 Ordinals

The notion of ordinal is central to classical set theory. In intuitionistic set theory, however, we cannot preserve such familiar features as the linear ordering of ordinals. So one might ask what ordinals are good for in **CZF**? Perhaps the main justification is that they supply us with a ranking of the universe and that we can still define many of the familiar set-theoretic operations by transfinite recursion on ordinals. This works as long as we make sure that definitions by transfinite recursion do not make case distinctions such as in the classical ordinal cases of successor and limit.

Definition: 9.16 An *ordinal* α is a transitive set of transitive sets, i.e., α and every element of α are transitive.

Note that this notion is Δ_0. Observe also that an element of an ordinal is an ordinal as well.

Variables $\alpha, \beta, \gamma, \delta, \ldots$ will be assumed to range over ordinals. **ON** denotes the class of ordinals.

Lemma: 9.17 *For a set x, let $x+1 := x \cup \{x\}$.*

1. $\alpha + 1 \in \mathbf{ON}$.
2. *If X is a set of ordinals, then $\bigcup X \in \mathbf{ON}$.*

Proof: (1) is obvious. For (2), suppose $z \in y \in \bigcup X$. Then $y \in \alpha$ for some $\alpha \in X$. Thus $z \in \alpha$ and so $z \in \bigcup X$. The latter shows that $\bigcup X$ is transitive. Since for every $y \in \bigcup X$ there is an ordinal $\alpha \in X$ such that $y \in \alpha$, y is an ordinal, too, and hence transitive. $\square$

As in the classical scenario, functions can be defined by transfinite recursion on ordinals.

Proposition: 9.18 (**ECST** + Set Induction) (Definition by Recursion on ordinals.) *If G is a total $(n+2)$–ary class function on $V^n \times \mathbf{ON} \times V$, i.e.*

$$\forall \vec{x} \alpha z \exists! u \, G(\vec{x}, \alpha, z) = u$$

then there is a $(n+1)$–ary class function $F : V^n \times \mathbf{ON} \to V$ such that

$$\forall \vec{x} \alpha [F(\vec{x}, \alpha) = G(\vec{x}, \alpha, (F(\vec{x}, \beta) | \beta \in \alpha))].$$

Proof: The proof is essentially the same as for Proposition 9.13 by letting $\Phi(f, \vec{x})$ be the formula

$$[f \text{ is a function}] \wedge [\mathbf{dom}(f) \in \mathbf{ON}] \wedge [\forall \beta \in \mathbf{dom}(f) \, (f(\beta) = G(\vec{x}, \beta, f \restriction \beta))].$$

$\square$

Definition: 9.19 (**ECST** + Set Induction) For any set x we define

$$\mathrm{rank}(x) \;\; := \;\; \bigcup \{\mathrm{rank}(y) + 1 : \; y \in x\}.$$

This definition is justified by Proposition 9.13.

Proposition: 9.20 (**ECST** + Set Induction)

1. $\forall x \; rank(x) \in \mathbf{ON}$.
2. $\forall \alpha \; rank(\alpha) = \alpha$.

Proof: (1): We use Set Induction on x. Suppose $\forall y{\in}x$ rank$(y) \in \mathbf{ON}$. Then rank$(y)+1 \in \mathbf{ON}$ for all $y{\in}x$ by Lemma 9.17 (1), and hence $\bigcup\{\text{rank}(y)+1 : y{\in}x\} \in \mathbf{ON}$ by Lemma 9.17 (2). Thus rank$(x) \in \mathbf{ON}$.

(2): Here we use induction on α. Suppose $\forall \beta{\in}\alpha$ rank$(\beta) = \beta$. Then, if $\beta{\in}\alpha$ we have $\beta \in$ rank(α) as $\beta{\in}\beta+1$. Hence $\alpha \subseteq$ rank(α). Now suppose $\beta \in$ rank(α). Then $\beta \in \gamma+1$ for some $\gamma{\in}\alpha$. As a result, $\beta{\in}\gamma$ or $\beta = \gamma$. But then $\beta{\in}\alpha$. Thus rank$(\alpha) \subseteq \alpha$ as well. □

Remark: 9.21 It has already been mentioned that due to the underlying logic systems like **IZF** can not prove that ordinals are linearly ordered by $\in$. One might be tempted to remedy this defect by considering a stricter notion of ordinal. Let's call an ordinal α *trichotomous* if

$$\forall \beta{\in}\alpha \, \forall \gamma{\in}\alpha \, (\beta{\in}\gamma \, \vee \, \beta = \gamma \, \vee \, \gamma{\in}\beta).$$

The "problem" with trichotomous ordinals is that even systems like **IZF** cannot prove the existence of enough trichotomous ordinals. Lemma 9.17, (2) fails for trichotomous ordinals and so does Lemma 9.20, (1). Indeed, it is consistent with **IZF** to assume that the trichotomous ordinals merely constitute a set.

9.5 Extension by Function Symbols

In classical set theory it is common practice to enrich the language of set theory by function symbols for provably total class functions. In the case of **ZF** this amounts to conservative extensions. In theories like **CZF**, however, separation is restricted. Adding function symbols to the language changes the stock of Δ_0 formulas. Hence in connection with **CZF** the question arises whether adding function symbols for provably total class functions could change the stock of provable theorems of the basic language.

Definition: 9.22 Let T be a theory whose language comprises the language of set theory and let $\phi(x_1, \ldots, x_n, y)$ be a formula such that

$$T \vdash \forall x_1 \ldots \forall x_n \, \exists! y \, \phi(x_1, \ldots, x_n, y).$$

Let $\mathtt{f}$ be a new n-ary function symbol and define $\mathtt{f}$ by:

$$\forall x_1 \ldots \forall x_n \, \forall y \, [\mathtt{f}(x_1, \ldots, x_n) = y \leftrightarrow \phi(x_1, \ldots, x_n, y)].$$

$\mathtt{f}$ will be called a *function symbol* of T.

It is an important property of classical set theory that function symbols can be treated as though they were atomic symbols of the basic language. The usual proofs of this fact employ full Separation. As this principle is not available in **ECST** and **CZF** some care has to be exercised in obtaining the same results for these theories.

Proposition: 9.23 (Extension by Function Symbols) *Let T be one of the theories* **ECST**, **ECST**+Set Induction, *or* **CZF**. *Suppose $T \vdash \forall \vec{x} \, \exists! y \Phi(\vec{x}, y)$. Let T_Φ be obtained by adjoining a function symbol F_Φ to the language, extending the schemata to the enriched language, and adding the axiom $\forall \vec{x} \Phi(\vec{x}, F_\Phi(\vec{x}\,))$. Then T_Φ is conservative over T.*

Proof: We define the following translation * for formulas of T_Φ:

$$\begin{aligned} \phi^* \quad &\equiv \quad \phi \text{ if } F_\Phi \text{ does not occur in } \phi; \\ (F_\Phi(\vec{x}\,) = y)^* \quad &\equiv \quad \Phi(\vec{x}, y). \end{aligned}$$

If ϕ is of the form $t = x$ with $t \equiv G(t_1, \ldots, t_k)$ such that one of the terms $t_1, \ldots, t_k$ is not a variable, then let

$$(t = x)^* \;\equiv\; \exists x_1 \ldots \exists x_k \, [(t_1 = x_1)^* \wedge \cdots \wedge (t_k = x_k)^* \wedge (G(x_1, \ldots, x_k) = x)^*] \,.$$

The latter provides a definition of $(t = x)^*$ by induction on t. If either t or s contains F_Φ, then let

$$\begin{aligned} (t \in s)^* \quad &\equiv \quad \exists x \exists y [(t = x)^* \wedge (s = y)^* \wedge x \in y], \\ (t = s)^* \quad &\equiv \quad \exists x \exists y [(t = x)^* \wedge (s = y)^* \wedge x = y], \\ (\neg \phi)^* \quad &\equiv \quad \neg \phi^* \\ (\phi_0 \Box \phi_1)^* \quad &\equiv \quad \phi_0^* \Box \phi_1^*, \quad \text{if } \Box \text{ is } \wedge, \vee, \text{ or } \rightarrow \\ (\exists x \phi)^* \quad &\equiv \quad \exists x \phi^* \\ (\forall x \phi)^* \quad &\equiv \quad \forall \phi^*. \end{aligned}$$

Let T_Φ^- be the restriction of T_Φ, where F_Φ is not allowed to occur in the Δ_0 Separation Scheme. Then it is obvious that $T_\Phi^- \vdash \phi$ implies $T \vdash \phi^*$. So it remains to show that T_Φ^- proves the same theorems as T_Φ. We first prove $T_\Phi^- \vdash \exists x \forall y \, [y \in x \leftrightarrow y \in a \wedge \phi(a)]$ for any Δ_0 formula ϕ of T_Φ.

We proceed by induction on ϕ.

1. $\phi(y) \equiv t(y) \in s(y)$. Now
$$T_\Phi \vdash \forall y \in a \exists! z[(z = t(y)) \wedge \forall y \in a \exists! u(u = s(y))].$$
Using Replacement (lemma 3.2) we find functions f and g such that
$$\mathbf{dom}(f) = \mathbf{dom}(g) = a \text{ and } \forall y \in a\,[f(y) = t(y) \wedge g(y) = s(y)]\,.$$
Therefore $\{y \in a : \phi(y)\} = \{y \in a : f(y) \in g(y)\}$ exists by Δ_0 Separation in T_Φ^-.

2. $\phi(y) \equiv t(y) = s(y)$. Similar.

3. $\phi(y) \equiv \phi_0(y) \Box \phi_1(y)$, where $\Box$ is any of $\wedge, \vee, \rightarrow$. This is immediate by induction hypothesis.

4. $\phi(y) \equiv \forall u \in t(y)\ \phi_0(u, y)$. We find a function f such that $\mathbf{dom}(f) = a$ and $\forall y \in a\, f(y) = t(y)$. Inductively, for all $b \in a$, $\{u \in \bigcup \mathbf{ran}(f) : \phi_0(u, b)\}$ is a set. Hence there is a function g with $\mathbf{dom}(g) = a$ and $\forall b \in a\, g(b) = \{u \in \bigcup \mathbf{ran}(f) : \phi_0(u, b)\}$. Then $\{y \in a : \phi(y)\} = \{y \in a : \forall u \in f(y)(u \in g(y))\}$.

5. $\phi(y) \equiv \exists u \in t(y)\, \phi_0(u, y)$. With f and g as above, $\{y \in a : \phi(y)\} = \{y \in a : \exists u \in f(y)(u \in g(y))\}$.

$\Box$

Remark: 9.24 The proof of Proposition 9.23 shows that the process of adding function symbols, starting with such theories as **ECST**, **ECST** + Set Induction, or **CZF**, can be iterated. So if e.g. $T_\Phi \vdash \forall \vec{x} \exists y\, \psi(\vec{x}, y)$, then
$$T_\Phi + \{\forall \vec{x} \exists y\, \psi(\vec{x}, F_\psi(\vec{x}))\}$$
will be conservative over T as well.

Problems

- (**ECST** + Set Induction) We define a relation $\lhd$ on ordered pairs by
$$\begin{aligned}\langle c, d\rangle \lhd \langle a, b\rangle \quad \text{iff} \quad & (c = a \wedge d \in \mathbf{TC}(b)) \vee (d = b \wedge c \in \mathbf{TC}(a)) \\ & \vee (c \in \mathbf{TC}(a) \wedge d \in \mathbf{TC}(b)).\end{aligned}$$
Prove $\lhd$-induction, i.e., whenever
$$\forall a, b\, [\forall x, y\, [\langle x, y\rangle \lhd \langle a, b\rangle \rightarrow \varphi(x, y)] \rightarrow \varphi(a, b)]$$
then $\forall a, b\, \varphi(a, b)$.

- (**ECST**+Set Induction) *(Definition by* $\lhd$*-Recursion.)*: If G is a total $(n+3)$–ary class function, i.e.

$$\forall \vec{x} uvz \exists! u \, G(\vec{x}, u, v, z) = u$$

then there is a total $(n+2)$–ary class function F such that for all $\vec{x}, a, b$,

$$F(\vec{x}, a, b) \quad = \quad G(\vec{x}, a, b, \{\langle u, v, F(\vec{x}, u, v)\rangle \mid \langle u, v\rangle \lhd \langle a, b\rangle\}).$$

- Show that there is class function $\# : \mathbf{ON}^2 \to \mathbf{ON}$ such that

$$\alpha \# \beta \quad = \quad \{\delta \# \eta \mid \delta \in \alpha \wedge \eta \in \beta\}.$$

- Show that we cannot prove in **CZF** that for all ordinal α, $0 \in \alpha + 1$. Where does the induction break down? (Hint: Show that $\mathbf{CZF} \vdash \forall \alpha \, (0 \in \alpha + 1) \to LEM$, where LEM stands for the law of excluded middle.)

- Similarly as in classical set theory, but using case-less definitions, we define the operations of addition, multiplication and exponentiation on ordinals:

$$\begin{aligned} \alpha + \beta &= \alpha \cup \{\alpha + \delta \mid \delta \in \beta\} \\ \alpha \cdot \beta &= \{\alpha \cdot \delta + \gamma \mid \gamma \in \alpha, \ \delta \in \beta\} \\ \alpha^{\beta} &= 1 \cup \{\alpha^{\delta} \cdot \gamma + \eta \mid \gamma \in \alpha, \ \delta \in \beta, \ \eta \in \alpha^{\delta}\}. \end{aligned}$$

Try to show the following (writing $<$ for $\in$):

1. $\beta < \gamma \to \alpha + \beta < \alpha + \gamma$.
2. $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$.
3. $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$.
4. $\alpha \cdot (\beta + \gamma) = (\alpha \cdot \beta) + (\alpha \cdot \gamma)$.
5. $\alpha^{\beta + \gamma} = \alpha^{\beta} \cdot \alpha^{\gamma}$.
6. $(\alpha^{\beta})^{\gamma} = \alpha^{\beta \cdot \gamma}$.

10 Choice Principles

The axiom of choice does not have an unambiguous status in constructive mathematics. On the one hand it is said to be an immediate consequence of the constructive interpretation of the quantifiers. Any proof of $\forall x \in a\, \exists y \in b\, \phi(x, y)$ must yield a function $f : a \to b$ such that $\forall x \in a\, \phi(x, f(x))$. This is certainly the case in Martin-Löf's intuitionistic theory of types. On the other hand, from the very earliest days, the axiom of choice has been criticised as an excessively non-constructive principle even for classical set theory. Moreover, it has been observed that the full axiom of choice cannot be added to systems of constructive set theory without yielding constructively unacceptable cases of excluded middle (see [17] and Proposition 10.3). Therefore one is naturally led to the question: *Which choice principles are acceptable in constructive set theory?* As constructive set theory has a canonical interpretation in Martin-Löf's intuitionistic theory of types this interpretation lends itself to being a criterion for constructiveness. We will consider set-theoretic choice principles as constructively justified if they can be shown to hold in the interpretation in type theory. Moreover, looking at constructive set theory from a type-theoretic point of view has turned out to be valuable heuristic tool for finding new constructive choice principles.

In this section we will study differing choice principles and their deductive relationships. To set the stage we present Diaconescu's result that the full axiom of choice implies certain forms of excluded middle.

10.1 Diaconescu's result

Restricted Excluded Middle, REM, is the schema $\phi \vee \neg\phi$ where ϕ is a restricted formula.

Recall that $\mathcal{P}(x) := \{u : u \subseteq x\}$, and *Powerset* is the axiom $\forall x \exists y\; y = \mathcal{P}(x)$.

Proposition: 10.1 *(i)* $\mathbf{ECST} + \textit{Exponentiation} + \mathbf{REM} \vdash$ Powerset.

(ii) The strength of $\mathbf{ECST}$+*Exponentiation*+$\mathbf{REM}$ *exceeds that of classical type theory with extensionality.*

Proof: (i): Set $\mathbf{0} := \emptyset$, $\mathbf{1} := \{\mathbf{0}\}$, and $\mathbf{2} := \{\mathbf{0}, \{\mathbf{0}\}\}$.

Suppose $u \subseteq \mathbf{1}$. On account of **REM** we have $\mathbf{0} \in u \vee \mathbf{0} \notin u$. Thus $u = \mathbf{1} \vee u = \mathbf{0}$; and hence $u \in \mathbf{2}$. This shows that $\mathcal{P}(\mathbf{1}) \subseteq \mathbf{2}$. As a result, $\mathcal{P}(\mathbf{1}) = \{u \in \mathbf{2} : u \subseteq \mathbf{1}\}$, and thus $\mathcal{P}(\mathbf{1})$ is a set by Restricted Separation.

Now let x be an arbitrary set, and put $b := {}^{x}(\mathcal{P}(\mathbf{1}))$. Exponentiation ensures that b is a set. For $v \subseteq x$ define $f_v \in b$ by

$$f_v(z) \;:=\; \{y \in \mathbf{1} :\; z \in v\},$$

and put

$$c \;:=\; \{\{z \in x :\; g(z) = \mathbf{1}\} :\; g \in b\}.$$

c is a set by Replacement. Observe that $\forall w \in c\,(w \subseteq x)$. For $v \subseteq x$ it holds $v = \{z \in x :\; f_v(z) = \mathbf{1}\}$, and therefore $v \in c$. Consequently, $\mathcal{P}(x) = \{v \in c : v \subseteq x\} = c$, thus $\mathcal{P}(x)$ is a set.

(ii): By means of ω many iterations of Powerset (starting with ω) we can build a model of intuitionistic type theory within $\mathbf{ECST}$ + Exponentiation + $\mathbf{REM}$. The Gödel-Gentzen negative translation can be extended so as to provide an interpretation of classical type theory with extensionality in intuitionistic type theory (cf. [52]).

In particular, $\mathbf{ECST}$ + Exponentiation + $\mathbf{REM}$ is stronger than classical second order arithmetic (with full Comprehension). □

Remark: 10.2 In actuality, it can be shown that $\mathbf{ECST} + \mathbf{EXP} + \mathbf{REM}$ is stronger than classical Zermelo Set Theory (see [64]).

The **Axiom of Choice**, **AC**, asserts that for all sets A and functions F with domain A such that $\forall i \in A\, \exists y \in F(i)$ there exists a function f with domain A such that $\forall i \in A\, f(i) \in F(i)$.

Proposition: 10.3 *(i)* $\mathbf{ECST} + \mathbf{EXP}$ + Full Separation + $\mathbf{AC} = \mathbf{ZFC}$.

(ii) $\mathbf{ECST} + \mathbf{AC} \vdash \mathbf{REM}$.

(iii) $\mathbf{ECST} + \mathbf{EXP} + \mathbf{AC} \vdash$ Powerset.

(iv) *The strength of* $\mathbf{ECST}+\mathbf{EXP}+\mathbf{AC}$ *exceeds that of classical type theory with extensionality.*

Proof: (i): Let ϕ be an arbitrary formula. Put

$$\begin{aligned} X &= \{n \in \omega :\; n = \mathbf{0} \,\vee\, [n = \mathbf{1} \wedge \phi]\}, \\ Y &= \{n \in \omega :\; n = \mathbf{1} \,\vee\, [n = \mathbf{0} \wedge \phi]\}. \end{aligned}$$

X and Y are sets by full Separation. We have

$$\forall z \in \{X, Y\}\, \exists k \in \omega\, (k \in z).$$

Using **AC**, there is a choice function f defined on $\{X, Y\}$ such that

$$\forall z \in \{X, Y\} \, [f(z) \in \omega \ \wedge \ f(z) \in z],$$

in particular, $f(X) \in X$ and $f(Y) \in Y$. Next, we are going to exploit the important fact

$$\forall n, m \in \omega \, (n = m \vee n \neq m). \tag{15}$$

As $\forall z \in \{X, Y\} \, [f(z) \in \omega]$, we obtain

$$f(X) = f(Y) \ \vee \ f(X) \neq f(Y)$$

by (15). If $f(X) = f(Y)$, then ϕ by definition of X and Y. So assume $f(X) \neq f(Y)$. As ϕ implies $X = Y$ (this requires Extensionality) and thus $f(X) = f(Y)$, we must have $\neg\phi$. Consequently, $\phi \vee \neg\phi$. Thus (i) follows from the fact that $\mathbf{ECST} + \mathbf{EXP} + \mathbf{EM} = \mathbf{ZF}$.

(ii): If ϕ is restricted, then X and Y are sets by Restricted Separation. The rest of the proof of (i) then goes through unchanged.

(iii) follows from (ii) and Proposition 10.1,(i).

(iv) follows from (ii) and Proposition 10.1,(ii). □

10.2 Constructive Choice Principles

The weakest constructive choice principle we consider is the **Axiom of Countable Choice**, $\mathbf{AC}_\omega$, i.e. whenever F is a function with with domain ω such that $\forall i \in \omega \, \exists y \in F(i)$, then there exists a function f with domain ω such that $\forall i \in \omega \, f(i) \in F(i)$.

A mathematically very useful axiom to have in set theory is the **Dependent Choices Axiom**, **DC**, i.e., for all sets a and (set) relations $R \subseteq a \times a$, whenever

$$(\forall x \in a) \, (\exists y \in a) \, xRy$$

and $b_0 \in a$, then there exists a function $f : \omega \to a$ such that $f(0) = b_0$ and

$$(\forall n \in \omega) \, f(n)Rf(n+1).$$

Even more useful in constructive set theory is the *Relativized Dependent Choices Axiom*, **RDC**.[5] It asserts that for arbitrary formulae ϕ and ψ, whenever

$$\forall x[\phi(x) \ \rightarrow \ \exists y(\phi(y) \ \wedge \ \psi(x, y))]$$

[5] In Aczel [2], **RDC** is called the dependent choices axiom and **DC** is dubbed the axiom of limited dependent choices. We deviate from the notation in [2] as it deviates from the usage in classical set theory texts.

and $\phi(b_0)$, then there exists a function f with domain ω such that $f(0) = b_0$ and

$$(\forall n \in \omega)[\phi(f(n)) \ \wedge \ \psi(f(n), f(n+1))].$$

A restricted form of **RDC** where ϕ and ψ are required to be Δ_0 will be called Δ_0-**RDC**.

The *Bounded Relativized Dependent Choices Axiom*, **bRDC**, is the following schema: For all Δ_0-formulae θ and ψ, whenever

$$(\forall x \in a)[\theta(x) \ \rightarrow \ (\exists y \in a)(\theta(y) \ \wedge \ \psi(x, y)]$$

and $b_0 \in a \wedge \phi(b_0)$, then there exists a function $f : \omega \rightarrow a$ such that $f(0) = b_0$ and

$$(\forall n \in \omega)[\theta(f(n)) \ \wedge \ \psi(f(n), f(n+1))].$$

Letting $\phi(x)$ stand for $x{\in}a \wedge \theta(x)$, one sees that **bRDC** is a consequence of Δ_0-**RDC**.

Here are some immediate consequences f **DC**.

Lemma: 10.4 *(i)* (**ECST** + **DC**) *If* ψ *is* Δ_0 *and* $(\forall x \in a)\,(\exists y \in a)\,\psi(x, y)$ *and* $b_0 \in a$*, then there exists a function* $f : \omega \rightarrow a$ *such that* $f(0) = b_0$ *and* $(\forall n \in \omega)\,\psi(f(n), f(n+1))$*.*

(ii) (**ECST**+**DC**) *If* ϕ *is an arbitrary formula and* $(\forall x \in a)\,(\exists! y \in a)\,\phi(x, y)$ *and* $b_0 \in a$*, then there exists a function* $f : \omega \rightarrow a$ *such that* $f(0) = b_0$ *and* $(\forall n \in \omega)\,\phi(f(n), f(n+1))$*.*

(iii) (**ECST** + Strong Collection + **DC**) *If* θ *is an arbitrary formula and* $(\forall x \in a)\,(\exists y \in a)\,\theta(x, y)$ *and* $b_0 \in a$*, then there exists a function* $f : \omega \rightarrow a$ *such that* $f(0) = b_0$ *and* $(\forall n \in \omega)\,\theta(f(n), f(n+1))$*.*

Proof: (i): Put $R = \{\langle x, y\rangle \in a \times a \mid \psi(x, y)\}$.

(ii): $(\forall x \in a)\,(\exists! y \in a)\,\phi(x, y)$ implies that there exists a function $f : a \rightarrow a$ such that $\forall x \in a\ \psi(x, f(x))$. Now let $R = f$.

(iii): Assume $(\forall x{\in}a)\,(\exists y{\in}a)\,\theta(x, y)$ and $b_0{\in}a$. Then

$$(\forall x{\in}a)\,(\exists z)\,[(\exists y{\in}a)\,(z = \langle x, y\rangle \ \wedge \ \theta(x, y))].$$

Using Strong Collection there exists a set S such that

$$\begin{gathered}(\forall x{\in}a)\,(\exists z{\in}S)\,(\exists y{\in}a)\,[z = \langle x, y\rangle \ \wedge \ \theta(x, y)] \\ (\forall z{\in}S)\,(\exists x'{\in}a)\,(\exists y'{\in}a)\,[z = \langle x', y'\rangle \ \wedge \ \theta(x', y')].\end{gathered} \tag{16}$$

In particular we have $(\forall x{\in}a)\,(\exists y{\in}a)\,\langle x,y\rangle \in S$. Employing **DC** there exists a function $f:\omega\to a$ such that $f(0)=b_0$ and $(\forall n{\in}\omega)\,f(n)\,S\,f(n+1)$. By (16) we get $(\forall n{\in}\omega)\,\theta(f(n),f(n+1))$. $\square$

Instead of using Strong Collection in Lemma 10.4 (iii) one can also use Collection in combination with **RDC**. This will be proved in Lemma 10.8 once we have shown that **RDC** implies induction on $\mathbb{N}$.

Proposition: 10.5 (**ECST**)

(i) **DC** *implies* $\mathbf{AC}_\omega$.

(ii) **bRDC** *and* **DC** *are equivalent.*

(iii) **RDC** *implies* **DC**.

Proof: (i): If z is an ordered pair $\langle x,y\rangle$ let $1^{st}(z)$ denote x and $2^{nd}(z)$ denote y.

Suppose F is a function with domain ω such that $\forall i\in\omega\,\exists x\in F(i)$. Let $A=\{\langle i,u\rangle|\ i\in\omega\ \wedge\ u\in F(i)\}$. A is a set by Union, Cartesian Product and restricted Separation. We then have

$$\forall x\in A\,\exists y\in A\ xRy,$$

where $R=\{\langle x,y\rangle\in A\times A\mid 1^{st}(y)=1^{st}(x)+1\}$. Pick $x_0\in F(0)$ and let $a_0=\langle 0,x_0\rangle$. Using **DC** there exists a function $g:\omega\to A$ satisfying $g(0)=a_0$ and

$$\forall i\in\omega\,[g(i)\in A\ \wedge\ 1^{st}(g(i+1))=1^{st}(g(i))+1].$$

Letting f be defined on ω by $f(i)=2^{nd}(g(i))$ one gets $\forall i\in\omega\ f(i)\in F(i)$.

(ii) We argue in **ECST** + **DC** to show **bRDC**. Assume

$$\forall x\in a[\phi(x)\ \to\ \exists y\in a(\phi(y)\ \wedge\ \psi(x,y))]$$

and $\phi(b_0)$, where ϕ and ψ are Δ_0. Let $\theta(x,y)$ be the formula $\phi(x)\ \wedge\ \phi(y)\ \wedge\ \psi(x,y)$ and $A=\{x\in a|\ \phi(x)\}$. Then θ is Δ_0 and A is a set by Δ_0 Separation. From the assumptions we get $\forall x\in A\,\exists y\in A\,\theta(x,y)$ and $b_0\in A$. Thus, by Lemma 10.4(i), there is a function f with domain ω such that $f(0)=b_0$ and $\forall n\in\omega\,\theta(f(n),f(n+1))$. Hence we get $\forall n\in\omega\,[\phi(n)\ \wedge\ \psi(f(n),f(n+1))]$.

The other direction is obvious.

(iii) is obvious. $\square$

RDC and induction on $\mathbb{N}$

It is worth noting that **RDC** and Δ_0-**RDC** entail induction principles on ω.

Lemma: 10.6 $\mathbf{ECST} + \Delta_0\text{-}\mathbf{RDC} \vdash \Sigma_1\text{-}\mathbf{IND}_\omega$.

Proof: Suppose $\theta(0) \wedge (\forall n{\in}\omega)(\theta(n) \rightarrow \theta(n+1))$, where $\theta(n)$ is of the form $\exists x\phi(n,x)$ with ϕ Δ_0. We wish to prove $(\forall n{\in}\omega)\theta(n)$.

If z is an ordered pair $\langle x, y\rangle$ let $1^{st}(z)$ denote x and $2^{nd}(z)$ denote y. Since $\theta(0)$ there exists a set x_0 such that $\phi(0, x_0)$. Put $a_0 = \langle 0, x_0\rangle$.

From $(\forall n{\in}\omega)(\theta(n) \rightarrow \theta(n+1))$ we can conclude

$$(\forall n{\in}\omega)\forall y\,[\phi(n,y) \rightarrow \exists w\,\phi(n+1,w)\,]$$

and thus

$$\forall z\,[\,\psi(z) \rightarrow \exists v\,(\,\psi(v)\ \wedge\ \chi(z,v)\,)],$$

where $\psi(z)$ stands for z *is an ordered pair* $\wedge\ 1^{st}(z) \in \omega\ \wedge\ \phi(1^{st}(z), 2^{nd}(z))$ and $\chi(z,v)$ stands for $1^{st}(v) = 1^{st}(z) + 1$. Note that ψ and χ are Δ_0. We also have $\psi(a_0)$. Thus by Δ_0-**RDC** there exists a function $f : \omega \rightarrow V$ such that $f(0) = a_0$ and

$$(\forall n{\in}\omega)\,[\,\psi(f(n))\ \wedge\ \chi(f(n), f(n+1))\,].$$

From $\chi(f(n), f(n{+}1))$, using induction on ω, one easily deduces that $1^{st}(f(n)) = n$ for all $n{\in}\omega$. Hence from $(\forall n{\in}\omega)\,\psi(f(n))$ we get $(\forall n{\in}\omega)\,\exists x\,\phi(n,x)$ and so $(\forall n{\in}\omega)\,\theta(n)$. □

Lemma: 10.7 $\mathbf{ECST} + \mathbf{RDC} \vdash \mathbf{IND}_\omega$.

Proof: Suppose $\theta(0)\ \wedge\ (\forall n{\in}\omega)(\theta(n)\ \rightarrow\ \theta(n+1))$. We wish to prove $(\forall n{\in}\omega)\theta(n)$. Let $\phi(x)$ and $\psi(x,y)$ be the formulas $x{\in}\omega \wedge \theta(x)$ and $y = x{+}1$, respectively. Then $\forall x\,[\phi(x)\ \rightarrow\ \exists y\,(\phi(y) \wedge \psi(x,y))]$ and $\phi(0)$. Hence, by **RDC**, there exists a function f with domain ω such that $f(0) = 0$ and $\forall n{\in}\omega\,[\phi(f(n))\ \wedge\ \psi(f(n), f(n+1))]$. Let $a = \{n{\in}\omega\ :\ f(n) = n\}$. Using induction on ω one easily verifies that $\omega \subseteq a$, and hence $f(n) = n$ for all $n{\in}\omega$. Hence, $\phi(n)$ for all $n{\in}\omega$, and thus $(\forall n{\in}\omega)\theta(n)$. □

With the help of the previous result, we can now show that **RDC** plus Collection implies a strong closure principle.

Proposition: 10.8 (**ECST** + **RDC** + Collection)

Suppose that $\forall x \exists y \phi(x, y)$. Then for every set d there exists a transitive set A such that $d \in A$ and

$$\forall x \in A\, \exists y \in A\, \phi(x, y).$$

Moreover, for every set d there exists a transitive set A and a function f : $\omega \to A$ such that $f(0) = d$ and $\forall n \in \omega\, \phi(f(n), f(n+1))$.

Proof: The assumption yields that $\forall x \in b\, \exists y \phi(x, y)$ holds for every set b. Since **RDC** implies the existence of the transitive closure of any set by Lemma 10.7 and Lemma 6.27, using Collection we get

$$\forall b\, \exists c\, [\theta(b, c) \wedge Tran(c)],$$

where $\theta(b, c)$ is the formula $\forall x \in b\, \exists y \in c\, \phi(x, y)$. Let B be a transitive set containing d. Employing **RDC** there exists a function g with domain ω such that $g(0) = B$ and $\forall n \in \omega\, \theta(g(n), g(n+1))$. Obviously $A = \bigcup_{n \in \omega} g(n)$ satisfies our requirements.

The existence of the function f follows from the latter since **RDC** entails **DC**. $\square$

10.3 The Presentation Axiom

The *Presentation Axiom*, **PAx**, is an example of a choice principle which is validated upon interpretation in type theory. In category theory it is also known as the *existence of enough projective sets*, **EPsets** (cf. [12]). In a category $\mathbb{C}$, an object P in $\mathbb{C}$ is *projective* (in $\mathbb{C}$) if for all objects A, B in $\mathbb{C}$, and morphisms $A \xrightarrow{f} B$, $P \xrightarrow{g} B$ with f an epimorphism, there exists a morphism $P \xrightarrow{h} A$ such that the following diagram commutes

$$\begin{tikzcd} A \arrow[r, "f"] & B \\ P. \arrow[u, dotted, "h"] \arrow[ur, "g"'] & \end{tikzcd}$$

It easily follows that in the category of sets, a set P is projective if for any P-indexed family $(X_a)_{a \in P}$ of inhabited sets X_a, there exists a function f with domain P such that, for all $a \in P$, $f(a) \in X_a$.

PAx (or **EPsets**), is the statement that every set is the surjective image of a projective set.

A set B is a **base** if every relation R with domain B extends a function with domain B. A **presentation** of a set A is a function with range A whose domain is a base.

Using the above terminology, **PAx** expresses that every set has a presentation and $\mathbf{AC}_\omega$ expresses that ω is a base whereas **AC** amounts to saying that every set is a base.

Proposition: 10.9 (**ECST**) **PAx** *implies* **DC**.

Proof: Assume $(\forall x{\in}A)\,(\exists y{\in}A)\,xRy$ and $b_0{\in}A$ for some set A and (set) relation R. By **PAx** there exists a base B and a function $h : B \to A$ such that A is the range of h. As a result,

$$\forall u \in B\, \exists v \in B\, h(u)\, R\, h(v).$$

Since B is a base there exists a function $g : B \to B$ such that $g \subseteq R$. Pick $u_0 \in B$ such that $h(u_0) = b_0$. Now define $f' : \omega \to B$ by $f'(0) = u_0$ and $f'(n+1) = g(f'(n))$. By induction on ω one easily verifies

$$\forall n \in \omega\, h(f'(n))\, R\, h(f'(n+1)).$$

Thus, letting $f(n) = h(f'(n))$ one obtains a function $f : \omega \to A$ satisfying $f(0) = b_0$ and $\forall n \in \omega f(n)\; R\; f(n+1)$. $\square$

Proposition: 10.10 (**ECST** + **EXP**) **PAx** *implies Fullness.*

Proof: Let C, D be sets. On account of **PAx**, we can pick a base B and a surjection $h : B \to C$. Let $E = \{S : \exists f \in {}^B D\; S = \{\langle h(u), f(u)\rangle : u \in B\}\}$. E is a set owing to Exponentiation, Replacement, and Δ_0 Separation. Also $E \subseteq mv(C, D)$. Let $R \in mv(C, D)$. Then $\forall u \in B\, \exists y \in D\, \langle h(u), y\rangle \in R$. Since B is a base there exists a function $f : B \to D$ such that $\forall u \in B\, \langle h(u), f(u)\rangle \in R$. Putting $S = \{\langle h(u), f(u)\rangle : u \in B\}$ one easily verifies $S \subseteq R$ and $S \in E$, ascertaining that E is full in $mv(C, D)$. $\square$

Corollary: 10.11 **ECST**+*Exponentiation*+**PAx**+*Strong Collection proves Subset Collection.*

Proof: This follows from the previous Proposition and Proposition 4.12. $\square$

10.4 The Axiom of Multiple Choice

Here we work in **ECST**.

Definition: 10.12 *If X is a set let* $\mathbf{mv}(X)$ *be the class of sets R of ordered pairs such that $X = \{x \mid \exists y(x,y) \in R\}$. A set C* covers *$R \in \mathbf{mv}(X)$ if*

$$\forall x \in X \exists y \in C[(x,y) \in R] \ \ \& \ \ \forall y \in C \exists x \in X[(x,y) \in R].$$

A class $\mathcal{Y}$ is a cover base *for a set X if every $R \in \mathbf{mv}(X)$ is covered by an image of a set in $\mathcal{Y}$. If $\mathcal{Y}$ is a set then it is a* small cover base *for X.*

Proposition: 10.13 (**ECST**) *$\mathcal{Y}$ is a cover base for X iff for every epi $Z \twoheadrightarrow X$ there is an epi $Y \twoheadrightarrow X$, with $Y \in \mathcal{Y}$, that factors through $Z \to X$.*

Proof: Let $\mathcal{Y}$ be a cover base for X and let $f : Z \twoheadrightarrow X$ be epi. Then $R = \{(x,z) \mid x = f(z)\} \in \mathbf{mv}(X)$ so that there is $g : Y \to Z$, with $Y \in \mathcal{Y}$, such that $ran(g)$ covers R. It follows that $f \circ g : Y \twoheadrightarrow X$ is epi.

Conversely, suppose that for every epi $f : Z \twoheadrightarrow X$ there is $g : Y \to Z$, with $Y \in \mathcal{Y}$, such that $f \circ g : Y \to X$, is epi. If $R \in \mathbf{mv}(X)$ let $f : R \to X$ and $h : R \to$ be the two projections on R; i.e. for $(x,z) \in R$, $f(x,z) = x$ and $h(x,z) = z$. Then f is epi so that there is $g : Y \to R$, with $Y \in \mathcal{Y}$, such that $f \circ g : Y \twoheadrightarrow X$ is epi. It follows that $ran(h \circ g)$ covers R. As this is an image of $Y \in \mathcal{Y}$ we have shown that $\mathcal{Y}$ is a cover base for X. □

Definition: 10.14 *A* **weak base** *is a set that has a small cover base.*

Definition: 10.15 *$\mathcal{Y}$ is a (***small***)* **collection family** *if it is a (small) cover base for each of its elements.*

Definition: 10.16

Weak Presentation Axiom (wPAx) *Every set is a weak base.*

Axiom of Multiple Choice (AMC) *Every set is in some small collection family.*

H-axiom *For every set A there is a smallest set $H(A)$ such that if $a \in A$ and $f : a \to H(A)$ then $ran(f) \in H(A)$.*

Proposition: 10.17 (**ECST**)*Any cover base for X is also a cover base for any image of X.*

Proof: Let $\mathcal{Y}$ be a cover base for the set X and let $q : X \twoheadrightarrow X'$ be epi. Given an epi $e' : Z' \twoheadrightarrow X'$ let $Z = \{(x, z') \in X \times Z' \mid q(x) = e'(z')\}$. It's projections $e : Z \twoheadrightarrow X$ and $q' : Z \twoheadrightarrow Z'$ are both epis. So there is $f : Y \to Z$, with $Y \in \mathcal{Y}$, such that $e \circ f : Y \to Z \twoheadrightarrow X$ is also epi. It follows that $q' \circ f : Y \to Z'$ and $e' \circ (q' \circ f) : Y \to Z' \twoheadrightarrow X'$ is epi, as $e' \circ (q' \circ f) = q \circ (e \circ f)$ and $q \circ (e \circ f)$ is epi. So $\mathcal{Y}$ is a cover base for X'. □

Theorem: 10.18 (**ECST**)

1. **PAx** $\Rightarrow$ **AMC**
2. **AMC** $\Rightarrow$ **wPAx**
3. **wPAx** + *Exponentiation* $\Rightarrow$ *Subset Collection*
4. **AMC** + *H-axiom* $\Rightarrow$ **REA**
5. *Collection* + **RDC** + **wPAx** $\Rightarrow$ **AMC**

Proof:

1. Observe that for any base set B the set $\{B\}$ is a collection family, for if $Z \twoheadrightarrow B$ is epi then the identity function $B \twoheadrightarrow B$ is an epi that factorises through $Z \twoheadrightarrow B$. Assume **PAx** and let A be a set. By **PAx** there is a base set B so that A is an image of B. By Proposition 10.17 $\{B, A\}$ is a collection family.

2. If $A \in \mathcal{Y}$, where $\mathcal{Y}$ is a small collection family, then $\mathcal{Y}$ is a cover base for A so that A is a weak base.

3. To prove Subset Collection, given sets A, B we want a set C of subsets of B such that every $R \in \mathbf{mv}({}^A B)$ is covered by some set in C. By **wPAx** choose a small cover base $\mathcal{Y}$ for A and let
$$C = \bigcup_{Y \in \mathcal{Y}} \{ran(g) \mid g \in^Y B\}.$$
This is a set by Exponentiation and Union-Replacement.

4. It suffices to show that if $\mathcal{Y}$ is a collection family then $H(\mathcal{Y})$ is a regular class. So let $b \in H(\mathcal{Y})$ and $R \in \mathbf{mv}({}^b H(\mathcal{Y}))$. Choose $a \in \mathcal{Y}$ and $f : a \twoheadrightarrow b$. Then $S \in \mathbf{mv}(a)$ where
$$S = \{(x, y) \in a \times H(\mathcal{Y}) \mid (f(x), y) \in R\},$$
so that there is $a' \in \mathcal{Y}$ and $g : a' \twoheadrightarrow H(\mathcal{Y})$ such that $ran(g)$ covers S. It follows that $ran(g)$ also covers R. As $ran(g) \in H(\mathcal{Y})$ we are done.

5. Given any set $\mathcal{Y}$, by **wPAx**,

$$(\forall X \in \mathcal{Y})(\exists \mathcal{Y}')\ [\mathcal{Y}' \text{ is a cover base for } X].$$

By Collection there is a set $\mathcal{U}$ such that

$$(\forall X \in \mathcal{Y})(\exists \mathcal{Y}' \in \mathcal{U})\ [\mathcal{Y}' \text{ is a cover base for } X].$$

If $\mathcal{Y}' = \bigcup \mathcal{U}$ then $(\mathcal{Y}, \mathcal{Y}') \in S$ where S is the class of all $(\mathcal{Y}, \mathcal{Y}')$ such that $\forall X \in \mathcal{Y}[\mathcal{Y}'$ is a cover base for $X]$. Thus

$$\forall \mathcal{Y}\ \exists \mathcal{Y}'\ (\mathcal{Y}, \mathcal{Y}') \in S.$$

By **RDC**, for any set A there is a sequence $\{\mathcal{Y}_n\}_{n \in \mathbb{N}}$ such that $\mathcal{Y}_0 = \{A\}$ and $(\mathcal{Y}_n, \mathcal{Y}_{n+1}) \in S$ for all $n \in \mathbb{N}$. Now let $\mathcal{Y} = \bigcup_{n \in \mathbb{N}} \mathcal{Y}_n$. Then $A \in \mathcal{Y}$ and it is easy to check that $\mathcal{Y}$ is a collection family.

$\square$

11 The Regular Extension Axiom and its Variants

11.1 Axioms and variants

The first large set axiom proposed in the context of constructive set theory was the *Regular Extension Axiom*, **REA**, which was introduced to accommodate inductive definitions in **CZF** (cf. [1], [3]).

Definition: 11.1 A set C is said to be **regular** if it is transitive, inhabited (i.e. $\exists u\, u \in C$) and for any $u \in C$ and $R \in \mathbf{mv}({}^uC)$ there exists a set $v \in C$ such that

$$\forall x \in u\, \exists y \in v\ \langle x, y\rangle \in R\ \wedge\ \forall y \in v\, \exists x \in u\ \langle x, y\rangle \in R.$$

We write $\mathbf{Reg}(C)$ to express that C is regular.

REA is the principle

$$\forall x\, \exists y\ (x \subseteq y\ \wedge\ \mathbf{Reg}(y)).$$

Definition: 11.2 There are interesting weaker notions of regularity.

A transitive inhabited set C is **weakly regular** if for any $u \in C$ and $R \in \mathbf{mv}({}^uC)$ there exists a set $v \in C$ such that

$$\forall x \in u\, \exists y \in v\ \langle x, y\rangle \in R.$$

We write $\mathbf{wReg}(C)$ to express that C is weakly regular. The **weakly Regular Extension Axiom** (**wREA**) is as follows: *Every set is a subset of a weakly regular set.*

A transitive inhabited set C is **functionally regular** if for any $u \in C$ and function $f : u \to C$, $\mathbf{ran}(f) \in C$. We write $\mathbf{fReg}(C)$ to express that C is functionally regular. The **functional Regular Extension Axiom** (**fREA**) is as follows: *Every set is a subset of a functionally regular set.*

There are also interesting notions of stronger regularity.

Definition: 11.3 A class A is said to be **$\bigcup$-closed** if for all $x \in A$, $\bigcup x \in A$.

A class A is said to be **closed under Exponentiation (Exp-closed)** if for all $x, y \in A$, ${}^xy \in A$.

One is naturally led to consider strengthenings of the notion of a regular set, for instance that the set should also be $\bigcup$-closed and Exp-closed.

A transitive inhabited set C is said to be **$\bigcup$-regular** if C is regular and $\bigcup$-closed. The $\bigcup$-*Regular Extension Axiom* ($\bigcup$**REA**) is as follows:

Every set is a subset of a $\bigcup$-regular set.

A transitive inhabited set C is said to be *strongly regular* if C is regular, $\bigcup$-closed and Exp-closed. The *Strong Regular Extension Axiom* (**sREA**) is as follows:

Every set is a subset of a strongly regular set.

Lemma: 11.4 (**ECST**) *If A is regular then A is weakly regular and functionally regular.*

Proof: Obvious. $\square$

Lemma: 11.5 (**ECST**) *Let A be functionally regular and $\mathbf{2} \in A$. Then, A is closed under Pairing, that is $\forall x, y \in A\ \{x, y\} \in A$. Moreover, if $b \in A$ and $f : b \to A$, then $f \in A$.*

Proof: Given $x, y \in A$ define a function $g : \mathbf{2} \to A$ by $g(\mathbf{0}) = x$ and $g(\mathbf{1}) = y$. Then $\{x, y\} = \mathbf{ran}(g) \in A$.

Let $b \in A$ and $f : b \to A$. As A is closed under Pairing, we get $\langle x, f(x)\rangle \in A$ whenever $x \in b$. Therefore, the function $(x \mapsto \langle x, f(x)\rangle)$ maps b to A, and thus its range, which is the function f, is an element of A. $\square$

Corollary: 11.6 (**ECST**) **fREA** *implies Exponentiation.*

Proof: Given sets B, C, choose a functionally regular set A such that $B, C \in A$. Then ${}^{B}C \subseteq A$ by Lemma 11.5, whence ${}^{B}C$ is a set by Bounded Separation. $\square$

In **ZF** one can show that every well-founded set can be collapsed onto a transitive set, this principle is known as the axiom Beta.

Definition: 11.7 The axiom **Beta** asserts: for every well-founded set (A, R) there is a function f with domain A, satisfying:

$$f(x) \quad = \quad \{f(y) \mid yRx\}, \tag{17}$$

for all $x \in A$. The function f is said to be **collapsing** for (A, R).

Note that the uniqueness of a function satisfying (17) is an immediate consequence of the well-foundedness of the relation. Moreover, the image of the collapsing function is a transitive set. To see this, let $u \in a \in \mathbf{ran}(f)$. Then $a = f(x)$ for some $x \in A$, and, as f satisfies equation (17), we get $u = f(y)$ for some yRx. Thus $u \in \mathbf{ran}(f)$.

Beta is not provable in **CZF** alone, though, but it is provable with the help of **fREA**.

Proposition: 11.8 ($\mathbf{ECST} + \mathbf{fREA}$) *Axiom Beta holds true.*

Proof: Let (A, R) be a well-founded set and let R^* be the transitive closure of R whose existence can be proved in $\mathbf{ECST} + \mathbf{fREA}$ by Lemma 6.25 and Corollary 11.6.

For $a \in A$, let $R^*_a = \{y \in A \mid yR^*a\}$. Choose a functionally regular set B such that $A, 2 \in B$ and for all $a \in A$, $R_a, R^*_a \cup \{a\} \in B$. Let $\mathcal{F}$ be the set of all functions $f \in B$ with domain $R^*_a \cup \{a\}$ for some $a \in A$ such that whenever $xR^*a \vee x = a$, then $f(x)$ satisfies the equation (17). Note that $\mathcal{F}$ is a set by Bounded Separation. The first fact to be noted about $\mathcal{F}$ is that all the functions in $\mathcal{F}$ are compatible, which is to say that if $x \in A$ and $x \in \mathbf{dom}(f) \cap \mathbf{dom}(g)$ for some $f, g \in \mathcal{F}$, then $f(x) = g(x)$. Formally one proves this by verifying that the set

$$\{x \in A \mid \forall f, g \in \mathcal{F}[x \in \mathbf{dom}(f) \cap \mathbf{dom}(g) \rightarrow f(x) = g(x)]\}$$

is R-inductive. As a result, $G = \bigcup \mathcal{F}$ is a function, too.

Next, we shall show that $\mathbf{dom}(G)$ is R-inductive. Let $a \in A$ and assume that $x \in \mathbf{dom}(G)$ for all xRa. By definition of $\mathcal{F}$ this entails $x \in \mathbf{dom}(G)$ for all xR^*a. We define f by

$$\begin{aligned} t(a) &= \{G(y) \mid yRa\} \\ f &= \{(x, G(x)) \mid xR^*a\} \cup \{(a, t(a))\}. \end{aligned}$$

As $\neg\, aR^*a$ holds by Corollary 9.3, f is a function. The domain of f is $R^*_a \cup \{a\}$ and the equation (17) holds for all x in f's domain. In order to be able to conclude that $a \in \mathbf{dom}(G)$ we need to show that $f \in B$. Since $x, G(x) \in B$ for all xR^*a and B is closed under taking pairs (since $2 \in B$) we get $(x, G(x)) \in B$ for all xR^*a. As $R_a \in B$, the functional regularity of B yields $\{G(y) \mid yRa\} \in B$, whence $t(a) \in B$. Therefore we have $f : R^*_a \cup \{a\} \rightarrow B$. Since $R^*_a \cup \{a\} \in B$, it follows that $f \in B$ by Lemma 11.5. Consequently, $f \in \mathcal{F}$. Thus $a \in \mathbf{dom}(G)$ as $a \in \mathbf{dom}(f)$.

Having shown that $\mathbf{dom}(G)$ is R-inductive, we get $\mathbf{dom}(G) = A$. Therefore G is the function that collapses (A, R). $\square$

Proposition: 11.9 (**ECST**) **REA** *implies Fullness.*

Proof: Let A, B be sets. Using **REA**, there exists a regular set Z such that $\mathbf{2}, A, B, A \times (A \times B) \in Z$. Let $C = \{S \in Z | \ S \in \mathbf{mv}({}^A B)\}$. S is a set by Δ_0 Separation. We claim that C is full in $\mathbf{mv}({}^A B)$. To see this let $R \in \mathbf{mv}({}^A B)$. Let

$$R^* = \{\langle x, \langle x, y\rangle\rangle | \ x \in A \ \wedge \ \langle x, y\rangle \in R\}.$$

$\mathbf{2} \in Z$ guarantees that Z is a model of Pairing and thus $R^* \in \mathbf{mv}({}^A Z)$. Employing the regularity of Z there exists $S^* \in Z$ such that

$$\forall x \in A \, \exists z \in S^* \, (\langle x, z\rangle \in R^*) \ \wedge \ \forall z \in S^* \, \exists x \in A \, (\langle x, z\rangle \in S^*).$$

As a result, $S^* \subseteq R$ and $S^* \in \mathbf{mv}({}^A B)$. Moreover, $S^* \in C$. $\square$

Corollary: 11.10 (**ECST** + Strong Collection) **REA** *implies Subset Collection.*

Proof: By Proposition 11.9 and Proposition 4.12. $\square$

Lemma: 11.11 (**ECST** + Strong Collection) *Assume that A is a regular set, $b \in A$ and $\forall x \in b \, \exists y \in A \, \phi(x, y)$. Then there exists a set $c \in A$ such that*

$$\forall x \in b \, \exists y \in c \, \phi(x, y) \ \wedge \ \forall y \in c \, \exists x \in b \, \phi(x, y).$$

Proof: $\forall x \in b \, \exists y \in A \, \phi(x, y)$ implies $\forall x \in b \, \exists z \, \psi(x, z)$, with $\psi(x, z)$ being the formula $\exists y \in A \, (\phi(x, y) \ \wedge \ z = \langle x, y\rangle)$. Using Strong Collection there exists a set R such that

$$\forall x \in b \, \exists z \in R \, \psi(x, z) \ \wedge \ \forall z \in R \, \exists x \in b \, \psi(x, z).$$

Thus $R \in \mathbf{mv}({}^b A)$. Owing to the regularity of A there exists a set $c \in A$ such that

$$\forall x \in b \, \exists y \in c \, \langle x, y\rangle \in R \ \wedge \ \forall y \in c \, \exists x \in b \, \langle x, y\rangle \in R.$$

As a consequence we get $\forall x \in b \, \exists y \in c \, \phi(x, y) \ \wedge \ \forall y \in c \, \exists x \in b \, \phi(x, y)$. $\square$

11.2 Some metamathematical results about REA

Lemma: 11.12 *On the basis of* **ZFC***, a set B is regular if and only if B is functionally regular.*

Proof: Obvious. $\square$

Proposition: 11.13 **ZFC** $\vdash$ **REA**.

Proof: The axiom of choice implies that arbitrarily large regular cardinals exists and that for each regular cardinal κ, $H(\kappa)$ is a regular set. Given any set b let μ be the cardinality of $\mathbf{TC}(b) \cup \{b\}$. Then the next cardinal after μ, denoted μ^+, is regular and $b \in H(\mu^+)$. $\square$

Proposition: 11.14 *(i)* $\mathbf{CZF} + \mathbf{AC}_\omega$ *does not prove that* $H(\omega \cup \{\omega\})$ *is a set.*

(ii) **CZF** *does not prove* **REA***.*

Proof: It has been shown by Rathjen (cf. [**?**]) that $\mathbf{CZF} + \mathbf{AC}_\omega$ has the same proof-theoretic strength as Kripke-Platek set theory, **KP**. The proof-theoretic ordinal of $\mathbf{CZF} + \mathbf{AC}_\omega$ is the so-called Bachmann-Howard ordinal $\psi_{\Omega_1}\varepsilon_{\Omega_1+1}$. Let

$$T := \mathbf{CZF} + \mathbf{AC}_\omega + H(\omega \cup \{\omega\}) \texttt{ is a set.}$$

Another theory which has proof-theoretic ordinal $\psi_{\Omega_1}\varepsilon_{\Omega_1+1}$ is the intuitionistic theory of arithmetic inductive definitions $\mathbf{ID}^i_1$. We aim at showing that T proves the consistency of $\mathbf{ID}^i_1$. The latter implies that T proves the consistency of $\mathbf{CZF} + \mathbf{AC}_\omega$ as well, yielding (i), owing to Gödel's Incompleteness Theorem.

Let $L_{HA}(P)$ be the language of Heyting arithmetic augmented by a new unary predicate symbol P. The language of $\mathbf{ID}^i_1$ comprises L_{HA} and in addition contains a unary predicate symbol I_ϕ for each formula $\phi(u, P)$ of $L_{HA}(P)$ in which P occurs only positively. The axioms of $\mathbf{ID}^i_1$ comprise those of Heyting arithmetic with the induction scheme for natural numbers extended to the language of $\mathbf{ID}^i_1$ plus the following axiom schemes relating to the predicates I_ϕ:

$$(ID^1_\phi) \qquad \forall x\,[\phi(x, I_\phi) \to I_\phi(x)]$$
$$(ID^2_\phi) \qquad \forall x\,[\phi(x, \psi) \to \psi(x)] \;\to\; \forall x\,[I_\phi(x) \to \psi(x)]$$

for every formula ψ, where $\phi(x, \psi)$ arises from $\phi(x, P)$ by replacing every occurrence of a formula $P(t)$ in $\phi(x, P)$ by $\psi(t)$.

Arguing in T we want to show that $\mathbf{ID}_1^i$ has a model. The domain of the model will be ω. The interpretation of $\mathbf{ID}_1^i$ in T is given as follows. The quantifiers of $\mathbf{ID}_1^i$ are interpreted as ranging over ω. The arithmetic constant 0 and the functions $+1, +, \cdot$ are interpreted by their counterparts on ω. It remains to provide an interpretation for the predicates I_ϕ, where $\phi(u, P)$ is a P positive formula of $L_{HA}(P)$. Let $\phi(u, v)^*$ be the set-theoretic formula which arises from $\phi(u, P)$ by, firstly, restricting all quantifiers to ω, secondly, replacing all subformulas of the form $P(t)$ by $t \in v$, and thirdly, replacing the arithmetic constant and function symbols by their set-theoretic counterparts. Let

$$\Gamma_\phi(A) = \{x \in \omega | \, \phi(x, A)^*\}$$

for every subset A of ω, and define a mapping $x \mapsto \Gamma_\phi^x$ by recursion on $H(\omega \cup \{\omega\})$ via

$$\Gamma_\phi^x = \Gamma_\phi(\bigcup_{u \in x} \Gamma_\Phi^u).$$

Finally put

$$I_\phi^* = \bigcup_{x \in H(\omega \cup \{\omega\})} \Gamma_\phi^x.$$

It is obvious that the above interpretation validates the arithmetic axioms of $\mathbf{ID}_1^i$. The validity of the interpretation of (ID_ϕ^1) follows from

$$\Gamma_\phi(I_\phi^*) \subseteq I_\phi^*. \tag{18}$$

Let $HC = H(\omega \cup \{\omega\})$. Before we prove (18) we show

$$\Gamma_\phi^{\in a} \subseteq \Gamma_\phi^a \tag{19}$$

for $a \in HC$, where $\Gamma_\phi^{\in a} = \bigcup_{x \in a} \Gamma_\phi^x$. (19) is shown by Set Induction on a. The induction hypothesis then yields, for $x \in a$,

$$\Gamma_\phi^{\in x} \subseteq \Gamma_\phi^x \subseteq \Gamma_\phi^{\in a}.$$

Thus, by monotonicity of the operator Γ_ϕ,

$$\Gamma_\phi(\Gamma_\phi^{\in x}) = \Gamma_\phi^x \subseteq \Gamma_\phi(\Gamma_\phi^{\in a}) = \Gamma_\phi^a,$$

and hence $\Gamma_\phi^{\in a} \subseteq \Gamma_\phi^a$, confirming (19).

To prove (18) assume $n \in \Gamma_\phi(I_\phi^*)$. Then $\phi(n, \bigcup_{x \in HC} \Gamma_\phi^x)^*$ by definition of Γ_Φ. Now, since $\bigcup_{x \in HC} \Gamma_\phi^x$ occurs positively in the latter formula one can show, by induction on the built up of ϕ, that

$$\phi(n, \Gamma_\phi^a)^* \tag{20}$$

for some $a \in HC$. The atomic cases are obvious. The crucial case is when $\phi(n, v)^*$ is of the form $\forall k \in \omega \psi(k, n, v)$. Inductively one then has

$$\forall k \in \omega \, \exists y \in HC \, \psi(k, n, \Gamma_\phi^y).$$

Employing Strong Collection, there exists $R \in \mathbf{mv}({}^\omega HC)$ such that

$$\forall k \in \omega \, \exists y \, [\langle k, y \rangle \in R \ \wedge \ \psi(k, n, \Gamma_\phi^y).$$

Using $\mathbf{AC}_\omega$ there exists a function $f : \omega \to HC$ such that $\forall k \in \omega \, \langle k, f(k) \rangle \in R$ and hence

$$\forall k \in \omega \, \psi(k, n, \Gamma_\phi^{f(k)}).$$

Let $b = \mathbf{ran}(f)$. It follows from (19) that $\Gamma_\phi^{f(k)}) \subseteq \Gamma_\phi^b$, and thus, by positivity of the occurrence of P in ϕ we get,

$$\forall k \in \omega \, \psi(k, n, \Gamma_\phi^b))^*.$$

The validity of the interpretation of (ID_ϕ^2) can be seen as follows. Assume

$$\forall i \in \omega \, [\phi(i, X) \to i \in X], \tag{21}$$

where X is a definable class. We want to show $I_\phi^* \subseteq X$. It suffices to show $\Gamma_\phi^a \subseteq X$ for all $a \in HC$. We proceed by induction on $a \in HC$. The induction hypothesis provides $\Gamma_\phi^{\in a} \subseteq X$. Monotonicity of Γ_ϕ yields $\Gamma_\phi(\Gamma_\phi^{\in a}) = \Gamma_\phi^a \subseteq \Gamma_\phi(X)$. By (19) it holds $\Gamma_\phi(X) \subseteq X$. Hence $\Gamma_\phi^a \subseteq X$.

We have now shown within T that $\mathbf{ID}_1^i$ has a model. Note also that, arguing in T, this model is a set as the mapping $\phi(u, P) \mapsto I_\phi^*$ is a function when we assume a coding of the syntax of $\mathbf{ID}_1^i$. As a result, by formalizing the notion of truth for this model, T proves the consistency of $\mathbf{ID}_1^i$, establishing (i).

(ii) It has been shown by Rathjen (cf. [**?**]) that $\mathbf{CZF} + \mathbf{REA}$ is of much greater proof-theoretic strength than $\mathbf{CZF}$. However, (ii) also follows from (i) as $\mathbf{REA}$ implies that $H(\omega \cup \{\omega\})$ is a set. $\square$

$\mathbf{ZF}$ proves $\mathbf{fREA}$, though this is not a triviality. Here we shall draw on [39], where it was shown that $\mathbf{ZF}$ proves that $H(\omega \cup \{\omega\})$ is a set.

Proposition: 11.15 $\mathbf{ZF} \vdash \mathbf{fREA}$

Proof: Every set x is contained in a transitive set A with $\omega \subseteq A$. Thus if we can show that $H(A)$ is a set we have found a set comprising x which is functionally regular. The main task of the proof is therefore to show that

$H(A)$ is a set. Let ρ be the supremum of all ordinals which are order types of well-orderings of subsets of A. (A well-ordering of a set B is a relation $R \subseteq B \times B$ such R linearly orders the elements of B and for every non-empty $X \subseteq B$ there exists an R-least element in X, i.e. $\exists u \in X \forall v \in X \neg vRu$.) Note that ρ exists owing to Power Set, Separation, Replacement, and Union. Also note that ρ is a cardinal $\geq \omega$ and for every well-ordering R of a subset of A, the order-type of R is less than ρ.

Let $\kappa = \rho^+$ (where ρ^+ denotes the least cardinal bigger than ρ). We shall show that $\text{rank}(s) < \kappa$ for every $s \in H(A)$, and thus

$$H(A) \subseteq V_\kappa. \tag{22}$$

For a set X let $\bigcup^n X$ be the n-fold union of X, i.e., $\bigcup^0 X = X$, and $\bigcup^{n+1} X = \bigcup(\bigcup^n X)$. Note that

$$\text{rank}(X) = \{\text{rank}(u) |\ u \in \mathbf{TC}(X)\} = \bigcup_{n\in\omega} \{\text{rank}(u) |\ u \in \bigcup^n X\}.$$

Let Θ be the set of all non-empty finite sequences of ordinals $< \rho$. We shall define a function F on $H(A) \times \omega \times \Theta$ such that for each $s \in H(A)$, if F_s denotes the function $F_s(n,t) = F(s,n,t)$, then F_s maps $\omega \times \Theta$ onto $\text{rank}(s)$. Since there is a bijection between Θ and ρ (cf. [44], 10.13), we then have $\text{rank}(s) < \kappa$, and thus $s \in V_\kappa$. We define the function F by recursion on n. For each n, we denote by F_s^n the function $F_s^n(t) = F(s,n,t)$. For $n = 0$ we let for each $s \in H(A)$ and each $\beta < \rho$,

$$F_s^0(\langle\beta\rangle) \quad = \quad \text{the } \beta\text{th element of } \{\text{rank}(u) |\ u \in s\}$$

if the set $\{\text{rank}(u) |\ u \in s\}$ has order-type $> \beta$, and $F_s^0(\langle\beta\rangle) = 0$ otherwise. If $t \in \Theta$ is not of the form $\langle\beta\rangle$, we put $F_s^0(t) = 0$.

Since there exists $b \in A$ and $g : b \to H(A)$ such that $s = \mathbf{ran}(g)$, the order type of $\{\text{rank}(x) |\ x \in s\}$ is an ordinal $< \rho$, owing to $b \subseteq A$. And hence F_s^0 maps Θ onto the set $\{\text{rank}(x) |\ x \in s\}$.

For $n = 1$, $s \in H(A)$, and $\beta_0, \beta_1 < \rho$ we let

$$F_s^1(\langle\beta_0, \beta_1\rangle) = \text{the } \beta_1\text{th element of } \{F_u^0(\langle\beta_0\rangle) |\ u \in s\},$$

if it exists, and $F_s^1(\langle\beta_0, \beta_1\rangle) = 0$ otherwise. If $t \in \Theta$ is not of the form $\langle\beta_0, \beta_1\rangle$, let $F_s^1(t) = 0$. In general, let

$$F_s^{n+1}(\langle\beta_0, \ldots, \beta_{n+1}\rangle) \quad = \quad \text{the } \beta_{n+1}\text{th element of } \{F_u^n(\langle\beta_0, \ldots, \beta_n\rangle) |\ u \in s\},$$

if it exists, and $F_s^{n+1}(\langle\beta_0, \ldots, \beta_{n+1}\rangle) = 0$ otherwise. If $t \in \Theta$ is not of the form $\langle\beta_0, \ldots, \beta_{n+1}\rangle$, let $F_s^{n+1}(t) = 0$.

For each $s \in H(A)$ and each $\langle \beta_0, \ldots, \beta_n \rangle \in \Theta$, the order-type of the set $\{F_u^n(\langle \beta_0, \ldots, \beta_n \rangle) |\ u \in s\}$ is an ordinal $< \rho$. Hence F_s^{n+1} maps Θ onto the set

$$\{F_u^n(\langle \beta_0, \ldots, \beta_n \rangle) |\ u \in s \wedge \langle \beta_0, \ldots, \beta_n \rangle \in \rho \times \cdots \times \rho\}.$$

It follows by induction that for each n and for each $s \in H(A)$, the function F_s^n maps Θ onto the set $\{\text{rank}(u) |\ u \in \bigcup^n s\}$. For each $s \in H(A)$, F_s therefore maps $\omega \times \Theta$ onto the set $\{\text{rank}(u) |\ u \in \mathbf{TC}(s)\} = \text{rank}(s)$.

This concludes the proof of (22). Finally, by Separation, it follows that $H(A)$ is a set. $\square$

Remark: 11.16 By [39] **ZF** proves that either $\text{rank}(H(\omega \cup \{\omega\})) = \aleph_1$ or $\text{rank}(H(\omega \cup \{\omega\})) = \aleph_2$. The latter is the case when $\aleph_1$ is singular.

Proposition: 11.17 *Let $HC = H(\omega \cup \{\omega\})$. If* **ZF** *is consistent, then* **ZF** *does not prove that HC is weakly regular.*

Proof: Assume that **ZF** is consistent. Let T be the theory **ZF** plus the assertion that the real numbers are a union of countably many countable sets. By results of Feferman and Levy it follows that T is consistent as well (see [28] or [38], Theorem 10.6). In the following we argue in T and identify the set of reals, $\mathbb{R}$, with the set of functions from ω to ω. Working towards a contradiction, assume that HC is weakly regular. Let $\mathbb{R} = \bigcup_{n \in \omega} X_n$, where each X_n is countable and infinite. By induction on $n \in \omega$ one verifies that $n \in HC$ for every $n \in \omega$, and thus $\omega \in HC$. If $f : \omega \to \omega$ define f^* by $f^*(n) = \langle n, f(n) \rangle$. Then $f^* : \omega \to HC$ as HC is closed under Pairing, and hence $f = \mathbf{ran}(f^*) \in HC$. As a result, $\mathbb{R} \subseteq HC$ and, moreover, $X_n \in HC$ since each X_n is countable. Furthermore, $\{X_n |\ n \in \omega\} \in HC$.

For each X_n let

$$\mathcal{G}_n = \{f : \omega \to X_n |\ f \text{ is 1-1 and onto}\}.$$

Note that $\mathcal{G}_n \subseteq HC$. Define $R \in \mathbf{mv}({}^{\{X_n|\ n \in \omega\}}HC)$ by

$$\langle X_n, f \rangle \in R \text{ iff } f \in \mathcal{G}_n.$$

By weak regularity there exists $B \in HC$ such that

$$\forall n \in \omega\, \exists f \in B\ \langle X_n, f \rangle \in R.$$

Now pick $g : \omega \to B$ such that $B = \mathbf{ran}(g)$. For every $x \in \mathbb{R}$ define $J(x)$ as follows. Select the least n such that $x \in X_n$ and then pick the least m such that $\langle X_n, g(m) \rangle \in R$, and let

$$J(x) = \langle n, (g(m))^{-1}(x) \rangle,$$

where $(g(m))^{-1}$ denotes the inverse function of $g(m)$. It follows that

$$J : \mathbb{R} \to \omega \times \omega$$

is a 1-1 function, implying the contradiction that $\mathbb{R}$ is countable. $\square$

Definition: 11.18 A class A is said to be $\bigcup$-*closed* if for all $x \in A$, $\bigcup x \in A$.

A class A is said to be *closed under Exponentiation (Exp-closed)* if for all $x, y \in A$, ${}^x y \in A$.

Proposition: 11.19 (**ZF**) *If A is a functionally regular $\bigcup$-closed set with $\mathbf{2} \in A$, then the least ordinal not in A, $o(A)$, is a regular ordinal.*

Proof: If $f : \alpha \to o(A)$, where $\alpha < o(A)$, then $\alpha \in A$ and thus $\mathbf{ran}(f) \in A$, and hence $\bigcup \mathbf{ran}(f) \in A$. Since $\mathbf{ran}(f)$ is a set of ordinals, $\bigcup \mathbf{ran}(f)$ is an ordinal, too. Let $\beta = \bigcup \mathbf{ran}(f)$. Then $\beta \in A$. Note that $\beta + 1 \in A$ as well since $\mathbf{2} \in A$ entails that A is closed under Pairing and $\beta + 1 = \bigcup\{\beta, \{\beta\}\}$. Since $f : \alpha \to \beta + 1$ this shows that $o(A)$ is a regular ordinal. $\square$

Corollary: 11.20 *If* **ZF** *is consistent, then so is the theory*

$$\mathbf{ZF} + HC \textit{ is not } \bigcup\textit{-closed.}$$

Proof: This follows from Proposition 11.19 and Proposition 11.17. $\square$

Corollary: 11.21 *If* $\mathbf{ZFC} + \forall\alpha\, \exists\kappa > \alpha\, (\kappa \texttt{ is a strongly compact cardinal})$ *is consistent, then so is the theory* **ZF** *plus the assertion that there are no $\bigcup$-closed functionally regular sets containing ω.*

Proof: By Proposition 11.19, the existence of a functionally regular $\bigcup$-closed set A with $\omega \in A$ would yield the existence of an uncountable regular ordinal. By [34], however, all uncountable cardinals can be singular under the assumption that $\mathbf{ZFC} + \forall\alpha\, \exists\kappa > \alpha\, (\kappa \texttt{ is a strongly compact cardinal})$ is a consistent theory. $\square$

The consistency assumption of the previous Proposition might seem exaggerated. It is, however, known that the consistency of

$$\mathbf{ZF} + \texttt{All uncountable cardinals are singular}$$

cannot be proved without assuming the consistency of the existence of some large cardinals. It was shown in [18] that if $\aleph_1$ and $\aleph_2$ are both singular one can obtain an inner model with a measurable cardinal.

Proposition: 11.22 (**ZF**) *If A is a weakly regular set with $\omega \in A$, then rank(A) is an uncountable ordinal of cofinality $> \omega$.*

Proof: Set $\kappa = \text{rank}(A)$. Obviously $\omega < \kappa$. Suppose $f : \omega \to \kappa$. Define $R \subseteq \omega \times A$ by nRa iff $f(n) < \text{rank}(a)$. Since for every ordinal $f(n)$ there exists a set $a \in A$ with rank $> f(n)$, R is a total relation. Employing the weak regularity of A, there exists a set $b \in A$ such that $\forall n \in \omega \, \exists x \in b \; f(n) < \text{rank}(x)$. As a result, $f : \omega \to \text{rank}(b)$ and $\text{rank}(b) < \kappa$. This shows that the cofinality of κ is bigger than ω. $\Box$

Corollary: 11.23 (**ZF**) **wREA** *implies that, for any set X, there is a cardinal κ such that X cannot be mapped onto a cofinal subset of κ.*

Proof: Let A be a weakly regular set such that $X \in A$. Set $\kappa = \text{rank}(A)$. Aiming at a contradiction, suppose there exists $f : X \to \kappa$ such that $\mathbf{ran}(f)$ is a cofinal subset of κ. Define $R \subseteq X \times A$ by uRa iff $f(u) < \text{rank}(a)$. Since for every ordinal $f(u)$ there exists a set $a \in A$ with $\text{rank}(a) > f(u)$, R is a total relation. Employing the weak regularity of A, there exists a set $b \in A$ such that $\forall u \in X \, \exists y \in b \; f(u) < \text{rank}(y)$. As a result, $f : X \to \text{rank}(b)$ and $\text{rank}(b) < \kappa$. But the latter contradicts the assumption that $\mathbf{ran}(f)$ is a cofinal subset of κ. $\Box$

Proposition: 11.24 *The theories* $\mathbf{CZF} + \mathbf{REA}$ *and*

$$\mathbf{CZF} + \forall x \, \exists A \, [x \in A \; \wedge \; \mathbf{Reg}(A) \; \wedge \; A \textit{ is } \bigcup\textit{-closed and Exp-closed}]$$

have the same proof-theoretic strength.

Proof: See [59], Theorem 4.7. $\Box$

The next result shows, however, that the strengthenings of **REA** we considered earlier are not provable in $\mathbf{CZF} + \mathbf{REA}$.

Proposition: 11.25 *If* **ZF** *is consistent, then* $\mathbf{CZF} + \mathbf{REA}$ *does not prove that there exists a regular set containing ω which is Exp-closed and $\bigcup$-closed.*

Proof: For a contradiction assume

$$\mathbf{CZF} + \mathbf{REA} \vdash \exists A \, [\mathbf{Reg}(A) \; \wedge \; \omega \in A \; \wedge \; A \texttt{ is Exp-closed and } \bigcup\texttt{-closed}.$$

Then **ZFC** would prove this assertion. In the following we work in **ZFC**. By Proposition 11.19 $\kappa = o(A)$ is a regular uncountable cardinal. We claim that

κ is a limit cardinal, too. Let $\rho < \kappa$ and $F : {}^{\rho}2 \to \mu$ be a surjective function. Suppose $\kappa \leq \mu$. Then let $X = \{g \in {}^{\rho}2 |\, F(g) < \kappa\}$. Note that

$$\{F(g) |\, g \in X\} = \kappa$$

since F is surjective. Since A is Exp-closed we have ${}^{({}^{\rho}2)}2 \in A$. Define a function $G : {}^{\rho}2 \to 2$ by $G(h) = 1$ if $h \in X$, and $G(h) = 0$ otherwise. Then $G \in A$. Further, define $j : G \to A$ by $j(\langle h, i\rangle) = F(h)$ if $i = 1$, and $j(\langle h, i\rangle) = 0$ otherwise. Then $\mathbf{ran}(j) \in A$. However, $\mathbf{ran}(j) = \{F(g) |\, g \in X\} \cup \{0\} = \kappa$, yielding the contradiction $\kappa \in \kappa$.

As a result, $\mu < \kappa$ and therefore κ cannot be a successor cardinal. Consequently we have shown the existence of a weakly inaccessible cardinal. But that cannot be done in **ZFC** providing **ZF** is consistent. □

11.3 ZF models of REA

Definition: 11.26 There is weak form of the axiom of choice, which holds in a plethora of **ZF** universes. The *axiom of small violations of choice*, **SVC**, has been studied by A. Blass [12]. It says in some sense, that all failure of choice occurs within a single set. **SVC** is the assertion that there is a set S such that, for every set a, there exists an ordinal α and a function from $S \times \alpha$ onto a.

Lemma: 11.27 *(i) If X is transitive and $X \subseteq B$, then $X \subseteq H(B)$.*
(ii) If $2 \in B$ and $x, y \in H(B)$, then $\langle x, y\rangle \in H(B)$.

Proof: (i): By Set Induction on a one easily proves that $a \in X$ implies $a \in H(B)$.

(ii): Suppose $2 \in B$ and $x, y \in H(B)$. Let f be the function $f : 2 \to H(B)$ with $f(0) = x$ and $f(1) = y$. Then $\mathbf{ran}(f) = \{x, y\} \in H(B)$. By repeating the previous procedure with $\{x\}$ and $\{x, y\}$ one gets $\langle x, y\rangle \in H(B)$. □

Theorem: 11.28 (**ZF**) **SVC** *implies* **AMC** *and* **REA**.

Proof: Let M be a ground model that satisfies **ZF** + **SVC**. Arguing in M let S be a set such that, for every set a, there exists an ordinal α and a function from $S \times \alpha$ onto a.

Let $\mathbb{P}$ be the set of finite partial functions from ω to S, and, stepping outside of M, let G be an M-generic filter in $\mathbb{P}$. By the proof of [12], Theorem 4.6, $M[G]$ is a model of **ZFC**.

Let A be an arbitrary set in M. Let $B = \bigcup_{n\in\omega} F(n)$, where

$$\begin{array}{rcl} F(0) & = & \mathbf{TC}(A \cup \mathbb{P}) \cup \omega \cup \{A, \mathbb{P}\} \\ F(n+1) & = & \{b \times \mathbb{P} : \; b \in \bigcup_{k\leq n} F(k)\}. \end{array}$$

Then $B \in M$. Let $Z = (H(B))^M$. Then $A \in Z$. First, we show by induction on n that $F(n) \subseteq Z$. As $F(0)$ is transitive, $F(0) \subseteq Z$ follows from Lemma 11.27, (i). Now suppose $\bigcup_{k\leq n} F(k) \subseteq Z$. An element of $F(n+1)$ is of the form $b \times \mathbb{P}$ with $b \in \bigcup_{k\leq n} F(k)$. If $x \in b$ and $p \in \mathbb{P}$ then $x, p \in Z$, and thus $\langle x, p\rangle \in Z$ by Lemma 11.27 since $2 \in B$. So, letting id be the identity function on $b \times \mathbb{P}$, we get $id : b \times \mathbb{P} \to Z$, and hence $\mathbf{ran}(id) = b \times \mathbb{P} \in Z$. Consequently we have $F(n+1) \subseteq Z$. It follows that $B \subseteq Z$.

We claim that

$$M \models Z \textit{ is a small collection family.} \tag{23}$$

To verify this, suppose that $x \in Z$ and $R \in M$ is a multi-valued function on x. x being an element of $\in (H(B))^M$, there exists a function $f \in M$ and $a \in B$ such that $f : a \to x$ and $\mathbf{ran}(f) = x$. As $M[G]$ is a model of **AC**, we may pick a function $\ell \in M[G]$ such that $\mathbf{dom}(\ell) = x$ and $\forall v \in x \; uR\ell(v)$. We may assume $x \neq \emptyset$. So let $v_0 \in x$ and pick d_0 such that $v_0 R d_0$. Let $\ddot{\ell}$ be a name for ℓ in the forcing language. For any $z \in M$ let $\check{z}$ be the canonical name for z in the forcing language. Define $\chi : \; a \times \mathbb{P} \to M$ by

$$\chi(u,p) := \begin{cases} w & \text{iff } f(u)Rw \text{ and} \\ & \quad p \Vdash [\ddot{\ell} \text{ is a function } \wedge \; \ddot{\ell}(\check{f}(\check{u})) = \check{w}] \\ d_0 & \text{otherwise.} \end{cases}$$

For each $u \in a$, there is a $w \in Z$ such that $f(u)Rw$ and $\ell(f(u)) = w$, and then there is a $p \in G$ that forces that $\ddot{\ell}$ is a function and $\ddot{\ell}(\check{f}(\check{u})) = \check{w}$, so w is in the range of χ. χ is a function with domain $a \times \mathbb{P}$, $\chi \in M$, and $\mathbf{ran}(\chi) \subseteq \mathbf{ran}(R)$. Note that $a \times \mathbb{P} \in B$, and thus we have $a \times \mathbb{P} \in Z$. As a result, with $C = \mathbf{ran}(\chi)$ we have $\forall v \in x \, \exists y \in C \; vRy \;\wedge\; \forall y \in C \, \exists v \in x \; vRy$, confirming the claim. $\square$

From the previous theorem and results in [12] it follows that **AMC** and **REA** are satisfied in all permutation models and symmetric models. A *permutation model* (cf. [38], chapter 4) is specified by giving a model V of **ZFC** with atoms in which the atoms form a set A, a group $\mathcal{G}$ of permutations of A, and a normal filter $\mathcal{F}$ of subgroups of $\mathcal{G}$. The permutation model then consists of the hereditarily symmetric elements of V.

A *symmetric model* (cf. [38], chapter 5), is specified by giving a ground model M of **ZFC**, a complete Boolean algebra B in M, an M-generic filter G in B, a group $\mathcal{G}$ of automorphisms of B, and a normal filter of subgroups of $\mathcal{G}$. The symmetric model consists of the elements of $M[G]$ that hereditarily have symmetric names.

If B is a set then HOD(B) denotes the class of sets hereditarily ordinal definable over B.

Corollary: 11.29 *The usual models of set theory without choice satisfy* **AMC** *and* **REA***. More precisely, every permutation model and symmetric model satisfies* **AMC** *and* **REA***. Furthermore, if V is a universe that satisfies* **ZF***, then for every transitive set $A \in V$ and any set $B \in V$ the submodels $L(A)$ and $HOD(B)$ satisfy* **AMC** *and* **REA***.*

Proof: This follows from Theorem 11.28 in conjunction with [12], Theorems 4.2, 4.3, 4.4, 4.5. $\square$

Corollary: 11.30 *On the basis of* **ZF***,* **AMC** *and* **REA** *do not imply the countable axiom of choice,* $\mathbf{AC}_\omega$*, and* **DC***. Moreover,* **AMC** *and* **REA** *do not imply any of the mathematical consequences of* **AC** *of [38], chapter 10. Among those consequences are the existence of a basis for any vector space and the existence of the algebraic closure of any field.*

Proof: This follows from Corollary 11.28 and [38], chapter 10. $\square$

12 Principles that ought to be avoided in CZF

In the previous section we saw that the unrestricted Axiom of Choice implies undesirable form of excluded middle. There are several other well known principles provable in classical set theory which also imply versions of excluded middle. Among them are the Foundation Axiom and Linearity of Ordinals.

Foundation Schema: $\exists x\phi(x) \rightarrow \exists x[\phi(x) \wedge \forall y \in x \neg\phi(y)]$ for all formulae ϕ.

Foundation Axiom: $\forall x\,[\exists y(y \in x) \rightarrow \exists y(y \in x \wedge \forall z \in y\, z \notin x)]$.

Linearity of Ordinals We shall conceive of *ordinals* as transitive sets whose elements are transitive too.

Let *Linearity of Ordinals* be the statement formalizing that for any two ordinals α and β the following trichotomy holds: $\alpha \in \beta \vee \alpha = \beta \vee \beta \in \alpha$.

Proposition: 12.1 *(i)* **CZF** + Foundation Schema = **ZF**.

(ii) **CZF** + Separation + Foundation Axiom = **ZF**.

(iii) **CZF** + Foundation Axiom $\vdash$ **REM**.

(iv) **CZF** + Foundation Axiom $\vdash$ Powerset.

(v) *The strength of* **CZF**+Foundation Axiom *exceeds that of classical type theory with extensionality.*

Proof: (i): For an arbitrary formula ϕ, consider

$$S_\phi := \{x \in \omega : x = \mathbf{1} \vee [x = \mathbf{0} \wedge \phi]\}.$$

We have $\mathbf{1} \in S_\phi$. By the Foundation Schema, there exists $x_0 \in S_\phi$ such that $\forall y \in x_0\, y \notin S_\phi$. By definition of S_ϕ, we then have

$$x_0 = \mathbf{1} \vee [x_0 = \mathbf{0} \wedge \phi].$$

If $x_0 = \mathbf{1}$, then $\mathbf{0} \notin S_\phi$, and hence $\neg\phi$. Otherwise we have $x_0 = \mathbf{0} \wedge \phi$; thus ϕ.

So we have shown **EM**, from which (i) ensues.

(ii): With full Separation S_ϕ is a set, and therefore the Foundation Axiom suffices for the previous proof.

(iii): For restricted ϕ, S_ϕ is a set be Restricted Separation, and thus $\phi \vee \neg\phi$ follows as in the proof of (i).

(iv) follows from (iii) and Proposition 10.1,(i).

(v) follows from (iii) and Proposition 10.1,(ii). $\square$

Proposition: 12.2 *(i)* **CZF** + "Linearity of Ordinals" $\vdash$ Powerset.

(ii) **CZF** + "Linearity of Ordinals" $\vdash$ **REM**.

(iii) **CZF** + "Linearity of Ordinals" + Separation = **ZF**.

Proof: (i): Note that $\mathbf{1}$ is an ordinal. If $u \subseteq \mathbf{1}$, then u is also an ordinal because of $\forall z \in u\, z = \mathbf{0}$. Furthermore, one readily shows that $\mathbf{2}$ is an ordinal. Thus, by Linearity of Ordinals,

$$\forall u \subseteq \mathbf{1}\, [u \in \mathbf{2} \vee u = \mathbf{2} \vee \mathbf{2} \in u].$$

The latter, however, condenses to $\forall u \subseteq \mathbf{1}\, [u \in \mathbf{2}]$. As a consequence we have,

$$\mathcal{P}(\mathbf{1}) = \{u \in \mathbf{2} : u \subseteq \mathbf{1}\},$$

and thus $\mathcal{P}(\mathbf{1})$ is a set. Whence, proceeding onwards as in the proof of Proposition 10.1,(i), we get Powerset.

(ii): Let ϕ be restricted. Put

$$\alpha := \{n \in \omega : n = \mathbf{0} \wedge \phi\}.$$

α is a set by Restricted Separation, and α is an ordinal as $\alpha \subseteq \mathbf{1}$. Now, by Linearity of Ordinals, we get

$$\alpha \in \mathbf{1} \ \vee \ \alpha = \mathbf{1}.$$

In the first case, we obtain $\alpha = \mathbf{0}$, which implies $\neg\phi$ by definition of α. If $\alpha = \mathbf{1}$, then ϕ. Therefore, $\phi \vee \neg\phi$.

(iii): Here $\alpha := \{n \in \omega : n = \mathbf{0} \wedge \phi\}$ is a set by Separation. Thus the remainder of the proof of (ii) provides $\phi \vee \neg\phi$. $\square$

13 Inductive Definitions

In this chapter Strong Infinity will not play a role. So we let $\mathbf{ECST}'$ be $\mathbf{ECST}-Strong\ Infinity$. We will also let $\mathbf{CZF}'$ be $\mathbf{ECST}'+Set\ Induction+Strong\ Collection$, or alternatively it is $\mathbf{CZF}-Infinity-Subset\ Collection$.

We will think of an inductive definition as a generalized notion of axiom system. We may characterize a (finitary) axiom system as follows. There are objects, which we will call the statements of the axiom system, and there are axioms and rules of inference. Each axiom is a statement and each rule of inference has instances that consist of finitely many premisses and a conclusion, both the premisses and conclusion being statements. So we may think of an instance of a rule of inference as an inference step X/a where X is the finite set of premisses and a is the conclusion. It is also convenient to think of each axiom a as such a step where the set X of premisses is empty. The theorems of an axiom system may be characterized as the smallest set of statements that include all the axioms and are closed under the rules of inference. Here, a set of statements is closed under a rule if, for each instance of the rule, if the premisses are in the set then so is the conclusion. If we let Φ be the set of steps determined by the axioms and the instances of the rules then we may characterize the set of theorems as the smallest set of statements such that for every step in Φ, if the premisses are in the set then so is the conclusion. Our generalization is to allow any objects to be statements and to start from an arbitrary class of steps, with each step having a set of premisses that need not be finite. So we are led to the following definitions.

13.1 Inductive Definitions of Classes

We define an *inductive definition* to be a class of ordered pairs. If Φ is an inductive definition and $(X, a) \in \Phi$ then we prefer to write $X/a \in \Phi$ and call X/a an *(inference) step* of Φ, with set X of *premisses* and *conclusion* a.

We associate with an inductive definition Φ the operator Γ on classes that assigns to each class Y the class $\Gamma(Y)$ of all conclusions a of inference steps X/a of Φ, with set X of premisses that is a subset of Y. We define a class Y to be Φ-*closed* if $\Gamma(Y) \subseteq Y$.

The class *inductively defined by* Φ is the smallest Φ-closed class if this exists. The main result of this section states that indeed this class $I(\Phi)$ does always exists.

Theorem: 13.1 (Class Inductive Definition Theorem) ($\mathbf{CZF}'$) *For any inductive definition Φ there is a smallest Φ-closed class $I(\Phi)$.*

The Proof

The proof involves the iteration of the class operator Γ until it closes up at its least fixed point which turns out to be the required class $I(\Phi)$. Note that Γ is monotone; i.e. for classes Y_1, Y_2

$$Y_1 \subseteq Y_2 \Rightarrow \Gamma(Y_1) \subseteq \Gamma(Y_2).$$

As an inductive definition need not be finitary; i.e. it can have steps with infinitely many premisses, we will need transfinite iterations of Γ in general. In classical set theory it is customary to use ordinal numbers to index iterations. Here it is unnecessary to develop a theory of ordinal numbers and we simply use sets to index iterations. This is not a problem as we can carry out proofs by set induction. The following result gives us the iterations we want. Call a class J of ordered pairs an *iteration class for* Φ if for each set a,

$$J^a = \Gamma(J^{\in a})$$

where $J^a = \{x \mid (a, x) \in J\}$ and $J^{\in a} = \bigcup_{x \in a} J^x$.

Lemma: 13.2 (**CZF**$'$) *Every inductive definition has an iteration class.*

Proof: Call a set G of ordered pairs *good* if

$$(*) \qquad\qquad (a, y) \in G \Rightarrow y \in \Gamma(G^{\in a}).$$

where

$$G^{\in a} = \{y' \mid \exists x \in a\ (x, y') \in G\},$$

Let $J = \bigcup\{G \mid G \text{ is good}\}$. We must show that for each a

$$J^a = \Gamma(J^{\in a}).$$

First, let $y \in J^a$. Then $(a, y) \in G$ for some good set G and hence by $(*)$, above, $y \in \Gamma(G^{\in a})$. As $G^{\in a} \subseteq J^{\in a}$ it follows that $y \in \Gamma(J^{\in a})$. Thus $J^a \subseteq \Gamma(J^{\in a})$.

For the converse inclusion let $y \in \Gamma(J^{\in a})$. Then $Y/y \in \Phi$ for some set $Y \subseteq J^{\in a}$. It follows that $\forall y' \in Y \exists x \in a\ y' \in J^x$ so that

$$\forall y' \in Y \exists G\ [\ G \text{ is good and } y' \in G^{\in a}].$$

By Strong Collection there is a set Z of good sets such that

$$\forall y' \in Y\ \exists G \in Z\ y' \in G^{\in a}.$$

Let $G = \{(a, y)\} \cup \bigcup Z$. Then $\bigcup Z$ is good and, as $Y/y \in \Phi$ and $Y \subseteq G^{\in a}$, G is good. As $(a, y) \in G$ we get that $y \in J^a$. Thus $\Gamma(J^{\in a}) \subseteq J^a$. $\square$

Proof of the theorem: It only remains to show that

$$J^\infty = \bigcup_{a \in V} J^a$$

is the smallest Φ-closed class. To show that J^∞ is Φ-closed let $Y/y \in \Phi$ for some set $Y \subseteq J^\infty$. Then $\forall y' \in Y \exists x\, y' \in J^x$. So, by Collection, there is a set a such that

$$\forall y' \in Y \exists x \in a\; y' \in J^x;$$

i.e. $Y \subseteq J^{\in a}$. Hence $y \in \Gamma(J^{\in a}) = J^a \subseteq J^\infty$. Thus J^∞ is Φ-closed.

Now let I be a Φ-closed class. We show that $J^\infty \subseteq I$. It suffices to show that $J^a \subseteq I$ for all a. We do this by Set Induction on a. So we may assume, as induction hypothesis, that $J^x \subseteq I$ for all $x \in a$. It follows that $J^{\in a} \subseteq I$ and hence

$$J^a = \Gamma(J^{\in a}) \subseteq \Gamma(I) \subseteq I,$$

the inclusions holding because Γ is monotone and I is Φ-closed. $\square$

Examples

Let A be a class.

1. $H(A)$ is the smallest class X such that for each set a that is an image of a set in A

   $$a \in Pow(X) \Rightarrow a \in X.$$

   Note that $H(A) = I(\Phi)$ where Φ is the class of all pairs (a, a) such that a is an image of a set in A.

2. If R is a subclass of $A \times A$ such that $R_a = \{x \mid xRa\}$ is a set for each $a \in A$ then $Wf(A, R)$ is the smallest subclass X of A such that

   $$\forall a \in A\, [R_a \subseteq X \Rightarrow a \in X].$$

   Note that $Wf(A, R) = I(\Phi)$ where Φ is the class of all pairs (R_a, a) such that $a \in A$.

3. If B_a is a set for each $a \in A$ then $W_{a \in A} B_a$ is the smallest class X such that
$$a \in A \;\&\; f : B_a \to X \;\Rightarrow\; (a, f) \in X.$$
Note that $W_{x \in A} B_a = I(\Phi)$ where Φ is the class of all pairs $(ran(f), (a, f))$ such that $a \in A$ and $f : B_a \to V$.

Call an inductive definition Φ *local* if $\Gamma(X)$ is a set for all sets X. For a local inductive definition Lemma 13.2 can be improved without any need to use Strong Collection. Note that if Φ is a set then Φ is local, so that the above examples $H(A), Wf(A, R)$ and $W_{x \in A} B_a$ of inductive definitions are all local when A is a set.

Lemma: 13.3 (**ECST** + *Set Induction*) *A local inductive definition has an iteration class J such that J^a and $J^{\in a}$ are sets for each set a.*

Proof: Given a local inductive definition Φ we can apply Proposition 9.13 to define by transfinite set recursion $F : V \to V$ such that, for each set a,
$$F(a) = \Gamma(\bigcup_{x \in a} F(x)).$$
Then $J = \{(a, x) \mid a \in V \;\&\; x \in F(a)\}$ is the desired iteration class. □

Note that as before we can define $J^\infty = \bigcup_{a \in V} J^a$ and show, using Collection that it is the smallest Φ-closed class $I(\Phi)$, and Strong Collection has been avoided. So only Collection is needed to prove the theorem for local inductive definitions.

13.2 Inductive definitions of Sets

We define a class B to be a *bound* for Φ if whenever $X/a \in \Phi$ then X is an image of a set $b \in B$; i.e. there is a function from b onto X. We define Φ to be *bounded* if

1. $\{y \mid X/y \in \Phi\}$ is a set for all sets X,

2. Φ has a bound that is a set.

Note that if Φ is a set then it is bounded.

Proposition: 13.4 (**ECST′** + **EXP**) *Every bounded inductive definition Φ is local; i.e. $\Gamma(X)$ is a set for each set X.*

Proof: Let B be a bound for Φ. If $Y/y \in \Phi$ then for some $b \in B$ there is a surjective $f : b \to Y$. So if X is a set then

$$\Gamma(X) = \bigcup_{f \in C} \{y \mid ran(f)/y \in \Phi\}$$

where $C = \bigcup_{b \in B} {}^b X$. By Exponentiation and Union-Replacement C is a set. As Φ is bounded $\{y \mid ran(f)/y \in \Phi\}$ is always a set, so that, by Union-Replacement $\Gamma(X)$ is a set. $\square$

The following result does not seem to need any form of Collection.

Theorem: 13.5 (**ECST**$'$ + *Set Induction*) *If Φ is a bounded local inductive definition, with a weakly regular set bound, then there is a smallest Φ-closed class $I(\Phi)$ which is a set.*

Proof: Let A be a weakly regular bound for Φ. Then, as Φ is local, we may apply Lemma 13.3 to get that $J^{\in A}$ is a set, where J is the iteration class for Φ. As $J^{\in A} \subseteq Y$ for any Φ-closed class Y it suffices to show that $J^{\in A}$ is Φ-closed.

So let $X/x \in \Phi$ with X a subset of $J^{\in A}$. Then, as A is a bound for Φ, there is $Z \in A$ and surjective $f : Z \to X$. So $\forall z \in Z\ f(z) \in J^{\in A}$ and hence $\forall z \in Z \exists a \in A\ f(z) \in J^a$. As A is a weakly regular set and $Z \in A$ there is $b \in A$ such that $\forall z \in Z \exists a \in b\ f(z) \in J^a$. Hence $X \subseteq \bigcup_{a \in b} J^a$ so that $x \in \Gamma(\bigcup_{a \in b} J^a) = J^b \subseteq J^{\in A}$. $\square$

Corollary: 13.6 (**ECST**$'$ + *Set Induction*) *If Φ is an inductive definition that is a subset of a weakly regular set then $I(\Phi)$ is a set.*

Combining Proposition 13.4 and Theorem 13.5 we get the following result.

Theorem: 13.7 (Set Induction Theorem) (**ECST**$'$+**EXP**+*Set Induction*+**wREA**) *If Φ is a bounded inductive definition then it is local and there is a smallest Φ-closed class $I(\Phi)$ which is a set.*

Corollary: 13.8 (**ECST**$'$ + **EXP** + *Set Induction* + **wREA**) *If A is a set then*

1. *$H(A)$ is a set,*
2. *if $R \subseteq A \times A$ such that $R_a = \{x \mid xRa\}$ is a set for each $a \in A$ then $Wf(A, R)$ is a set.*
3. *if B_a is a set for each $a \in A$ then $W_{a \in A} B_a$ is a set.*

13.3 Tree Proofs

We will give a characterisation of $I(\Phi)$ in terms of a suitable notion of tree proof. These will be well-founded trees, each given as a pair (a, Z), where a is the conclusion of the proof and Z is the set of proofs of the premisses of the final inference step X/a of the proof. We will call these trees *proto-proofs.* We will associate with each proto-proof p the set $Steps(p)$ of the inference steps that it uses. Then a proto-proof $p = (a, Z)$ will be a proof that $a \in I(\Phi)$ provided that $Steps(p) \subseteq \Phi$.

Definition: 13.9 *The class $\mathbb{P}$ of proto-proofs is inductively defined to be the smallest class such that, for all pairs $p = (a, Z)$, if $Z \subseteq \mathbb{P}$ then $p \in \mathbb{P}$; i.e. $\mathbb{P} = I(\Psi)$, where Ψ is the class of steps Z/p for pairs $p = (a, Z)$.*

In order to introduce the *Steps* operation we need some definitions.

Definition: 13.10 *Let $concl : V^2 \to V$, $Concl : Pow(V^2) \to V$ and $endstep : V \times Pow(V^2) \to V$ be given by*

$$\begin{array}{ll} concl(p) & = a \\ Concl(Z) & = \{concl(q) \mid q \in Z\} \\ endstep(p) & = (Concl(Z), a) \end{array}$$

for all pairs $p = (a, Z)$.

Lemma: 13.11 *There is a unique class function $Steps : \mathbb{P} \to Pow(Pow(V) \times V)$ such that, for $p = (a, Z) \in \mathbb{P}$,*

$$(*) \quad Steps(p) = \{endstep(p)\} \cup \bigcup\{Steps(q) \mid q \in Z\}.$$

Proof: Let SS be the class inductively defined to be the smallest class such that, for $p = (a, Z) \in \mathbb{P}$,

1. $(endstep(p), p) \in \mathsf{SS}$, and
2. if $(r, q) \in \mathsf{SS}$ for some $q \in Z$ then $(r, p) \in \mathsf{SS}$.

Let $Steps(p)$ be the class $\{r \mid (r, p) \in \mathsf{SS}\}$ for each $p \in \mathbb{P}$. Then $(*)$ is easily checked and then, by induction following the inductive definition of $\mathbb{P}$, we get that $Steps(p)$ is a set in $Pow(Pow(V) \times V)$ for all $p \in \mathbb{P}$. Also if $Steps' : V \to Pow(Pow(V) \times V)$ also satisfies $(*)$ for all $p \in \mathbb{P}$ then, again by induction following the inductive definition of $\mathbb{P}$ it is easy to check that $Steps'(p) = Steps(p)$ for all $p \in \mathbb{P}$. $\square$

Definition: 13.12 *For each inductive definition* Φ *we define the class* $\mathbb{P}(\Phi)$ *of* Φ-proofs *as follows.*

$$\mathbb{P}(\Phi) = \{p \in \mathbb{P} \mid Steps(p) \subseteq \Phi\}.$$

Theorem: 13.13 (CZF′) *For each inductive definition* Φ

$$I(\Phi) = I'$$

where $I' = \{concl(p) \mid p \in \mathbb{P}(\Phi)\}$.

Proof: The theorem will follow from the following two claims.

Claim 1 $concl(p) \in I(steps(p))$ for all $p \in \mathbb{P}$.

Claim 2 I' is Φ-closed.

For, by Claim 2, $I(\Phi) \subseteq I'$. For the converse inclusion, let $a \in I'$. Then $a = concl(p)$ for some $p \in \mathbb{P}(\Phi)$ and, by Claim 1, $concl(p) \in I(steps(p)) \subseteq I(\Phi)$, so that $a \in I(\Phi)$. It remains to prove the two claims. □

Proof of Claim 1: It suffices to show that

$$\mathbb{P}' = \{p \in \mathbb{P} \mid concl(p) \in I(Steps(p))\}$$

is Ψ-closed. So let $Z/p \in \Psi$, with $Z \subseteq \mathbb{P}'$, to show that $p \in \mathbb{P}'$. We have

$$p = (a, Z) = (concl(p), Z)$$

for some $a \in V$. As $Z \subseteq \mathbb{P}'$, if $q \in Z$ then

$$concl(q) \in I(Steps(q)) \text{ and } Steps(q) \subseteq Steps(p),$$

so that $concl(q) \in I(Steps(p))$. It follows that

$$\begin{array}{rcll} b \in Concl(Z) & \Rightarrow & b = concl(q) & \text{for some } q \in Z \\ & \Rightarrow & b \in I(Steps(p), & \end{array}$$

and hence $Concl(Z) \subseteq I(Steps(p))$ so that, as

$$Concl(Z)/concl(p) \in Steps(p),$$

$p \in \mathbb{P}'$. □

Proof of Claim 2: Let $X/a \in \Phi$ with $X \subseteq I'$. We must show that $a \in I'$. As $X \subseteq I'$,

$$(\forall b \in X)(\exists q \in \mathbb{P}(\Phi))\ b = concl(q).$$

By Strong Collection there is a set $Z \subseteq \mathbb{P}(\Phi) \subseteq \mathbb{P}$ such that

$$(\forall b \in X)(\exists q \in Z)\ b = concl(q) \text{ and } (\forall q \in Z)\ concl(q) \in X.$$

It follows that $Concl(Z) = X$. Let $p = (a, Z)$. We have $p \in \mathbb{P}$, as $Z \in Pow(\mathbb{P})$, and

$$Steps(p) = \{(Concl(Z), a)\} \cup \bigcup \{Steps(q) \mid q \in Z\}.$$

So $(Concl(Z), a) = (X, a) \in \Phi$ and if $q \in Z$ then $q \in \mathbb{P}(\Phi)$ so that $Steps(q) \subseteq \Phi$. Hence $Steps(p) \subseteq \Phi$ so that $p \in \mathbb{P}(\Phi)$. We conclude that $a = concl(p) \in I'$. □

Corollary: 13.14 (CZF′) *If $a \in I(\Phi)$ then $a \in I(\Phi_0)$ for some set $\Phi_0 \subseteq \Phi$.*

We can relativise Theorem 13.13 to a regular set.

Theorem: 13.15 (CZF′) *Let A be a regular set such that $2 \in A$. Then, for each class $\Phi \subseteq A \times A$,*

$$I(\Phi) = I_A(\Phi),$$

where $I_A(\Phi) = \{concl(p) \mid p \in \mathbb{P}(\Phi) \cap A\}$.

Proof: Trivially $I_A(\Phi) \subseteq I(\Phi)$ by Theorem 13.13. To show that $I(\Phi) \subseteq I_A(\Phi)$ it suffices to show that $I_A(\Phi)$ is Φ-closed. We argue as in the proof of Theorem 13.13 using our assumption that A is regular instead of Strong Collection. So let $X/a \in \Phi$ with $X \subseteq I_A(\Phi)$. We must show that $a \in I_A(\Phi)$. As $(X, a) \in \Phi \subseteq A \times A$ we have $X, a \in A$. As $X \subseteq I_A(\Phi)$,

$$(\forall b \in X)(\exists q \in A)[q \in \mathbb{P}(\Phi)\ \&\ b = concl(q)].$$

As $X \in A$ and A is regular there is $Z \in A$ such that $Z \subseteq \mathbb{P}(\Phi)$ and

$$(\forall b \in X)(\exists q \in Z)[b = concl(q)] \text{ and } (\forall q \in Z)[concl(q) \in X].$$

So $Concl(Z) = X$ and if $p = (a, Z)$ then $p \in \mathbb{P} \cap A$ and

$$Steps(p) = \{(X, a)\} \cup \bigcup \{Steps(q) \mid q \in Z\} \subseteq \Phi$$

so that $a = concl(p) \in I_A(\Phi)$. □

13.4 The Set Compactness Theorem

Our aim is to prove the following result.

Theorem: 13.16 ($\mathbf{CZF}' + \mathbf{REA}$) (Set Compactness) *For each set S and each set $P \subseteq Pow(S)$ there is a set B of subsets of $P \times S$ such that, for each class $\Phi \subseteq P \times S$,*

$$a \in I(\Phi) \iff a \in I(\Phi_0) \textit{ for some } \Phi_0 \in B \textit{ such that } \Phi_0 \subseteq \Phi.$$

Proof: Use **REA** to choose a regular set A such that $\{2\} \cup S \cup P \subseteq A$. Let $\Phi \subseteq P \times S$. By Theorem 13.15, $I(\Phi) = I_A(\Phi)$. Let B be the class $\{Steps(p) \cap (P \times S) \mid p \in \mathbb{P} \cap A\}$. Observe that

$$\begin{array}{rcl} a \in I(\Phi) & \Leftrightarrow & a = concl(p) \text{ for some } p \in \mathbb{P}(\Phi) \cap A \\ & \Leftrightarrow & a \in I(steps(p)) \text{ for some } p \in \mathbb{P}(\Phi) \cap A \\ & \Leftrightarrow & a \in I(\Phi_0) \text{ for some } \Phi_0 \in B \text{ such that } \Phi_0 \subseteq \Phi \end{array}$$

So it suffices to show that $\mathbb{P} \cap A$ is a set, as then B is a set, by Replacement. Let $\mathbb{P}_A = I(\Psi_A)$, where $\Psi_A = \Psi \cap (A \times A)$. As Ψ_A is a set so is $\mathbb{P}_A$, by Corollary 13.6. So it suffices to show that $\mathbb{P} \cap A = \mathbb{P}_A$. Trivially $\mathbb{P}_A \subseteq \mathbb{P} \cap A$. To show that $\mathbb{P} \cap A \subseteq \mathbb{P}_A$ it suffices to show that $\mathbb{P} \subseteq Y$, where $Y = \{p \mid p \in A \Rightarrow p \in \mathbb{P}_A\}$ and, for that, it suffices to show that Y is Ψ-closed; i.e. that, for $p = (a, Z)$, if $Z \subseteq Y$ then $p \in Y$.

So let $p = (a, Z)$ with $Z \subseteq Y$; i.e. $Z \cap A \subseteq \mathbb{P}_A$. To show that $p \in Y$ let $p \in A$. Then $a, Z \in A$ so that $Z \subseteq A$ and hence $Z = Z \cap A \subseteq \mathbb{P}_A$ so that $p \in \mathbb{P}_A$. Thus $p \in Y$ as required. $\square$

We may relativise the notion of theorem for an axiom system to a set X of assumptions treated as additional axioms. The set of theorems relative to X is then the smallest set of statements of the axiom system that include the axioms, are closed under the rules of inference and also include the assumptions from X. We generalise this idea to inductive definitions. Given a class X, let $I(\Phi, X)$ be the smallest Φ-closed class that has X as a subclass. This exists as it can be defined as $I(\Phi_X)$ where

$$\Phi_X = \Phi \cup (\{\emptyset\} \times X).$$

We can apply Corollary 13.14 to get the following result.

Proposition: 13.17 ($\mathbf{CZF}'$) *For each inductive definition Φ and each class X*

$$a \in I(\Phi, X) \iff a \in I(\Phi, X_0) \textit{ for some set } X_0 \subseteq X.$$

We get the following corollary of the theorem.

Corollary: 13.18 ($\mathbf{CZF'} + \mathbf{REA}$) *If Φ is a subset of $Pow(S) \times S$, where S is a set then there is a set B of subsets of S such that for each class $X \subseteq S$*

$$a \in I(\Phi, X) \iff a \in I(\Phi, X_0) \text{ for some } X_0 \in B \text{ such that } X_0 \subseteq X.$$

13.5 Closure Operations on a po-class

Given a class A a *partial ordering* of A is a subclass $\leq$ of $A \times A$ satisfying the standard axioms for a partial ordering; i.e.

1. $a \leq a$ for all $a \in A$,
2. $[a \leq b \wedge b \leq c] \rightarrow a \leq c$,
3. $[a \leq b \wedge b \leq a] \rightarrow a = b$,

A *po-class* is a class A with a partial ordering $\leq$.
Let A be a po-class. Then $f : A \rightarrow A$ is *monotone* if

$$x \leq y \rightarrow f(x) \leq f(y).$$

We define $c : A \rightarrow A$ to be a *closure operation* on A if it is monotone and for all $a \in A$

$$a \leq c(c(a)) \leq c(a).$$

Note that, for a closure operation c on A, if $a \in A$ then

$$c(a) \leq a \;\leftrightarrow\; c(a) = a \;\leftrightarrow\; \exists y \in A[a = c(y)].$$

We call a subclass C of A a *closure class* on A if for each $a \in A$ there is $\overline{a} \in C$ such that

1. $a \leq \overline{a}$,
2. $a \leq y \rightarrow \overline{a} \leq y$ for all $y \in C$.

Proposition: 13.19 *There is a one-one correspondence between closure operations and closure classes on a po-class A. To each closure operation $c : A \rightarrow A$ there corresponds the closure class $C = \{a \mid c(a) = a\}$ of fixed points of c. Conversely to each closure class C there corresponds the closure operation c which associates with each $a \in A$ the unique $\overline{a} \in C$ satisfying 1,2 above. These correspondences are inverses of each other.*

Example: Let A be a set. Then $Pow(A)$ is a class that is a po-class, when partially ordered by the subset relation on $Pow(A)$.

Let Φ be an inductive definition that is a subset of $Pow(A) \times A$. We call Φ an *inductive definition on* A. Let

$$C_\Phi = \{X \in Pow(A) \mid X \text{ is } \Phi\text{-closed}\}.$$

Then C_Φ is a closure class on $Pow(A)$ whose associated closure operation $c_\Phi : Pow(A) \to Pow(A)$ can be given by

$$c_\Phi(X) = I(\Phi, X)$$

for all sets $X \subseteq A$.

Which closure operations arise in this way? Call a monotone operation $f : Pow(A) \to Pow(A)$ *set-based* if there is a subset B of $Pow(A)$ such that whenever $a \in f(X)$, with $X \in Pow(A)$, then there is $Y \in B$ such that $Y \subseteq X$ and $a \in f(Y)$. We call B a *baseset* for f.

Theorem: 13.20 *Let $c : Pow(A) \to Pow(A)$, where A is a set. Then $c = c_\Phi$ for some inductive definition Φ on A if and only if c is a set-based closure operation on $Pow(A)$.*

Proof: Let $c = c_\Phi$, where Φ is an inductive definition on the set A. That c is a closure operator is an easy consequence of its definition. That it is set-based is the content of Corollary 13.18. For the converse, let c be a set based closure operator on $Pow(A)$, with baseset B and associated closure class C. Let Φ be the set of all pairs (Y, a) such that $Y \in B$ and $a \in c(Y)$. This is a set by Union-Replacement, as $B = \bigcup_{Y \in B}(\{Y\} \times c(Y))$. It is clearly an inductive definition on A. It is easy to check that for any set $X \subseteq A$ X is Φ-closed if and only if $X \in C$, which will give us the desired result that $c = c_\Phi$. $\square$

14 Coinduction

14.1 Coinduction of Classes

Definition: 14.1 (Relation Reflection Scheme, RRS) *For classes S, R with $R \subseteq S \times S$, if $a \in S$ and $\forall x \in S \exists y \in S\ xRy$ then there is a set $S_0 \subseteq S$ such that $a \in S_0$ and $\forall x \in S_0 \exists y \in S_0\ xRy$.*

Proposition: 14.2 (ECST)

1. **RDC** *implies* **RRS**.
2. **RRS** *implies* **FRS**.

Let Φ be an inductive definition on a class S; i.e. Φ is a subclass of $Pow(S) \times S$. For each $a \in S$ let $\Phi_a = \{X \mid (X, a) \in \Phi\}$. For each subclass B of S let

$$\Gamma B = \{a \in S \mid \exists X \in \Phi_a\ X \subseteq B\}.$$

We call B Φ-*inclusive* if $B \subseteq \Gamma B$.

Theorem: 14.3 ($\mathbf{CZF}^- + \mathbf{RRS}$) $\bigcup\{X \in Pow(S) \mid X \subseteq \Gamma X\}$ *is the largest Φ-inclusive class.*

Proof: Let $J = \bigcup\{X \in Pow(S) \mid X \subseteq \Gamma X\}$. First observe that $J \subseteq \Gamma J$. For if $a \in J$ then $a \in X \subseteq \Gamma X$ for some set $X \subseteq J$ so that $a \in \Gamma J$, as Γ is monotone. It remains to show that if $B \subseteq \Gamma B$ then $B \subseteq J$. So let $a \in B$ to show that $a \in J$.

Let $A = Pow(B)$. If $X \in A$ then $X \subseteq \Gamma B$; i.e.

$$\forall x \in X \exists y [y \in A \ \&\ (y, x) \in \Phi].$$

So, by Strong Collection, there is a set Y such that

$$\forall x \in X \exists y \in Y [y \in A \ \&\ (y, x) \in \Phi]$$

and

$$\forall y \in Y \exists x \in X [y \in A \ \&\ (y, x) \in \Phi].$$

Now let $Z = \cup Y$. Then $Z \in A$ and $X \subseteq \Gamma Z$. Thus

$$\forall X \in A \exists Z \in A [X \subseteq \Gamma Z].$$

By **RRS** there is a set $A_0 \subseteq A$ such that $\{a\} \in A_0$ and

$$\forall X \in A_0 \exists Z \in A_0 [X \subseteq \Gamma Z].$$

Let $W = \cup A_0 \in Pow(S)$. Then $a \in W \subseteq \Gamma W$ so that $a \in J$.

$\square$

For each subclass B of S let

$$\Delta B = \{a \in S \mid \forall X \in \Phi_a \ X \between B\},$$

where $X \between B$ if $X \cap B$ is inhabited. We call B *Φ-progressive* if $B \subseteq \Delta B$.

Lemma: 14.4 (CZF$^-$) *If Φ_a is a set for all $a \in S$ then, for each subclass B of S,*

$$\Delta B = \{a \in S \mid \exists Y \in \Phi'_a \ Y \subseteq B\},$$

where $\Phi' = \{(Y, a) \in Pow(S) \times S \mid a \in \Delta Y\}$.

Proof: We must show that

$$a \in \Delta B \iff (\exists Y \in Pow(B)) \ a \in \Delta Y.$$

The implication from right to left just uses the monotonicity of Δ. For the other direction let $a \in \Delta B$. Then

$$\forall X \in \Phi_a \exists x [x \in X \ \& \ x \in B]$$

so that, as Φ_a is a set, by Strong Collection there is a set Y such that

$$\forall X \in \Phi_a \exists x \in Y [x \in X \ \& \ x \in B]$$

and

$$\forall x \in Y \exists X \in \Phi_a [x \in X \ \& \ x \in B].$$

Then $Y \in Pow(B)$ and $a \in \Delta Y$ giving the right hand side. $\square$

Theorem: 14.5 (CZF$^-$ + RRS) *If Φ_a is a set for all $a \in S$ then $\bigcup\{X \in Pow(S) \mid X \subseteq \Delta X\}$ is the largest Φ-progressive class.*

Proof: By the lemma B is Φ-progressive iff B is Φ'-inclusive and we can apply the previous theorem to complete the proof. $\square$

14.2 Coinduction of Sets

Here we assume that S, Φ are sets with $\Phi \subseteq Pow(S) \times S$ and prove in a certain extension of **CZF** that the class

$$J = \bigcup\{x \in Pow(S) \mid x \subseteq \Gamma x\}$$

is a set and is the largest Φ-inclusive set. As J is the union of all Φ-inclusive sets it is a Φ-inclusive class that includes all Φ-inclusive sets. So it is only necessary to show that J is a set.

Recall that a regular set A is strongly regular if it is closed under the union operation; i.e. $\forall x \in A \ \bigcup x \in A$. Also **REA**/$\bigcup$**REA** is the axiom that states that every set is a subset of a regular/strongly regular set. We now strengthen these axioms by requiring that the regular/strongly regular set also satisfy the second order version of the Relation Reflection Scheme **RRS**.

Definition: 14.6 *Let A be a regular/strongly regular set. We define it to be* **RRS** regular/**RRS** strongly regular *if also, for all sets $A' \subseteq A$ and $R \subseteq A' \times A'$, if $a_0 \in A'$ and $\forall x \in A' \exists y \in A' \ xRy$ then there is $A_0 \in A$ such that $a_0 \in A_0 \subseteq A'$ and $\forall x \in A_0 \exists y \in A_0 \ xRy$.*

Definition: 14.7 (RRS-REA/RRS-$\bigcup$REA) *Every set is a subset of a* **RRS** *regular/***RRS** *strongly regular set.*

Theorem: 14.8 (CZF+RRS-$\bigcup$REA) *If S, Φ and J are as above then J is a set and is the largest Φ-inclusive set.*

Proof: By **RRS-$\bigcup$REA** there is a **RRS** strongly regular set A such that $S \cup \{\Phi_a \mid a \in S\} \subseteq A$. Recall that Γ was the monotone set continuous operator defined as follows. For each class B

$$\Gamma(B) = \{a \in S \mid \exists X \in \Phi_a \ X \subseteq B\}.$$

Let

$$J_A = \bigcup\{x \in A \cap Pow(S) \mid x \subseteq \Gamma x\}.$$

Then J_A is a set that is a union of Φ-inclusive sets and so is itself a Φ-inclusive set. As $J_A \subseteq J$ it suffices to show that $J \subseteq J_A$.

So let $a_0 \in J$; i.e. $a_0 \in Y$ for some set Y such that $Y \subseteq \Gamma Y$. So

$$\forall a \in Y \ \exists X \in \Phi_a \ X \subseteq Y.$$

Now let $Z \in A'$ where $A' = Pow(Y) \cap A$. Then

$$\forall a \in Z\ \exists X \in A\ [X \in \Phi_a\ \&\ X \subseteq Y].$$

As A is regular there is $Z_0 \in A$ such that

$$\forall a \in Z\ \exists X \in Z_0\ [X \in \Phi_a\ \&\ X \subseteq Y]$$

and

$$\forall X \in Z_0\ \exists a \in Z\ [X \in \Phi_a\ \&\ X \subseteq Y].$$

So $Z_0 \subseteq Pow(Y)$. Let $Z' = \cup Z_0$. Then $Z' \in Pow(Y)$ and

$$\forall a \in Z\ \exists X \in \Phi_a\ X \subseteq Z'.$$

Also, as A is closed under unions, $Z' \in A$ and so $Z' \in A'$.

We have shown that

$$\forall Z \in A'\ \exists Z' \in A'\ Z \subseteq \Gamma Z'.$$

As A is **RRS** regular and $\{a_0\} \in A' \subseteq A$ there is a set $A_0 \in A$ such that $\{a_0\} \in A_0 \subseteq A'$ and

$$\forall Z \in A_0\ \exists Z' \in A_0\ Z \subseteq \Gamma Z'.$$

Let $Y' = \cup A_0 \in A$, using again the assumption that A is closed under unions, and observe that $a_0 \in Y' \subseteq \Gamma Y'$. So $a_0 \in J_A$ and we are done. □

Corollary: 14.9 (CZF+RRS-$\bigcup$REA) *If S, Φ and J are as above then there is a largest Φ-progressive set.*

Proof: Apply Lemma 14.4.

□

15 $\bigvee$-Semilattices

15.1 Set-generated $\bigvee$-Semilattices

Let S be a po-class. If $X \subseteq S$ and $a \in S$ then a is a *supremum* of X if for all $x \in S$

$$\forall y \in X[y \leq x] \;\leftrightarrow\; a \leq x.$$

Note that a supremum is unique if it exists. The supremum of a subclass X of S will be written $\bigvee X$. A po-class is a $\bigvee$*-semilattice* if every subset has a supremum.

Let S be a $\bigvee$-semilattice . A subset G is a *generating set for* S if for every $a \in S$

$$G_a = \{x \in G \mid x \leq a\}$$

is a set and $a = \bigvee G_a$. An $\bigvee$-semilattice is *set-generated* if it has a generating set.

Example: For each set A the po-class $Pow(A)$ is a set-generated $\bigvee$-semilattice with set $G = \{\{a\} \mid a \in A\}$ of generators.

Theorem: 15.1 *Let C be a closure class on an $\bigvee$-semilattice S. Then C is a $\bigvee$-semilattice, when given the partial ordering induced from S. If S is set-generated then so is C. Moreover every set-generated $\bigvee$-semilattice arises in this way from a closure class C on a $\bigvee$-semilattice $Pow(A)$ for some set A.*

Proof: Let c be the closure operator associated with the closure class C on the $\bigvee$-semilattice S. It is easy to check that C has the supremum operation $\bigvee^C$ given by $\bigvee^C X = c(\bigvee X)$ for each subset X of C. Now assume that S has a set G of generators. Let

$$G^C = \{c(x) \mid x \in G\}.$$

We show that G^C is a set of generators for C. For each $a \in C$ let

$$G^C_a = \{y \in G^C \mid y \leq a\}.$$

We must show that G^C_a is a set and $a = \bigvee^C G^C_a$. Observe that

$$\begin{aligned} G^C_a &= \{c(x) \mid x \in G \wedge c(x) \leq a\} \\ &= \{c(x) \mid x \in G \wedge x \leq a\} \\ &= \{c(x) \mid x \in G_a\} \end{aligned}$$

so that G_a^C is a set. Also observe that $\bigvee^C G_a^C = c(\bigvee\{c(x) \mid x \in G_a\})$. It follows first that $a = \bigvee\{x \mid x \in G_a\} \leq \bigvee\{c(x) \mid x \in G_a\} \leq \bigvee^C G_a^C$ and second that $\bigvee^C G_a^C = \bigvee\{c(x) \mid x \in G_a\} \leq a$, as if $x \in G_a$ then $x \leq a$ so that $c(x) \leq a$. So we get that $a = \bigvee^C G_a^C$.

Finally suppose that S is a set-generated $\bigvee$-semilattice , with set G of generators. Let $c : Pow(G) \to Pow(G)$ be given by

$$c(X) = G_{\bigvee X}$$

for all $X \in Pow(G)$. Then it is easy to observe that c is a closure operation on $Pow(G)$. If C is the associated closure class then the function $C \to S$ that maps each $X \in C$ to $\bigvee X \in S$ is an isomorphism between C and S with inverse the function that maps each $a \in S$ to $G_a \in C$. □

15.2 Set Presentable $\bigvee$-Semilattices

Given a generating set G for S a subset R of $G \times Pow(G)$ is a *relation set over G for S* if for all $(a, X) \in G \times Pow(G)$

$$a \leq \bigvee X \;\leftrightarrow\; \exists Y \subseteq X\ [\ (a, Y) \in R\ ].$$

A *set presentation of S* is a pair (G, R) consisting of a generating set G for S and a relation set R over G for S.

Definition: 15.2 *A* set presentable $\bigvee$-semilattice *is a $\bigvee$-semilattice that has a set presentation.*

Example: For each set A the po-class $Pow(A)$ is a set presentable $\bigvee$-semilattice with set $G = \{\{a\} \mid a \in A\}$ of generators and relation set

$$R = \{(\{a\}, \{\{a\}\}) \mid a \in A\}.$$

Theorem: 15.3 *If $S = Pow(A)$, for some set A and C is a closure class then C is set-presentable if and only if the closure operation associated with C is set-based.*

Proof: Assume that $S = Pow(A)$, for some set A, and that c is the closure operation on S associated with C. Also assume that $B \subseteq S$ is a baseset for c. Then for all $X \subseteq A$ and all $a \in A$

$$(*) \qquad a \in c(X) \;\leftrightarrow\; \exists Y \in B\ [Y \subseteq X \wedge a \in c(Y)].$$

Now let A' be a regular set such that $B \cup G \subseteq A'$ and let

$$R = \{(Q, Z) \mid Q \in G \wedge Z \in A' \wedge Q \subseteq c(\cup Z) \wedge Z \subseteq G\}.$$

Claim 1: R is a set.

Proof: First observe that $T = \{Z \in A' \mid Z \subseteq G\}$ is a set. Also, for each $Z \in T$ we may form the set $\cup Z$ so that $c(\cup Z)$ is also a set and hence $S_Z = \{Q \in G \mid Q \subseteq c(\cup Z)\}$ is a set. Hence, by Union-Replacement $R = \bigcup_{Z \in T}(S_z \times \{Z\})$ is a set. □

Now let $X \in Pow(G)$ and $Q \in C$.

Claim 2: $Z \subseteq X \wedge QRZ \ \rightarrow \ Q \subseteq \bigvee X$.

Proof: Let $Z \subseteq X \wedge QRZ$. Then $Q \subseteq c(\cup Z) \subseteq c(\cup X)$ and hence $Q \subseteq \bigvee X$. □

Claim 3: $Q \subseteq \bigvee X \ \rightarrow \ \exists Z[Z \subseteq X \wedge QRZ]$.

Proof: Let $Q \subseteq \bigvee X$. Then by $(*)$ there is $Y \in B$ such that

$$Y \subseteq \cup X \wedge Q \subseteq c(Y).$$

As $Y \subseteq \cup X$

$$\forall y \in Y \exists Q' \in X \ y \in Q'.$$

As A' is regular, $Y \in A'$ and $X \subseteq A'$ there is $Z \in A'$ such that

$$\mathbb{B}(y \in Y, Q' \in Z)[\ y \in Q' \wedge Q' \in X\ ].$$

So $Y \subseteq \cup Z$ and $Z \subseteq X$ so that $Q \subseteq c(\cup Z)$ and $Z \subseteq X \subseteq G$ and hence also QRZ. □

It follows from these claims that (G, R) is a set presentation of C.

Now let (G, R) be a set presentation of a $\bigvee$-semilattice S. We show that S is isomorphic to a set presentable $\bigvee$-semilattice obtained from an inductive definition as above. Let Φ be the converse relation to R; i.e. it is the set of all pairs (X, a) such that aRX. Then Φ is an inductive definition that is a subset of $Pow(G) \times G$. Observe that there is a one-one correspondence between the class C of subsets X of G that are Φ-closed and the elements of S given by the function $C \to S$ mapping $X \mapsto \bigvee X$ and its inverse function $S \to C$ mapping $a \mapsto G_a = \{x \in G \mid x \leq a\}$. This is easily seen to be an isomorphism of the po-classes. $\square$

15.3 $\bigvee$-congruences on a $\bigvee$-semilattice

Let S be a $\bigvee$-semilattice . We define an equivalence relation $\approx$ on S to be a $\bigvee$-*congruence* on S if, for each set I, if $x_i, y_i \in S$ such that $x_i \approx y_i$ for all $i \in I$ then

$$\bigvee_{i \in I} x_i \approx \bigvee_{i \in I} y_i.$$

A preorder $\preceq$ on S is a $\bigvee$-*congruence pre-order* on S if for each subset X of S and each $a \in S$

$$\bigvee X \preceq a \;\leftrightarrow\; \forall x \in X\, [x \preceq a].$$

Proposition: 15.4 *There is a one-one correspondence between $\bigvee$-congruences and $\bigvee$-congruence pre-orders on S. To each $\bigvee$-congruence $\approx$ there corresponds the $\bigvee$-congruence pre-order $\preceq$ where*

$$x \preceq y \;\leftrightarrow\; \bigvee\{x, y\} \approx y.$$

Conversely to each $\bigvee$-congruence pre-order $\preceq$ corresponds the $\bigvee$-congruence $\approx$ where

$$x \approx y \;\leftrightarrow\; [x \preceq y \wedge y \preceq x].$$

These correspondences are inverses of each other.

Proposition: 15.5 *If $c : S \to S$ is a closure operation on S and we define $\approx$ by*

$$x \approx y \;\leftrightarrow\; c(x) = c(y)$$

for all $x, y \in S$ then $\approx$ is a $\bigvee$-congruence on S.

Proof: The relation $\approx$ is obviously an equivalence relation on S. Now suppose that $x_i \approx y_i$ for all $i \in I$, where I is a set. So $c(x_i) = c(y_i)$ for all $i \in I$. Let $x = \bigvee_{i \in I} x_i$ and $y = \bigvee_{i \in I} y_i$. Note that, as $y_i \leq c(y_i) = c(x_i)$ for all $i \in I$,

$$y = \bigvee_{i \in I} y_i \leq \bigvee_{i \in I} c(y_i) = \bigvee_{i \in I} c(x_i).$$

As $x_i \leq x$ for each $i \in I$ and c is monotone, $y \leq \bigvee_{i \in I} c(x_i) \leq c(x)$ and hence $c(y) \leq c(x)$. Similarily $c(x) \leq c(y)$ so that $c(x) = c(y)$. Thus we have shown that $\approx$ is a $\bigvee$-congruence on S. $\square$

Proposition: 15.6 *Let $\preceq$ be a $\bigvee$-congruence preorder on $S = Pow(A)$, where A is a set. Then the associated $\bigvee$-congruence $\approx$ comes from a closure operation c, as in the previous theorem, provided that for every $X \in S$ the class $\{a \in A \mid \{a\} \preceq X\}$ is a set. Then we can define $c(X)$ to be that set.*

16 General Topology in Constructive Set Theory

We wish to develop some general topology in constructive set theory. There are some initial problems to be overcome. The first problem is that in general the class of open sets cannot generally be assumed to be a set. This is because of the lack of the powerset axiom in constructive set theory. Without having powersets only the empty topological space will have its open sets forming a set. Another issue that needs to be kept in mind is that because we do not have full separation there will generally be open classes, i.e. unions of classes of open sets, that are not known to be sets. Even though the open sets will generally be only a class rather than a set there will usually be a set base generating the topology. So the notion of a set-based topological space will be the main notion of interest.

But there is another problem to be overcome. We sometimes want to construct a 'topological space' whose points form a class that is not known to be a set. This is particularly the case when we construct the concrete space of formal points of a formal topology. To allow for this we will formulate a precise notion of concrete space that generalises the notion of a set-based topological space by allowing the points to form a class. The set-based spaces will then be those concrete spaces that are small; i.e. have only a set of points. One of our concerns will be to find conditions on a concrete space that ensure that it is small.

16.1 Topological and concrete Spaces

Definition: 16.1 *We define a* topology *on a set X to be a class $\mathcal{T}$ of subsets of X, the* open sets*, that include the sets $\emptyset$ and X and are closed under unions and binary intesections; i.e.*

1. $\mathcal{X} \in Pow(\mathcal{T}) \Rightarrow \bigcup \mathcal{X} \in \mathcal{T}$,
2. $X_1, X_2 \in Pow(\mathcal{T}) \Rightarrow X_1 \cap X_2 \in \mathcal{T}$.

A set-base *for the topology is a subset $\mathcal{B}$ of $\mathcal{T}$ such that $\bigcup \mathcal{B} = X$ and, for $X_1, X_2 \in \mathcal{B}$, if $x \in X_1 \cap X_2$ then $x \in X$ for some $X \in \mathcal{B}$ such that $X \subseteq X_1 \cap X_2$.*

Note that a topological space $(X, \mathcal{T})$ is determined by any set-base $\mathcal{B}$, as $X = \bigcup \mathcal{B}$ and, for $Y \in Pow(X)$,

$$Y \in \mathcal{T} \quad \Leftrightarrow \quad Y = \bigcup \{Z \in \mathcal{B} \mid Z \subseteq Y\}.$$

Definition: 16.2 *A* concrete space $\underline{X} = (X, S, \{\alpha_x\}_{x \in X})$ *consists of a class X of points, a set S of neighborhood indices and an assignment of a neighborhood system $\alpha_x \in Pow(S)$ to each point x such that the following conditions hold, where for each $a \in S$*

$$B_a = \{x \in X \mid a \in \alpha_x\}.$$

1. *$X = \bigcup_{a \in S} B_a$,*
2. *If $x \in B_{a_1} \cap B_{a_2}$ then there is $a \in S$ such that $x \in B_a \subseteq B_{a_1} \cap B_{a_2}$.*

The concrete space is defined to be small *if X is a set.*

These conditions state that the classes B_a form a base of open classes for a 'topology' of open classes, the base being indexed by the set S and being locally small in the sense that the neighborhood system α_x of each point x is always a set.

Note that when the concrete space is small then the classes B_a are open sets and form the set-base for a topology on the set X. So the small concrete spaces are just the topological spaces with an explicitly given set-base.

16.2 Formal Topologies

Some background

Formal Topology has been introduced as a version of the point-free approach to point-set topology that can be developed in the setting of Martin-Löf's Constructive Type Theory. The aim here is to present a development of the ideas of Formal Topology in the alternative setting of Constructive Set Theory.

There are at least two advantages to using the setting of Constructive Set Theory rather than the setting of Constructive Type Theory. The first one is that Constructive Set Theory is a much more familiar setting for the development of mathematics than Constructive Type Theory. Much of the standard development of elementary mathematics in classical axiomatic set theory carries over smoothly, with a little care, to the development of elementary constructive mathematics in Constructive Set Theory. At present there is still no generally accepted standard approach to the presentation of elementary constructive mathematics in Constructive Type Theory.

The second advantage is that the setting of Constructive Type Theory is too restrictive. This is because it builds in the treatment of logic using the Propositions-as-Types idea, so that the type-theoretic Axiom of Choice and so Countable Choice and Dependent Choices are justified. Constructive

Set Theory is more flexible and general. While systems of Constructive Set Theory have natural interpretations in systems of Constructive Type Theory where logic is treated using the Propositions-as-types idea, such systems of Constructive Set Theory also have other interpretations obtained by reinterpreting the logic in ways analogous to what happens in topos theory. In topos theory there are many examples of topoi, e.g. suitable sheaf topoi, where Countable Choice does not hold. But nevertheless much of the results of point-free topology can be carried out in such topoi and the constructions can usually be refined to give results in Constructive Set Theory. Some refinement is needed because the Powerset Axiom holds in a topos, and this axiom is not available (or wanted) in Constructive Set Theory.

We take the key starting point for point-free topology in classical mathematics to be the adjunction between the category of topological spaces and the category of locales. With each topological space can be associated the locale of its open subsets and, in the reverse direction, with any locale can be associated the topological space of its points and these operations give rise to the two functors of the adjunction. The idea of point-free topology is that many definitions and results about topological spaces have more natural versions for locales and that it is these point-free versions for locales that are of interest in topos theory, rather than the original versions. Surprisingly for a given standard example of a topological space, such as the space of real numbers, it is not the locale of open sets under inclusion that is the locale of primary interest, but rather another more constructive and usually inductively generated locale that is used to represent the topology. In fact the topology is the topology of points of this primary locale and this is the natural way to construct the topological space. In the case of the real numbers the two locales can be proved isomorphic using the axiom of choice, but in general they need not be isomorphic.

The adjunction between topological spaces and locales still works in a topos, by exploiting the Powerset Axiom. In Constructive Set Theory we do not have this axiom and some care is needed even to give the key definitions of topological space and locale. For example perhaps the simplest example of a locale is the class of all subsets of a singleton set with set inclusion. Without assuming the Powerset Axiom we cannot take this locale to be a set. So our definition of a locale has to allow a locale to have a class of elements that need not be a set. Clearly a locale should be at least a partially ordered class that is a meet semi-lattice in which every subset has a supremum and meets distribute over suprema. We might in addition require there to be a set of generators; i.e. a subset G of the locale such that for every element a of the locale $a = \bigvee G_a$ where $G_a = \{x \mid x \leq a\}$ is a set. We may call such a locale a set-generated locale. Given such a set G of generators we may further require there to be a function $C : G \to Pow(G)$ such that for $a \in G$ and $U \in Pow(G)$

$$a \leq \bigvee U \quad \Leftrightarrow \quad (\exists V \in C(a))[V \subseteq U].$$

Call such a function C a set-presentation of the locale. When the locale has a set of generators with a set-presentation we may call the locale a set-presented locale. Note that the locale $Pow(A)$ of all subsets of a set A, partially ordered by set inclusion, is set-presented, with set $G = \{\{a\} \mid a \in A\}$ of generators and set-presentation C that assigns $C(\{a\}) = \{\{a\}\}$ to each $\{a\} \in G$.

The Definition

Definition: 16.3 *A formal topology $\underline{S} = (S, \lhd)$ consists of a set S and a subclass $\lhd$ of $\subseteq S \times Pow(S)$ satisfying the following conditions for $U, V \in Pow(S)$, where $U\downarrow = \{d \in S \mid \exists u \in U\ d \lhd \{u\}\}$ and $U \downarrow V = (U\downarrow) \cap (V\downarrow)$.*

1. $a \in U \Rightarrow a \lhd U$.
2. $a \lhd U \ \&\ \forall x \in U\ x \lhd V \ \Rightarrow\ a \lhd V$.
3. $a \lhd U \ \&\ a \lhd V \ \Rightarrow a \lhd U \downarrow V$.

$C : S \to Pow(Pow(S))$ *is a* set-presentation *of $\underline{S}$ if*

$$a \lhd U \ \Leftrightarrow\ (\exists V \in C(a))[V \subseteq U]$$

Definition: 16.4 *A* formal point *of a formal topology $\underline{S}$ is a subset α of S such that*

FP1: $\exists a(a \in \alpha)$,

FP2: $a, b \in \alpha \Rightarrow \exists c \in \alpha(c \in \{a\} \downarrow \{b\})$,

FP3. : $a \in \alpha \ \Rightarrow\ (\forall U \in Pow(S))[a \lhd U \ \Rightarrow\ (\exists c \in \alpha)(c \in U)]$.

A formal point α is a maximal formal point *if $\alpha \subseteq \beta \Rightarrow \alpha = \beta$ for every formal point β.*

Note that the third condition for a formal point involves a quantification over the class of all subsets U of S which cover a. This is an unbounded quantifier. But when the formal topology has a set presentation C the range of U can be restricted to the set $C(a)$ so that the third condition can be replaced by the following one.

3′. $a \in \alpha \;\Rightarrow\; (\forall U \in C(a))(\exists c \in \alpha)(c \in U)$.

So we get a restricted definition of the class of points.

Proposition: 16.5 *The class X of formal points of a formal topology $\underline{S} = (S, \lhd)$ can be made into the concrete space $\underline{Pt}(\underline{S}) = (X, S, \{\alpha\}_{\alpha \in X})$.*

Conversely, given a concrete space $\underline{X} = (X, S, \{\alpha_x\}_{x \in X})$, we can obtain a formal topology $\underline{Ft}(\underline{X}) = (S, \lhd_{\underline{X}})$ where

$$a \lhd_{\underline{X}} U \quad \Leftrightarrow \quad B_a \subseteq \bigcup_{b \in U} B_b.$$

!!!! Note: These two correspondences should form a category theoretic adjunction between the categories of concrete spaces and formal topologies, once the two categories have been suitably defined

16.3 Separation Properties

We now formulate some separation properties for concrete spaces and the regularity separation property for formal topologies.

Definition: 16.6 *Let $\underline{X} = (X, S, \{\alpha_x\}_{x \in X})$ be a concrete space. It is defined to be T_0 if for all points x, y*

$$\alpha_x = \alpha_y \Rightarrow x = y,$$

and is T_1 if for all points x, y

$$\alpha_x \subseteq \alpha_y \Rightarrow x = y.$$

It is defined to be regular *if, for all $a \in S$, if $Y = B_a$ then*

$$(*) \quad (\forall x \in Y)(\exists b \in S)[x \in B_b \;\&\; X \subseteq Y \cup \neg B_b],$$

where, for each open class Z,

$$\neg Z = \bigcup \{B_a \mid a \in S \;\&\; B_a \cap Z = \emptyset\}.$$

Note that $\neg Z$ is the largest open class disjoint from Z. Finally a T_3-space is defined to be a regular, T_1-space.

Observe that in a regular space (*) holds for any open class Y and, when the space is small, we have classically the usual notion of regularity, as then

$$X \subseteq Y \cup \neg B_b \quad \Leftrightarrow \quad Cl(B_b) \subseteq Y,$$

where $Cl(B_b)$ is the closure of B_b.

Definition: 16.7 *Let* $\underline{S} = (S, \lhd)$ *be a formal topology. Let*

$$b \between c \quad \Leftrightarrow \quad (\exists a \in S)(a \in \{b\} \downarrow \{c\})$$

for $b, c \in S$ *and let* $b^* = \{c \in S \mid \neg b \between c\}$ *for* $b \in S$. *We can now define*

$$W_a = \{b \in S \mid (\forall d \in S)(d \lhd \{a\} \cup b^*)\}$$

for $a \in S$ *and call the formal topology* regular *if* $a \lhd W_a$ *for all* $a \in S$.

Proposition: 16.8 *A concrete space* $\underline{X}$ *is a regular concrete space iff the associated formal topology* $\underline{Ft}(\underline{X})$ *is a regular formal topology.*

Theorem: 16.9 *If* $\underline{S}$ *is a regular formal topology then* $\underline{Pt}(\underline{S})$ *is a* T_3 *concrete space.*

Proof: Let $\underline{\mathrm{S}}$ be a regular formal topology with class X of formal points; i.e. the class of points of the concrete space $\underline{\mathrm{Ft}}(\underline{\mathrm{S}})$. Recall that $B_b = \{\alpha \in X \mid b \in \alpha\}$ for $b \in S$. We will use the following lemma. Only part 3 requires regularity.

Lemma: 16.10 *Let* $\alpha \in X$. *Then*

1. $b, c \in \alpha \Rightarrow b \between c$,
2. $(\exists c \in \alpha)(c \in b^*) \;\Rightarrow\; \alpha \in \neg B_b$,
3. *For each* $a \in \alpha$ *there is* $b \in \alpha$ *such that for any formal point* β

$$a \in \beta \text{ or } (\exists c \in \beta)(c \in b^*).$$

Proof:

1. Let $b, c \in \alpha$. Then, by condition 2 of Definition 16.4, there is $a \in \alpha$ such that $a \in \{b\} \downarrow \{c\}$ and hence $b \between c$.
2. Assume that $(\exists c \in \alpha)(c \in b^*)$. Then $\alpha \in B_c$ and

$$\begin{aligned} \gamma \in B_c \cap B_b \;&\Rightarrow b, c \in \gamma \\ &\Rightarrow b \between c \\ &\Rightarrow c \notin b^* \end{aligned}$$

contradicting $c \in b^*$. So $B_c \cap B_b = \emptyset$. Thus $\alpha \in \neg B_b$.

3. If $a \in \alpha$ then, as $a \lhd W_a$, there is $b \in \alpha$ such that $b \in W_a$, by condition 3 of Definition 16.4. Now, for any formal point β choose $d \in \beta$ by condition 1 of Definition 16.4. Then, as $b \in W_a$, we have $d \lhd \{a\} \cup b^*$ so that, by condition 3 of Definition 16.4 there is $c \in \beta$ such that $c \in \{a\} \cup b^*$; i.e. either $c = a$ or $c \in b^*$ so that $a \in \beta$ or $(\exists c \in \beta)(c \in b^*)$.

We first show that $\underline{\mathrm{Pt}}(\underline{\mathrm{S}})$ is T_1; i.e. we must show that when α, β are formal points of $\underline{\mathrm{S}}$ with $\beta \subseteq \alpha$ then $\alpha \subseteq \beta$. So let $a \in \alpha$. We show that $a \in \beta$. By part 3 of the lemma there is $b \in \alpha$ such that either $a \in \beta$ or $c \in b^*$ for some $c \in \beta$. In the latter case, as $\beta \subseteq \alpha$, we have $b, c \in \alpha$, so that, by part 1 of the lemma, $b \between c$, contradicting $c \in b^*$. So we get $a \in \beta$, as desired.

It remains to show that $\underline{\mathrm{Pt}}(\underline{\mathrm{S}})$ is regular; i.e. given $a \in S$ and $\alpha \in B_a$ we must show that $\alpha \in B_b$ for some $b \in S$ such that $X \subseteq B_a \cup \neg B_b$. By part 3 of the lemma there is $b \in \alpha$ such that $X \subseteq \{\beta \mid \beta \in B_a \text{ or } (\exists c \in \beta)(c \in b^*)\}$, so that, by part 2 of the lemma we are done.

16.4 The points of a set-generated formal topology

This section is inspired by a recent draft paper of Erik Palmgren, where it is shown in constructive type theory that if the formal points of a set generated formal topology are always maximal formal points then the formal points form a set. Here we prove this result in constructive set theory. But first some definitions.

It will be convenient to use some terminology from domain theory. Call a partially ordered class a *directed complete partial order (dcpo)* if every directed subset has a sup. A dcpo $\mathcal{X}$ is *set-generated* if there is a subset X such that, for every $a \in \mathcal{X}$, $\{x \in X \mid x \leq a\}$ is a directed set whose sup is a. It is easy to observe that the class of formal points of any formal topology, when ordered by the subset relation, form a dcpo. Our main result is the following.

Theorem: 16.11 ($\mathbf{CZF} + \bigcup \mathbf{REA} + \mathbf{DC}$) *The dcpo of formal points of a set-presented formal topology is a set-generated dcpo.*

Call a partially ordered class *flat* if $x \leq y \Rightarrow x = y$. Note that the assumption that the formal points are always maximal formal points can be rephrased as the assumption that the poclass of formal points is flat. So the statement of Palmgren's result, expressed in constructive set theory, becomes the following.

Corollary: 16.12 *If the poclass of formal points of a set-presented formal topology is flat then the formal points form a set.*

To prove this from the theorem it suffices to observe the following result.

Lemma: 16.13 *The elements of any flat set-generated dcpo form a set.*

Proof: If X is a set of generators for the dcpo then for any element a there must be $x \in X$ such that $x \leq a$, as X_a is directed. As the dcpo is flat $a = x \in X$. Thus the set X is the class of all the elements of the dcpo. $\square$

We will obtain the theorem from a more abstract result. To state the abstract result we need some definitions. Let S, S' be sets, let $\Gamma : Pow(S) \to Pow(S')$ and let $R : S' \to Pow(S)$. We define $\alpha \in Pow(S)$ to be Γ, R*-closed* if

$$(\forall x \in \Gamma(\alpha))(\exists y \in \alpha)\ y \in R_x.$$

It is easy to see that the poclass of Γ, R-closed subsets of S, when ordered by the subset relation, form a dcpo, when Γ is monotone and finitary. We have the following abstract result.

Theorem: 16.14 ($\mathbf{CZF} + \bigcup \mathbf{REA} + \mathbf{DC}$) *If Γ is monotone and finitary then the dcpo of Γ, R-closed sets is a set-generated dcpo.*

To apply this to get Theorem 16.11 it suffices, given a formal topology $(S, \lhd)$ with set presentation $C : S \to Pow(Pow(S))$, to define a set S', a monotone, finitary $\Gamma : Pow(S) \to Pow(S')$ and $R : S' \to Pow(S)$ so that a subset of S is a formal point iff it is Γ, R-closed. We now do this. For each $\alpha \in Pow(S)$ let

$$\Gamma(\alpha) = \{0\} + (\alpha \times \alpha) + \sum_{a \in \alpha} C(a)$$

and let $S' = \Gamma(S)$. Then $\Gamma : Pow(S) \to Pow(S')$ is monotone and finitary. Let $R_b \in Pow(S)$ for $b \in S'$ be given by

$$\begin{cases} R_{(1,0)} & = S, \\ R_{(2,(b_1,b_2))} & = \{b_1\} \downarrow \{b_2\} \quad \text{for } (b_1, b_2) \in S \times S, \\ R_{(3,(b,V))} & = V \quad\quad\quad\quad\ \text{for } (b, V) \in \sum_{a \in S} C(a). \end{cases}$$

It is now easy to see that the three conditions $1, 2, 3'$ for a formal point, can be combined into one using Γ and R to give us the following result.

Lemma: 16.15 *A subset α of S is a formal point of $(S, \lhd)$ iff α is Γ, R-closed.*

Proof of Theorem 16.14

Let S, S', Γ, R be as in the statement of the theorem. Let $Fin(S)$ be the set of all finite subsets of S. By $\bigcup$**REA** we may choose a regular set A closed under unions so that $\{\mathbb{N}\} \cup \{\Gamma(\alpha) \mid \alpha \in Fin(S)\}$ is a subset of A.

Lemma: 16.16 *For all sets $\alpha \subseteq S$*

1. $\alpha \in A \ \Rightarrow\ Fin(\alpha) \in A$,
2. $\alpha \in A \ \Rightarrow\ \Gamma(\alpha) \in A$.

Proof: Let α be a subset of S in A.

1. $Fin(\alpha) = \bigcup_{n\in\mathbb{N}}\{ran(f) \mid f \in ({}^{\{1,\dots,n\}}\alpha)\}$. As ${}^{\{1,\dots,n\}}\alpha \in A$ can be proved by induction on $n \in \mathbb{N}$ we get that $Fin(\alpha) \in A$.
2. Observe that $\Gamma(\alpha) = \bigcup\{\Gamma(\alpha_0) \mid \alpha_0 \in Fin(\alpha)\}$ and apply part 1.

□

Now let γ be a Γ, R-closed subset of S. We must show that the set A_γ of Γ, R-closed subsets of γ is directed and has union γ. Let $P = A \cap Pow(S)$ and let

$$T = \{(\alpha, \beta) \in P \times P \mid \alpha \subseteq \beta \ \&\ (\forall x \in \Gamma(\alpha))(\exists y \in \beta)\ y \in R_x\}$$

Lemma: 16.17 $(\forall \alpha \in P)(\exists \beta \in P)\ (\alpha, \beta) \in T$.

Proof: Let $\alpha \in P$. So $\alpha \in A$ and $\alpha \subseteq \gamma$. If $x \in \Gamma(\alpha)$ then $x \in \Gamma(\gamma)$ so that $y \in R_x$ for some $y \in \gamma$, by part 1, as γ is a formal point. Thus, as $\gamma \subseteq S \subseteq A$,

$$(\forall x \in \Gamma(\alpha))(\exists y \in A)[y \in R_x \cap \gamma].$$

As A is regular and, by part 2 $\Gamma(\alpha) \in A$, there is $\beta_0 \in A$ such that

$$(\forall x \in \Gamma(\alpha))(\exists y \in \beta_0)[y \in R_x \cap \gamma]$$

and

$$(\forall y \in \beta_0)(\exists x \in \Gamma(\alpha))[y \in R_x \cap \gamma].$$

Let $\beta = \alpha \cup \beta_0$. Then $\beta \subset \gamma$ and $\beta \in A$, as A is closed under unions. So $\beta \in P$ and also

$$\alpha \subseteq \beta \ \&\ (\forall x \in \Gamma(\alpha))(\exists y \in \beta)[y \in R_x].$$

Thus $(\alpha, \beta) \in T$. □

Corollary: 16.18 *If $\alpha_0 \in P$ then there is $\alpha \in A_\gamma$ such that $\alpha_0 \subseteq \alpha$.*

Proof: Let $\alpha_0 \in P$. Then, by **DC**, there is an infinite sequence $\alpha_0, \alpha_1, \ldots$ of elements of P such that $(\alpha_n, \alpha_{n+1}) \in T$ for all $n \in \mathbb{N}$. It follows that

$$\alpha_0 \subseteq \alpha_1 \subseteq \cdots \subseteq \gamma$$

and each $\alpha_n \in A$. As $\mathbb{N} \in A$ and A is strongly regular $\alpha = \bigcup_{n\in\mathbb{N}} \alpha_n$ is in A and $\alpha_0 \subseteq \alpha \subseteq \gamma$. It remains to show that α is Γ, R-closed. We must show that

$$(\forall x \in \Gamma(\alpha))(\exists y \in \alpha)\ y \in R_x.$$

So let $x \in \Gamma(\alpha)$. As Γ is finitary $x \in \Gamma(\alpha_n)$ for large enough n and then $y \in R_x$ for some $y \in \alpha_{n+1} \subseteq \alpha$, giving what we want. □

The proof of the theorem is completed with the following result.

Corollary: 16.19

1. *A_γ has an element.*

2. *If $\alpha_1, \alpha_2 \in A_\gamma$ then there is $\alpha \in A_\gamma$ such that $\alpha_1 \cup \alpha_2 \subseteq \alpha$.*

3. *If $x \in \gamma$ then there is $\alpha \in A_\gamma$ such that $x \in \alpha$.*

Proof:

1. Apply the lemma with $\alpha_0 = \emptyset$.

2. Apply the lemma with $\alpha_0 = \alpha_1 \cup \alpha_2$.

3. Apply the lemma with $\alpha_0 = \{x\}$.

□

16.5 A generalisation of a result of Giovanni Curi

Subset Collection

We work informally in **CZF**. Let A, B be sets. A class relation $R \subseteq A \times B$ is *total from A to B* if

$$(\forall x \in A)(\exists y \in B)[(x, y) \in R].$$

We write $\mathbf{mv}(B^A)$ for the class of all such total relations from A to B that are sets. The Subset Collection Scheme is equivalent to the following axiom.

For all sets A, B there is a subset C of the class $\mathbf{mv}(B^A)$ such that every set in $\mathbf{mv}(B^A)$ has a subset in C. We write $\mathbf{subcoll}(A, B)$ for the class of all such sets C.

Call a class *predicative* if it can be defined by a restricted formula, possibly having set parameters. Note that, by Restricted Separation, the intersection of any predicative class with a set is a set. It follows that any predicative subclass of a set is a set.

Lemma: 16.20 *Let A, B be sets and let $\mathcal{D}, \mathcal{R}$ be classes, with $\mathcal{D}$ a predicative subclass of $\mathbf{mv}(B^A)$ such that there are class functions mapping $R : \mathcal{D} \mapsto \alpha_R : \mathcal{R}$ and $\alpha : \mathcal{R} \mapsto R_\alpha : \mathcal{D}$ such that if $\alpha \in \mathcal{R}$ and $R \in \mathbf{mv}(B^A)$ is a subset of R_α then $R \in \mathcal{D}$ and $\alpha_R = \alpha$. Then $\mathcal{R}$ is a set.*

Proof: By the above formulation of Subset Collection choose $C \in \mathbf{subcoll}(A, B)$ and let $D = C \cap \mathcal{D}$. As $\mathcal{D}$ is a predicative class D is a set. It is now easy to see that under our assumptions

$$\mathcal{R} = \{\alpha_R \mid R \in D\}$$

so that using the Replacement Scheme we get that $\mathcal{R}$ is a set. □

The Main Lemma

We assume given $\mathcal{S} = (S, \prec, \asymp)$, where $\prec$ and $\asymp$ are set relations on the set S.

Definition: 16.21 *Call a subset α of S an* adequate set (for $\mathcal{S}$) *if*

A1: $b, c \in \alpha \Rightarrow b \asymp c$,

A2: $a \in \alpha \Rightarrow (\exists b \in \alpha)(b \prec a)$.

It is strongly adequate (for $\mathcal{S}$) *if also*

A3: $b \prec a \Rightarrow (\exists c \in \alpha)(b \asymp c \Rightarrow c = a)$.

Note the following observation.

Proposition: 16.22 *If α satisfies A3 and β is adequate then*

$$\alpha \subseteq \beta \Rightarrow \beta \subseteq \alpha.$$

Proof: Assume that $\alpha \subseteq \beta$ and $a \in \beta$. Then, by $A2$ for β,

$$b \prec a \text{ for some } b \in \beta.$$

By $A3$ for α,

$$b \asymp c \Rightarrow c = a \text{ for some } c \in \alpha.$$

As $\alpha \subseteq \beta$, $b, c \in \beta$ so that, by $A1$ for β, $b \asymp c$ and hence $c = a$, so that $a \in \alpha$.$\square$

An application of this observation is that every strongly adequate set is a maximally adequate set; i.e. it is maximal among the adequate sets.

The Main Lemma: *If $\prec$ and $\asymp$ are set relations on a set S then the strongly adequate sets for $(S, \prec, \asymp)$ form a set.*

Proof: Let $W = \{(a,b) \in S \times S \mid b \prec a\}$ and let $\mathcal{R}$ be the class of strongly adequate sets for $\mathcal{S}$. For $\alpha \in \mathcal{R}$ let

$$R_\alpha = \{((a,b),c) \in W \times S \mid c \in \alpha \,\&\, (b \asymp c \Rightarrow c = a)\}.$$

Then, by $A3$, $R_\alpha \in \mathbf{mv}(S^W)$. For $R \in \mathbf{mv}(S^W)$ let

$$\alpha_R = \{c \in S \mid (\exists w \in W)(w,c) \in R\}.$$

> **Lemma: 16.23** *Let $\alpha \in \mathcal{R}$, $R \in \mathbf{mv}(S^W)$ and $R \subseteq R_\alpha$. Then $\alpha_R = \alpha$.*
>
> **Proof:** To show that $\alpha_R \subseteq \alpha$ let $a \in \alpha_R$. Then $(w,a) \in R$ for some $w \in W$ so that $(w,a) \in R_\alpha$, as $R \subseteq R_\alpha$. It follows that $a \in \alpha$.
>
> To show that $\alpha \subseteq \alpha_R$ let $a \in \alpha$. Then, by $A2$, there is $b \in \alpha$ such that $b \prec a$. As $(a,b) \in W$ and $R \in \mathbf{mv}(S^W)$ there is c such that $((a,b),c)$ is in R and so in R_α, so that $c \in \alpha$ and
>
> $$b \asymp c \Rightarrow c = a.$$
>
> As $b, c \in \alpha$, by $A1$, $b \asymp c$ and so $c = a$ so that $((a,b),a) \in R$ and hence $a \in \alpha_R$. $\square$

Now let $\mathcal{D} = \{R \in \mathbf{mv}(S^W) \mid \alpha_R \in \mathcal{R}\}$. Then $\mathcal{D}$ is a predicative class and trivially $R \in \mathcal{D} \Rightarrow \alpha_R \in \mathcal{R}$. By Lemma 16.23 $\alpha \in \mathcal{R} \Rightarrow R_\alpha \in \mathcal{D}$. So, by Lemma 16.20 and Lemma 16.23 again we get that $\mathcal{R}$ is set. $\square$

The application to locally compact regular formal topologies

Definition: 16.24 *A* formal topology $(S, \lhd, Pos)$ with Pos *consists of a formal topology* $(S, \lhd)$ *with a subset* Pos *such that whenever* $a \lhd U$*, (i) if* $a \in Pos$ *the* U^+ *is inhabited and (ii)* $a \lhd U^+$*, where* $U^+ = U \cap Pos$.

We use the following definitions of the notions of a locally compact formal topology and of a P-regular formal topology.

Definition: 16.25 *A formal topology* $(S, \lhd)$ *is* locally compact *if there is a function* $i : S \to Pow(S)$ *such that for all* $a \in S$ $a \lhd i(a)$ *and if* $a \lhd U$ *then for any* $b \in i(a)$ *there is a finite subset* V *of* U *such that* $b \lhd V$.

Definition: 16.26 *The formal topology* $(S, \lhd)$ *is* P*-regular if* $a \lhd wc_P(a)$ *where* $wc_P : S \to Pow(S)$ *is defined as follows. For* $a \in S$ *let*

$$wc_P(a) = \{b \in S \mid (\forall d \in S)(d \lhd \{a\} \cup b^*_P)\}.$$

Here $b^*_P = \{c \in S \mid (\forall x \in P)\neg(x \lhd b, c)\}$.

Definition: 16.27 *A formal topology* $(S, \lhd)$ *without* Pos *is* regular *if it is* P*-regular where* $P = \{a \in S \mid \neg(a \lhd \emptyset)\}$*. A formal topology* $(S, \lhd, Pos)$ *with* Pos *is regular if it is* Pos*-regular.*

Definition: 16.28 *A subset* α *of a formal topology* $(S, \lhd, Pos)$ *with* Pos *is* regular *if*

1. $\exists a(a \in \alpha)$,
2. $(a \in \alpha \;\&\; b \in \alpha \to (\exists c \in \alpha)(c \lhd a, b)$,
3. $a \lhd b \;\&\; a \in \alpha \;\Rightarrow\; b \in \alpha$,
4. $\alpha \subseteq Pos$,
5. $a \in \alpha \to (\exists b \in \alpha)(b \in wc_{Pos}(a))$,

and is maximal regular *if also*

5. $b \in wc_{Pos}(a) \to (\exists c \in \alpha)(c \in \{a\} \cup b^*_{Pos})$.

The above definitions may be found in the preprint: *The Points of (Locally) Compact Regular Formal Topologies* by Giovanni Curi.

Theorem: 16.29 *The maximal continuous subsets of a locally compact regular formal topology form a set.*

Proof: We assume given a locally compact regular topology $(S, \lhd, Pos)$. Let

$$\begin{array}{lcl} a \prec b & \Leftrightarrow & a \in i(b), \\ b \asymp c & \Leftrightarrow & (\exists a \in Pos)(a \lhd b, c). \end{array}$$

Then the maximal continuous subsets of S are easily seen to form a predicative subclass of the set of strongly adequate subsets of S so that they form a set by Restricted Separation. $\square$
Recall the definition of the notion of a formal point of a formal topology $(S, \lhd)$.

Definition: 16.30 *A set $\alpha \subseteq S$ is a* formal point *of the formal topology $(S, \lhd)$ if*

FP1: $\exists a(a \in \alpha)$,

FP2: $(\forall a, b \in \alpha)(\exists c \in \alpha)(c \lhd a, b)$,

FP3: $(\forall a \in \alpha)(\forall U \in Pow(S))(a \lhd U \Rightarrow (\exists b \in \alpha)(b \in U))$.

Curi has characterized the formal points of any locally compact regular formal topology as the maximal continuous subsets and his proof of this fact seems to hold in **CZF** so that *maximal continuous subsets* can be replaced by *formal points* in the Theorem.

More Results

Let $(S, \lhd)$ be a formal topology (without Pos) and let P be a subset of S. We call a point of $(S, \lhd)$ that is a subset of P a *P-point*. So if $(S, \lhd, Pos)$ is a formal topology (with Pos) then a point of $(S, \lhd, Pos)$ is a Pos-point.

Theorem: 16.31 *If $(S, \lhd)$ is a P-regular formal topology, where P is a subset of S, then the P-points of $(S, \lhd)$ form a subclass of a set.*

Proof: Let $(S, \lhd)$ be a P-regular formal topology, where P is a subset of S. Define

$$\begin{array}{lcl} a \prec b & \Leftrightarrow & a \in wc_P(B), \\ b \asymp c & \Leftrightarrow & (\exists a \in P)(a \lhd b, c) \end{array}$$

Note that $b^*_P = \{c \in S \mid b \not\asymp c\}$. By the Main Lemma it is enough to prove the following result.

Lemma: 16.32 *If α is a P-point of $(S, \lhd)$ then α is strongly adequate for $(S, \prec, \asymp)$.*

Proof: Let α be a P-point of $(S, \triangleleft)$. We must show that $A1, A2, A3$ hold.

A1 Let $b, c \in \alpha$. Then, by $FP2$, there is $a \in \alpha$ such that $a \triangleleft b, c$. As α is a P-point $a \in P$. Thus $b \asymp c$.

A2 Let $a \in \alpha$. As $a \triangleleft wc_P(a)$ we may apply $FP3$ to get that $b \in \alpha$ for some $b \in wc_P(a)$; i.e.

$$(\exists b \in \alpha)(b \prec a).$$

A3 Let $b \prec a$; i.e. $b \in wc_P(a)$, so that for all $d \in S$

$$d \triangleleft \{a\} \cup b^*_P.$$

By $FP1$ we can choose $d \in \alpha$ so that, by FP3,

$$(\exists c \in \alpha)(c \in b^*_P \vee c = a).$$

It follows that, because $b \asymp c \Rightarrow c \notin b^*_P$,

$$(\exists c \in \alpha)((b \asymp c) \Rightarrow (c = a)).$$

Set-presentable formal topologies

Recall the following definition.

Definition: 16.33 *A formal topology* $(S, \triangleleft)$ *is* set-presentable *if there is a function*
$C : S \to Pow(S)$ *such that for all* $a \in S$ *and all* $U \in Pow(S)$

$$a \triangleleft U \;\Leftrightarrow\; (\exists V \in C(a))[V \subseteq U].$$

The function C *is called a* set-presentation *of the formal topology.*

Theorem: 16.34 *The points of a set-presentable formal topology* $(S, \triangleleft)$ *form a predicative class.*

Proof: Definition 16.30 would show that the class of formal points is predicative except for the quantifier $(\forall U \in Pow(S))$ in $FP3$ which is not a restricted quantifier. But given a set-presentation C we can replace this quantifier in $FP3$ by $(\forall U \in C(a))$ and the resulting condition would be equivalent to $FP3$ and using this we can show that the class of formal points is predicative.$\square$

Corollary: 16.35 *The* P*-points of a set-presentable* P*-regular formal topology form a set.*

Theorem: 16.36 *Every locally compact formal topology is set-presentable.*

Proof: Let $(S, \triangleleft)$ be a locally compact formal topology via $i : S \to Pow(S)$. So for all $a \in S$ we have $a \triangleleft i(a)$ and if $a \triangleleft U$ then

$$(\forall b \in i(a))(\exists V \in \mathcal{F})[V \subseteq U \ \& \ b \triangleleft V],$$

where $\mathcal{F}$ is the set of finite subsets of S. By Subset Collection there is a set G of subsets of $\mathcal{F}$ such that for all $a \in S$ and all $U \in Pow(S)$, if $a \triangleleft U$ then, for some $F \in G$,

$$(i) \qquad (\forall b \in i(a))(\exists V \in F)[V \subseteq U \ \& \ b \triangleleft V]$$

$$(ii) \qquad (\forall V \in F)(\exists b \in i(a))[V \subseteq U \ \& \ b \triangleleft V]$$

So, given $a \triangleleft U$ let $F \in G$ such that (i) and (ii) and let $Z = \cup F$. $Z \subseteq U$ and also $a \triangleleft Z$, as $(\forall b \in i(a)(b \triangleleft Z)$ and $a \triangleleft i(a)$. For $a \in S$ let

$$C(a) = \{\cup F \mid F \in G \ \& \ a \triangleleft \cup F\}.$$

Then C gives a set-presentation of the formal topology.□

Concrete Spaces

Definition: 16.37 *A* concrete space (X, S) *consists of a set X of points and a set S of subsets of X that form a base for a topology; i.e. $X = \cup S$ and, for all $b, c \in S$ and all $x \in b \cap c$ there is $a \in S$ such that $x \in a$ and $a \subseteq b \cap c$.*

Note that a set Y of points of a concrete space is open if every element of Y is an element a subset of Y that is in S, or equivalently if $Y = \cup U$ for some subset U of S.

Theorem: 16.38 *Let (X, S) be a concrete space, let Pos be the set of inhabited sets in S and for $a \in S$ and $U \in Pow(S)$ let*

$$a \triangleleft U \ \Leftrightarrow \ a \subseteq \cup U.$$

Then $(S, \triangleleft, Pos)$ is a set-presentable formal topology. Moreover, for every point $x \in X$ of the concrete space the set $\alpha_x = \{a \in S \mid x \in a\}$ is a formal point of the formal topology.

Proof: To show that $(S, \triangleleft, pos)$ is a formal topology is routine. We obtain a set presentation using Subset Collection to first obtain a set G of subsets of S such that whenever $a \in S$ and $R \in \mathbf{mv}(S^a)$ then there is $Z \in G$ such that $R \in \mathbf{mv}(Z^a)$ and $\breve{R} \in \mathbf{mv}(a^Z)$, where $\breve{R} = \{(b, x) \mid (x, b) \in R\}$.

For $a \in S$ let $C(a) = \{\cup Z \mid Z \in G \ \&\ a \subseteq \cup Z\}$. Trivially $V \in C(a) \Rightarrow a \lhd V$. Now let $a \lhd U$. Then $R \in \mathbf{mv}(S^a)$, where $R = \{(x, b) \mid x \in b \ \&\ b \in U\}$. It follows that there is $Z \in G$ such that $R \in \mathbf{mv}(Z^a)$ and $\breve{R} \in \mathbf{mv}(a^Z)$. So if $V = \cup Z$ then $Z \in C(a)$ and $Z \subseteq U$. Thus $a \lhd U \Rightarrow (\exists Z \in C(a))(Z \subseteq U)$ and we have shown that C is a set-presentation of the formal topology. $\square$

When the formal points of a formal space $(S, \lhd, Pos)$ form a set $Pt(S)$ then we obtain a concrete space $(Pt(S), \overline{S})$, where, if $Z_a = \{\alpha \in Pt(S) \mid a \in \alpha\}$, $\overline{S} = \{Z_a \mid a \in S\}$.

17 Large sets in constructive set theory

Large cardinals play a central role in modern set theory. This section deals with large cardinal properties in the context of intuitionistic set theories. Since in intuitionistic set theory $\in$ is not a linear ordering on ordinals the notion of a cardinal does not play a central role. Consequently, one talks about *"large set properties"* instead of *"large cardinal properties"*. When stating these properties one has to proceed rather carefully. Classical equivalences of cardinal notion might no longer prevail in the intuitionistic setting, and one therefore wants to choose a rendering which intuitionistically retains the most strength. On the other hand certain notions have to be avoided so as not to imply excluded third. To give an example, cardinal notions like measurability, supercompactness and hugeness have to be expressed in terms of elementary embeddings rather than ultrafilters.

We shall, however, not concern ourselves with very large cardinals here and rather restrict attention to the very first notions of largeness introduced by Hausdorff and Mahlo, that is, inaccessible and Mahlo sets and the pertaining hierarchies of inaccessible and Mahlo sets.

17.1 Inaccessibility

The background theory for most of this section will be $\mathbf{CZF}^-$, i.e., $\mathbf{CZF}$ without Set Induction.

Definition: 17.1 If A is a transitive set and ϕ is a formula with parameters in A we denote by ϕ^A the formula which arises from ϕ by replacing all unbounded quantifiers $\forall u$ and $\exists v$ in ϕ by $\forall u \in A$ and $\exists v \in A$, respectively.

We can view any transitive set A as a structure equipped with the binary relation $\in_A = \{\langle x, y\rangle \mid x \in y \in A\}$. A set-theoretic sentence whose parameters lie in A, then has a canonical interpretation in $(A, \in_A)$ by interpreting $\in$ as $\in_A$, and $(A, \in_A) \models \phi$ is logically equivalent to ϕ^A. We shall usually write $A \models \phi$ in place of ϕ^A.

Definition: 17.2 A set I is said to be *inaccessible* if I is a regular set such that the following are satisfied:

1. $\omega \in I$,
2. $\forall a \in I\ \bigcup a \in I$,
3. $\forall a \in I\,[a \text{ inhabited } \to \bigcap a \in I]$,
4. $\forall A, B \in I\, \exists C \in I\ \ I \models$ "*C is full in* $\mathbf{mv}({}^{A}B)$".

We will write $\mathbf{inacc}(I)$ to convey that I is an inaccessible set.

Let **INACC** be the principle

$$\forall x\,\exists I\,[x\in I\ \wedge\ \mathbf{inacc}(I)\,].$$

At first blush, the preceding definition of 'inaccessibility' may seem arbitrary. It will, however, soon become clear that it captures the essence of the traditional definition.

Lemma: 17.3 (**ECST**) *Every inaccessible set is a model of* Δ_0 *Separation.*

Proof: Let I be inaccessible. First we verify that I is a model of the theory $\mathbf{ECST}_0$ of Definition 5.1. Clearly I is a model of Extensionality. I is a model of Replacement since I is regular and I is a model of the Union Axiom since I is closed under Union. By Lemma 11.5, I is a model of Pairing. I is also a model of the Emptyset Axiom as $0 \in I$ on account of $\omega \in I$ and I being transitive.

As a result of $I \models \mathbf{ECST}_0$, 17.2 (3) and Theorem 5.6 we have that I is model of Binary Intersection Axiom. Thus by Corollary 5.7, I is a model of Δ_0 Separation. □

Corollary: 17.4 (**ECST**) *Every inaccessible set is a model of* **ECST**.

Proof: Let I be regular. By the previous Lemma and its proof, I is a model of **ECST**. Definition 17.2 (1) implies that I is a model of the Strong Infinity Axiom while 17.2 (4) guarantees that I is a model of Fullness. One easily verifies that I is also a model of Strong Collection (Exercise). Hence I is a model of $\mathbf{CZF}^-$. □

Corollary: 17.5 (**CZF**) *Every inaccessible set is a model of* **CZF**.

Proof: This is obvious as Set Induction implies $I \vDash$ Set Induction for any transitive set I. □

Definition 17.2 (4) only guarantees that an inaccessible set is a model of Fullness. The next result shows that inaccessible sets satisfy "Fullness" in a much stronger sense.

Lemma: 17.6 (**ECST**) *If I is set-inaccessible, then for all $A, B \in I$ there exists $C \in I$ such that C is full in* $\mathbf{mv}({}^{A}B)$.

Proof: Let I be an inaccessible set. We first show:

$$\forall A{\in}I \text{ “}I \cap \mathbf{mv}({}^A I) \textit{ is full in } \mathbf{mv}({}^A I)\text{”;} \tag{24}$$

$$\forall A,B{\in}I\, \exists C{\in}I\ I \models \text{“}C \textit{ is full in } \mathbf{mv}({}^A B)\text{”.} \tag{25}$$

To prove (24), let $A{\in}I$ and $R \in \mathbf{mv}({}^A I)$. Then R is a subset of $A \times I$ such that for all $x{\in}A$ there is $y{\in}I$ such that xRy. Let R' be the set of all $(x,(x,y))$ such that xRy. Then $R' \in \mathbf{mv}({}^A I)$ also, as I is closed under Pairing. Hence, as I is regular, there is $S{\in}I$ such that $\forall x{\in}A\, \exists z{\in}S\ xR'z \wedge \forall z{\in}S\, \exists x{\in}A\ xR'z$. Hence $S \in (I \cap \mathbf{mv}({}^A I))$ and S is a subset of R. So (24) is proved. (25) is just stating that $I \models$ *“Fullness”*, which follows from 4.12 since I is a model of $\mathbf{CZF}^-$.

Now let $A, B{\in}I$ and choose $C{\in}I$ as in (25). It follows that $C \subseteq \mathbf{mv}({}^A B)$ and:

$$\forall R'{\in}I\, [R' \in \mathbf{mv}({}^A B) \ \rightarrow\ \exists R_0{\in}C\, (R_0 \subseteq R')\,].$$

We want to show that C is actually full in $\mathbf{mv}({}^A B)$. For this it suffices, given $R \in \mathbf{mv}({}^A B)$ to find a subset R' of R such that $R' \in (I \cap \mathbf{mv}({}^A B))$, as then we can get $R_0{\in}C$, as above, a subset of R' and hence of R.

But, as B is a subset of I, $R \in \mathbf{mv}({}^A I)$ so that, by (24), there is a subset R' of R such that $R'{\in}(I \cap \mathbf{mv}({}^A I))$. It follows that $R' \in (I \cap \mathbf{mv}({}^A B))$ and we are done. $\square$

Corollary: 17.7 (**ECST**) *If I is an inaccessible set then I is Exp-closed, i.e., whenever $A, B \in I$ then ${}^A B \in I$.*

Proof: By Lemma 17.6 there exists a set $C \in I$ such that C is full in $\mathbf{mv}({}^A B)$. Now define $X = \{f \in C \mid f : A \to B\}$. Then $X = {}^A B$ and by Δ_0 Separation in I we have $X \in I$. $\square$

Corollary: 17.8 (**ECST+REM**) *If I is an inaccessible set then I is closed under taking powersets, i.e., whenever $A \in I$ then $\mathcal{P}(A) \in I$.*

Proof: If $X \in I$, then ${}^X 2 \in I$ by 17.7, thus the power set of X is in I, too, as $\{y \mid y \subseteq X\} = \{\{v \in X \mid f(v) = 0\} : f \in {}^X 2\}$, using classical logic. $\square$

As the next result shows, from a classical point of view inaccessible sets are closely related to inaccessible cardinals.

Corollary: 17.9 *(i)* (**ZF**) *If I is set-inaccessible, then there exists a weakly inaccessible cardinal κ such that $I = V_\kappa$.*

(ii) (**ZFC**) *I is set-inaccessible if and only if there exists a strongly inaccessible cardinal κ such that $I = V_\kappa$.*

Proof: (i): First note that with the help of classical logic, Replacement implies Full Separation.

Let V_α denote the αth level of the von Neumann hierarchy. By Corollary 17.8 it holds that for all ordinals $\alpha \in I$, $(V_\alpha)^I = V_\alpha$, where $(V_\alpha)^I$ stands for the αth level of the von Neumann hierarchy as defined within I. Therefore $I = V_\kappa$, where κ is the least ordinal not in I (another use of classical logic). It is readily shown that κ is weakly inaccessible.

(ii): It remains to show that κ is a strong limit. Let $\rho < \kappa$. Using **AC** one finds an ordinal λ together with a bijection $G : {}^\rho 2 \to \lambda$. Set $D := \{f \in {}^\rho 2 \mid G(f) < \kappa\}$. As $D \subseteq {}^\rho 2$ and I is closed under taking power sets, it follows $D \in I$. If $\kappa \leq \lambda$, then $F := G \restriction D$ would provide a counterexample to the regularity of Z. Thus $\lambda < \kappa$. $\square$

Corollary: 17.10 *The following theories prove the same formulae:*

(i) $\mathbf{CZF} + \exists I\, \mathbf{inacc}(I) + \mathbf{EM}$

(ii) $\mathbf{ZF} + \exists I\, \mathbf{inacc}(I)$

They are equiconsistent with $\mathbf{ZFC} + \exists\kappa$ *"κ inaccessible cardinal".*

Proposition: 17.11 *The theories* $\mathbf{CZF}^- + \mathbf{INAC} + \mathbf{EM}$ *and*

$$\mathbf{ZFC} + \forall\alpha\, \exists\kappa\, (\alpha < \kappa \,\wedge\, \kappa \textit{ is a strongly inaccessible cardinal})$$

are equiconsistent.

Proof: Exercise. $\square$

17.2 Mahloness in constructive set theory

This section introduces the notion of a Mahlo set and explores some of its **CZF** provable properties.

Recall that in classical set theory a cardinal κ is said to be *weakly Mahlo* if the set $\{\rho < \kappa : \rho \textit{ is regular}\}$ is stationary in κ. A cardinal μ is *strongly Mahlo* if the set $\{\rho < \kappa : \rho \textit{ is a strongly inaccessible cardinal}\}$ is stationary in μ.

Definition: 17.12 A set M is said to be *Mahlo* if M is set-inaccessible and for every $R \in \mathbf{mv}(^M M)$ there exists a set-inaccessible $I \in M$ such that

$$\forall x \in I\, \exists y \in I\ \langle x, y\rangle \in R.$$

Proposition: 17.13 (**ZFC**) *A set M is Mahlo if and only if $M = V_\mu$ for some strongly Mahlo cardinal μ.*

Proof: This is an immediate consequence of Corollary 17.9. $\square$

Lemma: 17.14 (**CZF**$^-$) *If M is Mahlo and $R \in \mathbf{mv}(^M M)$, then for every $a \in M$ there exists a set-inaccessible $I \in M$ such that $a \in I$ and*

$$\forall x \in I\, \exists y \in I\ \langle x, y\rangle \in R.$$

Proof: Set $S := \{\langle x, \langle a, y\rangle\rangle :\ \langle x, y\rangle \in R\}$. Then $S \in \mathbf{mv}(^M M)$ too. Hence there exists $I \in M$ such that $\forall x \in I\, \exists y \in I\ \langle x, y\rangle \in S$. Now pick $c \in I$. Then $\langle c, d\rangle \in S$ for some $d \in I$. Moreover, $d = \langle a, y\rangle$ for some y. In particular, $a \in I$.

Further, for each $x \in I$ there exists $u \in I$ such that $\langle x, u\rangle \in S$. As a result, $u = \langle a, y\rangle$ and $\langle x, y\rangle \in R$ for some y. Since $u \in I$ implies $y \in I$, the latter shows that $\forall x \in I\, \exists y \in I\ \langle x, y\rangle \in R$. $\square$

Lemma: 17.15 (**CZF**$^-$) *Let M be Mahlo. If $\forall x \in M\, \exists y \in M\, \phi(x, y)$, then there exists $S \in \mathbf{mv}(^M M)$ such that*

$$\forall xy\, [\langle x, y\rangle \in S \to \phi(x, y)].$$

Proof: The assumption yields $\forall x \in M\, \exists z \in M\, \psi(x, z)$, where

$$\psi(x, z) \quad := \quad \exists y \in M\, (z = \langle x, y\rangle\ \wedge\ \phi(x, y)).$$

By Strong Collection there exists a set S such that $\forall x \in M\, \exists z \in S\, \psi(x, z)$ and $\forall z \in S\, \exists x \in M\, \psi(x, z)$. As a result, $\forall x \in M\, \exists y \in M\ \langle x, y\rangle \in S$, and thus $S \in \mathbf{mv}(^M M)$. Moreover, if $\langle x, y\rangle \in S$, then $y \in M$ and $\phi(x, y)$ holds. $\square$

Corollary: 17.16 (**CZF**$^-$) *Let M be Mahlo. If $\forall x \in M\, \exists y \in M\, \phi(x, y)$, then for every $a \in M$ there exists a set-inaccessible $I \in M$ such that $a \in I$ and*

$$\forall x \in I\, \exists y \in I\ \phi(x, y).$$

Proof: This follows from Lemma 17.15 and Lemma 17.14. □

In a paper from 1911 Mahlo [46] investigated two hierarchies of regular cardinals. In view of its early appearance this work is astounding for its refinement and its audacity in venturing into the higher infinite. Mahlo called the cardinals considered in the first hierarchy π_α*-numbers.* In modern terminology they are spelled out as follows:

$$\begin{array}{rll} \kappa \text{ is } 0\text{-}\textit{weakly inaccessible} & \text{iff} & \kappa \text{ is regular;} \\ \kappa \text{ is } (\alpha+1)\text{-}\textit{weakly inaccessible} & \text{iff} & \kappa \text{ is a regular limit of } \alpha\text{-weakly inaccessibles} \\ \kappa \text{ is } \lambda\text{-}\textit{weakly inaccessible} & \text{iff} & \kappa \text{ is } \alpha\text{-weakly inaccessible for every } \alpha < \lambda \end{array}$$

for limit ordinals λ. Mahlo also discerned a second hierarchy which is generated by a principle superior to taking regular fixed-points. Its starting point is the class of ρ_0-numbers which later came to be called weakly Mahlo cardinals.

A hierarchy of *strongly* α*-inaccessible cardinals* is analogously defined, except that the strongly 0-inaccessibles are the strongly inaccessible cardinals.

In classical set theory the notion of a strongly Mahlo cardinal is much stronger than that of a strongly inaccessible cardinal. This is e.g. reflected by the fact that for every strongly Mahlo cardinal μ and $\alpha < \mu$ the set of strongly α-inaccessible cardinals below μ is closed and unbounded in μ (cf.[42], Ch.I,Proposition 1.1). In the following we show that similar relations hold true in the context of constructive set theory as well.

Definition: 17.17 An *ordinal* is a transitive set whose elements are transitive too. We use letters $\alpha, \beta, \gamma, \delta$ to range over ordinals.

Let A, B be classes. A is said to be *unbounded in* B if

$$\forall x \in B\, \exists y \in A\, (x \in y \ \wedge \ y \in B).$$

Let Z be set. Z is said to be α*-set-inaccessible* if Z is set-inaccessible and there exists a family $(X_\beta)_{\beta\in\alpha}$ of sets such that for all $\beta \in \alpha$ the following hold:

- X_β is unbounded in Z.
- X_β consists of set-inaccessible sets.
- $\forall y \in X_\beta\, \forall \gamma \in \beta\ X_\gamma$ is unbounded in y.

The function F with domain α satisfying $F(\beta) = X_\beta$ will be called a *witnessing function for the* α*-set-inaccessibility of* Z*.*

Corollary: 17.18 (**CZF**) *If Z is α-set-inaccessible and $\beta \in \alpha$, then Z is β-set-inaccessible.*

Lemma: 17.19 (**CZF**) *If Z is set-inaccessible, then Z is α-set-inaccessible iff for all $\beta \in \alpha$ the β-set-inaccessibles are unbounded in Z.*

Proof: One direction is obvious. So suppose that for all $\beta \in \alpha$ the β-set-inaccessibles are unbounded in Z; thus

$$\forall \beta \in \alpha \forall x \in Z \exists u \in Z (x \in u \wedge u \text{ is } \beta\text{-set-inaccessible}).$$

Using Strong Collection, there is a set S such that S consists of triples $\langle \beta, u, x \rangle$, where $\beta \in \alpha$, $x \in u \in Z$ and u is β-set-inaccessible, and for each $\beta \in \alpha$ and $x \in Z$ there is a triple $\langle \beta, u, x \rangle \in S$. Put

$$S_\beta = \{u : \exists x \in Z \, \langle \beta, u, x \rangle \in S\}.$$

Again by Strong Collection there exists a set $\mathcal{F}$ of functions such that for all $\beta \in \alpha$ and and $u \in S_\beta$ there is a function $f \in \mathcal{F}$ witnessing the β-set-inaccessibility of u, and, conversely, any $f \in \mathcal{F}$ is a witnessing function for some $u \in S_\beta$ for some $\beta \in \alpha$. Now define a function F with domain α via

$$F(\beta) = S_\beta \cup \bigcup \{f(\beta) : \ f \in \mathcal{F}; \beta \in \mathbf{dom}(f)\}.$$

As S_β is unbounded in Z, so is $F(\beta)$. Let $y \in F(\beta)$ and suppose $\gamma \in \beta$. If $y \in S_\beta$, then there is an $f \in \mathcal{F}$ witnessing the β-set-inaccessibility of y, thus $f(\gamma)$ is unbounded in y and a fortiori $F(\gamma)$ is unbounded in y.

Now assume that $y \in f(\beta)$ for some $f \in \mathcal{F}$ with $\beta \in \mathbf{dom}(f)$. As $f \restriction \beta$ witnesses the β-set-inaccessibility of y, $f(\gamma)$ is unbounded in y, thus $F(\gamma)$ is unbounded in y. $\square$

The preceding lemma shows that the notion of being α-set-inaccessible is closely related to Mahlo's π_α-numbers. To state this precisely, we recall the notion of κ being *α-strongly inaccessible* (for ordinals α and cardinals κ) which is defined as α-weak inaccessibility except that κ is also required to be a strong limit, i.e. $\forall \rho < \kappa \, (2^\rho < \kappa)$.

Corollary: 17.20 (**ZFC**) *κ is α-strongly inaccessible iff V_κ is α-set-inaccessible.*

Theorem: 17.21 (**CZF**) *Let M be Mahlo. Then for every $\alpha \in M$, the set of α-set-inaccessibles is unbounded in M.*

Proof: We will prove this by induction on α. Suppose this is true for all $\beta \in \alpha$. By the regularity of M we get

$$\forall x \in M\, \exists y \in M\, [x \in y \;\wedge\; \forall \beta \in \alpha\, \exists z \in y\;\, z \text{ is } \beta\text{-set-inaccessible}]. \tag{26}$$

Using Lemma 17.15, we conclude that for every $a \in M$ there exists a set-inaccessible $I \in M$ such that $a \in I$ and

$$\forall x \in I\, \exists y \in I\, (x \in y \;\wedge\; \forall \beta \in \alpha\, \exists z \in y\;\, z \text{ is } \beta\text{-set-inaccessible}).$$

Hence the β-set-inaccessibles are unbounded in I and, by Lemma 17.19, I is α-set-inaccessible. As a result, the α-set-inaccessibles are unbounded in M.□

Corollary: 17.22 (**CZF**) *Let M be Mahlo. If $\alpha \in M$, then M is α-set-inaccessible.*

Proof: Follows from Theorem 17.21 and Lemma 17.19. □

18 Intuitionistic Kripke-Platek set theory

One of the fragments of **ZF** which has been studied intensively is Kripke-Platek set theory, **KP**. Its standard models are called *admissible sets*. One of the reasons that this is a truly remarkable theory is that a great deal of set theory requires only the axioms of **KP**. An even more important reason is that admissible sets have been a major source of interaction between model theory, recursion theory and set theory. **KP** arises from **ZF** by completely omitting the Powerset axiom and restricting Separation and Collection to absolute predicates (cf. [7]), i.e. Δ_0 formulas. These alterations are suggested by the informal notion of 'predicative'. The intuitionistic version of **KP**, **IKP**, arises from **CZF** by omitting Subset Collection and replacing Strong Collection by Δ_0 *Collection*, i.e.,

$$\forall x \in a\, \exists y\, \phi(x,y) \to \exists z\, \forall x \in a\, \exists y \in z\, \phi(x,y)$$

for all Δ_0 formulae ϕ.

By $\mathbf{IKP}_0$ we denote the system **IKP** bereft of Set Induction.

18.1 Basic principles

The intent of this section is to explore which of the well known provable consequences of **KP** carry over to **IKP**.

Proposition: 18.1 ($\mathbf{IKP}_0$) *If A, B are sets then so is the class $A \times B$.*

Proof: First note that the proof of the uniqueness of ordered pairs in Proposition 3.1 is a $\mathbf{IKP}_0$ proof. Further, the existence proof of the Cartesian product given in Proposition 4.4 requires only Δ_0 Collection. $\square$

Definition: 18.2 The collection of Σ *formulae* is the smallest collection containing the Δ_0 formulae closed under conjunction, disjunction, bounded quantification and unbounded existential quantification. The collection of Π *formulae* is the smallest collection containing the Δ_0 formulae closed under conjunction, disjunction, bounded quantification and unbounded universal quantification.

Given a formula ϕ and a variable w not appearing in ϕ, we write ϕ^w for the result of replacing each unbounded quantifier $\exists x$ and $\forall x$ in ϕ by $\exists x \in w$ and $\forall x \in w$, respectively.

Lemma: 18.3 *For each Σ formula the following are intuitionistically valid:*

(i) $\phi^u \ \wedge \ u \subseteq v \rightarrow \phi^v$,

(ii) $\phi^u \rightarrow \phi$.

Proof: Both facts are proved by induction following the inductive definition of Σ formula. $\square$

Theorem: 18.4 (Σ Reflection Principle). *For all Σ formulae ϕ we have the following:*

$$\mathbf{IKP}_0 \vdash \phi \leftrightarrow \exists a \phi^a.$$

(Here a is any set variable not occurring in ϕ; we will not continue to make these annoying conditions on variables explicit.) *In particular, every Σ formula is equivalent to a Σ_1 formula in* $\mathbf{IKP}_0$.

Proof: We know from the previous lemma that $\exists a\, \phi^a \rightarrow \phi$, so the axioms of $\mathbf{IKP}_0$ come in only in showing $\phi \rightarrow \exists a\, \phi^a$. proof is by induction on ϕ, the case for Δ_0 formulae being trivial. We take the three most interesting cases, leaving the other two to the reader.

Case 0. If ϕ is Δ_0 then $\phi \leftrightarrow \phi^a$ holds for every set a.

Case 1. ϕ is $\psi \wedge \theta$. By induction hypothesis, $\mathbf{IKP}_0 \vdash \psi \leftrightarrow \exists a\, \psi^a$ and $\mathbf{IKP}_0 \vdash \theta \leftrightarrow \exists a\, \theta^a$. Let us work in $\mathbf{IKP}_0$, assuming $\psi \wedge \theta$. Now there are a_1, a_2 such that ψ^{a_1}, θ^{a_2}, so let $a = a_1 \cup a_2$. Then ψ^a and θ^a hold by the previous lemma, and hence ϕ^a.

Case 2. ϕ is $\psi \vee \theta$. By induction hypothesis, $\mathbf{IKP}_0 \vdash \psi \leftrightarrow \exists a\, \psi^a$ and $\mathbf{IKP}_0 \vdash \theta \leftrightarrow \exists a\, \theta^a$. Let us work in $\mathbf{IKP}_0$, assuming $\psi \vee \theta$. Then ψ^{a_1} for some set a_1 or there is a set a_2 such that θ^{a_2}. In the first case we have $\psi^a \vee \theta^a$ with $a := a_1$ while in the second case we have $\psi^a \vee \theta^a$ with $a := a_2$.

Case 2. ϕ is $\forall u \in v\, \psi(u)$. The inductive assumption yields $\mathbf{IKP}_0 \vdash \psi(u) \leftrightarrow \exists a\, \psi(u)^a$. Again, working in $\mathbf{IKP}_0$, assume $\forall u \in v\, \psi(u)$ and show $\exists a\, \forall u \in v\, \psi(u)^a$. For each $u \in v$ there is a b such that $\psi(u)^b$, so by Δ_0 Collection there is an a_0 such that $\forall u \in v\, \exists b \in a_0 \psi(u)^b$. Let $a = \bigcup a_0$. Now, for every $u \in v$, we have $\exists b \subseteq a\, \psi(u)^b$; so $\forall u \in v \psi(u)^a$, by the previous lemma.

Case 3. ϕ is $\exists u\, \psi(u)$. Inductively we have $\mathbf{IKP}_0 \vdash \psi(u) \leftrightarrow \exists b\, \psi(u)^b$. Working in $\mathbf{IKP}_0$, assume $\exists u\, \psi(u)$. Pick u_0 such $\psi(u_0)$ and b such that $\psi(u_0)^b$. Letting $a = b \cup \{u_0\}$ we get $u_0 \in a$ and $\psi(u_0)^a$ by the previous lemma. Thence $\exists a\, \exists u \in a\, \psi(u)^a$. $\square$

In Platek's original definition of admssible set he took the Σ Reflection Principle as basic. It is very powerful, as we'll see below. Δ_0 Collection is easier to verify, however.

Theorem: 18.5 (The Strong Σ Collection Principle). *For every Σ formula ϕ the following is a theorem of* $\mathbf{IKP}_0$*: If $\forall x \in a\, \exists y \phi(x,y)$ then there is a set b such that $\forall x \in a\, \exists y \in b\, \phi(x,y)$ and $\forall y \in b\, \exists x \in a\, \phi(x,y)$.*

Proof: Assume that
$$\forall x \in a \exists y \in b\, \phi(x,y).$$
By Σ Reflection there is a set c such that
$$\forall x \in a\, \exists y \in c\, \phi(x,y)^c. \tag{27}$$
Let
$$b = \{y \in c |\, \exists x \in a\, \phi(x,y)^c\}, \tag{28}$$
by Δ_0 Separation. Now, since $\phi(x,y)^c \to \phi(x,y)$ by 18.3, (27) gives us $\forall x \in a\, \exists y \in b\, \phi(x,y)$, whereas (28) gives us $\forall y \in b\, \exists x \in a\, \phi(x,y)$. $\square$

Theorem: 18.6 (Σ Replacement). *For each Σ formula $\phi(x,y)$ the following is a theorem of* $\mathbf{IKP}_0$*: If $\forall x \in a\, \exists! y\, \phi(x,y)$ then there is a function f, with* $\mathbf{dom}(f) = a$*, such that $\forall x \in a\, \phi(x, f(x))$.*

Proof: By Σ Reflection there is a set d such that
$$\forall x \in a\, \exists y \in d\, \phi(x,y)^d.$$
Since $\phi(x,y)^d$ implies $\phi(x,y)$ we get $\forall x \in a\, \exists! y \in d\, \phi(x,y)^d$. Thus, defining $f = \{\langle x,y\rangle \in a \times d |\, \phi(x,y)^d\}$ by Δ_0 Separation, f is a function satisfying $\mathbf{dom}(f) = a$ and $\forall x \in a\, \phi(x, f(x))$. $\square$

The above is sometimes infeasible because of the uniqueness requirement $\exists!$ in the hypothesis. In these situations it is usually the next result which comes to the rescue.

Theorem: 18.7 (Strong Σ Replacement). *For each Σ formula $\phi(x,y)$ the following is a theorem of* $\mathbf{IKP}_0$*: If $\forall x \in a\, \exists y\, \phi(x,y)$ then there is a function f with* $\mathbf{dom}(f) = a$ *such that for all $x \in a$, $f(x)$ is inhabited and $\forall x \in a\, \forall y \in f(x)\, \phi(x,y)$.*

Proof: By Strong Σ Collection there is a b such that $\forall x \in a\, \exists y \in b\, \phi(x,y)$ and $\forall y \in b\, \exists x \in a\, \phi(x,y)$. Hence, by Σ Reflection, there is a d such that
$$\forall x \in a\, \exists y \in b\, \phi(x,y)^d \quad \text{and} \quad \forall y \in b\, \exists x \in a\, \phi(x,y)^d.$$

For any fixed $x \in a$ there is a unique set c_x such that

$$c_x = \{y \in b |\, \phi(x,y)^d\}$$

by Δ_0 Separation and Extensionality; so, by Σ Replacement, there is a function f with domain a such that $f(x) = c_x$ for each $x \in a$. $\square$

One principle of **KP** that is not provable in **IKP** is Δ_1 Separation. This is the principle that whenever $\forall x \in a\, [\phi(x) \leftrightarrow \psi(x)]$ holds for a Σ formula ϕ and a Π formula ψ then the class $\{x \in a |\, \phi(x)\}$ is a set. The reason is that classically $\forall x \in a\, [\phi(x) \leftrightarrow \psi(x)]$ entails $\forall x \in a\, [\phi(x) \vee \neg\psi(x)]$ which is classically equivalent to a Σ formula.

18.2 Σ Recursion in IKP

The mathematical power of **KP** resides in the possibility of defining Σ functions by $\in$-recursion and the fact that many interesting functions in set theory are definable by Σ Recursion. Moreover the scheme of Δ_0 Separation allows for an extension with provable Σ functions occurring in otherwise bounded formulae.

Proposition: 18.8 (Definition by Σ Recursion in **IKP**.) *If G is a total $(n+2)$–ary Σ definable class function of* **IKP***, i.e.*

$$\mathbf{IKP} \vdash \forall \vec{x} y z \exists! u\, G(\vec{x}, y, z) = u$$

then there is a total $(n+1)$–ary Σ class function F of **IKP** *such that*[6]

$$\mathbf{IKP} \vdash \forall \vec{x} y [F(\vec{x}, y) = G(\vec{x}, y, (F(\vec{x}, z) | z \in y))].$$

Proof: Let $\Phi(f, \vec{x})$ be the formula

$$[f \text{ is a function}] \wedge [\mathbf{dom}(f) \text{ is transitive}] \wedge [\forall y \in \mathbf{dom}(f)\, (f(y) = G(\vec{x}, y, f \restriction y))].$$

Set

$$\psi(\vec{x}, y, f) = [\Phi(f, \vec{x}) \wedge y \in \mathbf{dom}(f)].$$

Claim $\quad \mathbf{IKP} \vdash \forall \vec{x}, y \exists! f \psi(\vec{x}, y, f)$.

Proof of Claim: By $\in$ induction on y. Suppose $\forall u \in y\, \exists g\, \psi(\vec{x}, u, g)$. By Strong Σ Collection we find a set A such that $\forall u \in y\, \exists g \in A\, \psi(\vec{x}, u, g)$ and $\forall g \in A \exists u \in y\, \psi(\vec{x}, u, g)$. Let $f_0 = \bigcup\{g : g \in A\}$. By our general assumption there exists a u_0 such that $G(\vec{x}, y, (f_0(u) | u \in y)) = u_0$. Set $f = f_0 \cup \{\langle y, u_0 \rangle\}$.

[6] $(F(\vec{x}, z) | z \in y) \;:=\; \{\langle z, F(\vec{x}, z)\rangle : z \in y\}$

Since for all $g \in A$, $\mathrm{dom}(g)$ is transitive we have that $\mathrm{dom}(f_0)$ is transitive. If $u \in y$, then $u \in \mathbf{dom}(f_0)$. Thus $\mathbf{dom}(f)$ is transitive and $y \in \mathbf{dom}(f)$. We have to show that f is a function. But it is readily shown that if $g_0, g_1 \in A$, then $\forall x \in \mathbf{dom}(g_0) \cap \mathbf{dom}(g_1)[g_0(x) = g_1(x)]$. Therefore f is a function. This also shows that $\forall w \in \mathbf{dom}(f)[f(w) = G(\vec{x}, w, f \restriction w)]$, confirming the claim (using Set Induction).

Now define F by

$$F(\vec{x}, y) = w \;\; := \;\; \exists f[\psi(\vec{x}, y, f) \wedge f(y) = w].$$

$\square$

Corollary: 18.9 *There is a* Σ *function* **TC** *of* **IKP** *such that*

$$\mathbf{IKP} \vdash \forall a[\mathbf{TC}(a) = a \cup \bigcup\{\mathbf{TC}(x) : x \in a\}].$$

Proposition: 18.10 (Definition by **TC**–Recursion) *Under the assumptions of Proposition 18.8 there is an* $(n+1)$*–ary* Σ *class function* F *of* **IKP** *such that*

$$\mathbf{IKP} \vdash \forall \vec{x} y[F(\vec{x}, y) = G(\vec{x}, y, (F(\vec{x}, z) | z \in \mathbf{TC}(y)))].$$

Proof: Let $\theta(f, \vec{x}, y)$ be the Σ formula

$$[f \text{ is a function}] \wedge [\mathbf{dom}(f) = \mathbf{TC}(y)] \wedge [\forall u \in \mathbf{dom}(f)[f(u) = G(\vec{x}, u, f \restriction \mathbf{TC}(u))]].$$

Prove by $\in$–induction that $\forall y \exists! f\, \theta(f, \vec{x}, y)$. Suppose $\forall v \in y\, \exists! g\, \theta(g, \vec{x}, v)$. We then have

$$\forall v \in y \exists! a \exists g[\theta(g, \vec{x}, v) \wedge G(\vec{x}, v, g) = a].$$

By Σ Replacement there is a function h such that $\mathbf{dom}(h) = y$ and

$$\forall v \in y\, \exists g\, [\theta(g, \vec{x}, v) \wedge G(\vec{x}, v, g) = h(v)]\,.$$

Employing Strong Collection to $\forall v \in y\, \exists! g\; \theta(g, \vec{x}, v)$ also provides us with a set A such that $\forall v \in y\, \exists g \in A\, \theta(g, \vec{x}, v)$ and $\forall g \in A\, \exists v \in y\, \theta(g, \vec{x}, v)$. Now let $f = (\bigcup\{g : g \in A\}) \cup h$. Then $\theta(f, \vec{x}, y)$. $\square$

Definition: 18.11 Let T be a theory whose language comprises the language of set theory and let $\phi(x_1, \ldots, x_n, y)$ be a Σ formula such that

$$T \vdash \forall x_1 \ldots \forall x_n\, \exists! y\, \phi(x_1, \ldots, x_n, y).$$

Let `f` be a new n-ary function symbol and define `f` by:

$$\forall x_1 \ldots \forall x_n\, \forall y\, [\mathtt{f}(x_1, \ldots, x_n) = y \leftrightarrow \phi(x_1, \ldots, x_n, y)].$$

`f` is then called a Σ *function symbol* of T.

It is an important property of classical Kripke-Platek set theory that Σ function symbols can be treated as though they were atomic symbols of the basic language, thereby expanding the notion of Δ_0 formula. The usual proofs of this fact employ Δ_1 Separation (cf. [7], I.5.4). As this principle is not available in **IKP** some care has to be exercised in obtaining the same results for $\mathbf{IKP}_0$ and **IKP**.

Proposition: 18.12 (Extension by Σ Function Symbols) *Let T be a theory obtained from one of the theories $\mathbf{IKP}_0$ or* **IKP** *by iteratively adding Σ function symbols. Suppose $T \vdash \forall\vec{x}\,\exists! y\,\Phi(\vec{x}, y)$, where Φ is a Σ formula. Let T_Φ be obtained by adjoining a Σ function symbol F_Φ to the language, extending the schemata to the enriched language, and adding the axiom $\forall\vec{x}\;\Phi(\vec{x}, F_\Phi(\vec{x}\,))$. Then T_Φ is conservative over T.*

Proof: We define the following translation * for formulas of T_Φ:

$$\begin{aligned} \phi^* &\equiv \phi \text{ if } F_\Phi \text{ does not occur in } \phi \\ (F_\Phi(\vec{x}\,) = y)^* &\equiv \Phi(\vec{x}, y) \end{aligned}$$

If ϕ is of the form $t = x$ with $t \equiv G(t_1, \ldots, t_k)$ such that one of the terms $t_1, \ldots, t_k$ is not a variable, then let

$$(t = x)^* \equiv \exists x_1 \ldots \exists x_k\,[(t_1 = x_1)^* \wedge \cdots \wedge (t_k = x_k)^* \wedge (G(x_1, \ldots, x_k) = x)^*]\,.$$

The latter provides a definition of $(t = x)^*$ by induction on t. If either t or s contains F_Φ, then let

$$\begin{aligned} (t \in s)^* &\equiv \exists x \exists y[(t = x)^* \wedge (s = y)^* \wedge x \in y], \\ (t = s)^* &\equiv \exists x \exists y[(t = x)^* \wedge (s = y)^* \wedge x = y], \\ (\neg\phi)^* &\equiv \neg\phi^* \\ (\phi_0 \Box \phi_1)^* &\equiv \phi_0^* \Box \phi_1^*, \quad \text{if } \Box \text{ is } \wedge, \vee, \text{ or } \rightarrow \\ (\exists x\phi)^* &\equiv \exists x\phi^* \\ (\forall x\phi)^* &\equiv \forall\phi^*. \end{aligned}$$

Let T_Φ^- be the restriction of T_Φ, where F_Φ is not allowed to occur in the Δ_0 Separation Scheme and the Δ_0 Collection Scheme. Then it is obvious that $T_\Phi^- \vdash \phi$ implies $T \vdash \phi^*$. So it remains to show that T_Φ^- proves the same theorems as T_Φ. We first prove $T_\Phi^- \vdash \exists x \forall y\,[y \in x \leftrightarrow y \in a \wedge \phi(a)]$ for any Δ_0 formula ϕ of T_Φ. *For* **IKP** *we also have to consider Δ_0 Collection.*

We proceed by induction on ϕ.

1. $\phi(y) \equiv t(y) \in s(y)$. Now

$$T_\Phi \vdash \forall y \in a \exists! z[(z = t(y)) \wedge \forall y \in a \exists! u(u = s(y))].$$

Using Σ Replacement (*Some more arguments might be in order here to show that $z = t(y)$ is equivalent to a Σ formula*) we find functions f and g such that

$$\mathbf{dom}(f) = \mathbf{dom}(g) = a \text{ and } \forall y \in a\,[f(y) = t(y) \wedge g(y) = s(y)]\,.$$

Therefore $\{y \in a : \phi(y)\} = \{y \in a : f(y) \in g(y)\}$ exists by Δ_0 Separation in T_Φ^-.

2. $\phi(y) \equiv t(y) = s(y)$. Similar.

3. $\phi(y) \equiv \phi_0(y) \Box \phi_1(y)$, where $\Box$ is any of $\wedge, \vee, \rightarrow$. This is immediate by induction hypothesis.

4. $\phi(y) \equiv \forall u \in t(y)\ \phi_0(u, y)$. We find a function f such that $\mathbf{dom}(f) = a$ and $\forall y \in a\, f(y) = t(y)$. Inductively, for all $b \in a$, $\{u \in \bigcup \mathbf{ran}(f) : \phi_0(u, b)\}$ is a set. Hence there is a function g with $\mathbf{dom}(g) = a$ and $\forall b \in a\, g(b) = \{u \in \bigcup \mathbf{ran}(f) : \phi_0(u, b)\}$. Then $\{y \in a : \phi(y)\} = \{y \in a : \forall u \in f(y)(u \in g(y))\}$.

5. $\phi(y) \equiv \exists u \in t(y)\, \phi_0(u, y)$. With f and g as above, $\{y \in a : \phi(y)\} = \{y \in a : \exists u \in f(y)(u \in g(y))\}$.

$\Box$

Remark: 18.13 The proof of Proposition 18.12 shows that the process of adding defined function symbols to **IKP** or $\mathbf{IKP}_0$ can be iterated. So if e.g. $T_\Phi \vdash \forall \vec{x} \exists y\, \psi(\vec{x}, y)$ for a Δ_0 formula of T_Φ, then also $T_\Phi + \{\forall \vec{x} \exists y\, \psi(\vec{x}, F_\psi(\vec{x}))\}$ will be conservative over T.

18.3 Inductive Definitions in IKP

Here we investigate some parts of the theory of inductive definitions which can be developed in **IKP**.

An *inductive definition* Φ is a class of pairs. Intuitively an inductive definition is an abstract proof system, where $\langle x, A\rangle \in \Phi$ means that A is a set of premises and x is a Φ-consequence of these premises.

Φ is a Σ inductive definition if Φ is a Σ definable class.

A class X is said to be Φ-*closed* if $A \subseteq X$ implies $a \in X$ for every pair $\langle a, A\rangle \in \Phi$.

Theorem: 18.14 (**IKP**) *For any* Σ *inductive definition* Φ *there is a smallest* Φ*-closed class* $\mathbf{I}(\Phi)$*; moreover,* $\mathbf{I}(\Phi)$ *is a* Σ *class as well.*

Proof: Call a set relation G *good* if whenever $\langle x, y\rangle \in G$ there is a set A such that $\langle y, A\rangle \in \Phi$ and

$$\forall u \in A\, \exists v \in x\ \langle v, u\rangle \in G.$$

Call a set Φ-*generated* if it is in the range of some good relation. Note that the notion of being a good set relation and of being a Φ-generated set are both Σ definable.

To see that the class of Φ-generated sets is Φ-closed, let A be a set of Φ-generated sets, where $\langle a, A\rangle \in \Phi$. Then

$$\forall y \in A\, \exists G\, [G \text{ is good } \wedge\ \exists x\, (\langle x, y\rangle \in G)].$$

Thus, by Strong Σ Collection, there is a set C of good sets such that

$$\forall y \in A\, \exists G \in C\, \exists x\, (\langle x, y\rangle \in G).$$

Letting $G_0 = \bigcup C \cup \{\langle b, a\rangle\}$, where $b = \{u : \exists y\, \langle u, y\rangle \in \bigcup C\}$, G_0 is good and $\langle b, a\rangle \in G_0$. Thus a is Φ-generated. Whence $\mathbf{I}(\Phi)$ is Φ-closed. Now if X is another Φ-closed class and G is good, then by set induction on x it follows that $\langle x, y\rangle \in G$ implies $y \in X$, so that $\mathbf{I}(\Phi) \subseteq X$. $\square$

Theorem: 18.15 (**IKP**) *Let* Φ *be a* Σ *inductive definition. For any class* X *define*

$$\Gamma_\Phi(X) = \{y|\ \exists A\, (\langle y, A\rangle \in \Phi\ \wedge\ A \subseteq X)\}.$$

Then there exists a unique Σ *class* K *such that*

$$K^a \quad = \quad \Gamma_\Phi(\bigcup_{x\in a} K^x) \tag{29}$$

holds for all sets b*, where* $K^a = \{u|\ \langle a, u\rangle \in K\}$*. Moreover, it holds* $\mathbf{I}(\Phi) = \bigcup_a K^a$*.*

Proof: Uniqueness is obvious by Set Induction on a. Let $\Gamma = \Gamma_\Phi$. Note that Γ is monotone, i.e., if $X \subseteq Y$ then $\Gamma(X) \subseteq \Gamma(Y)$. Define

$$K = \bigcup\{G|\ G \text{ is a good set}\}.$$

We first show (29).

"$\subseteq$": Let $z \in K^a$. Then there exists a good set G such that $\langle a, z\rangle \in G$. Hence $z \in \Gamma(\bigcup_{b\in a} G^b)$. Since $\bigcup_{b\in} G^b \subseteq \bigcup_{b\in a} K^b$ and Γ is monotone we get $z \in \Gamma(\bigcup_{b\in a} K^b)$.

"$\supseteq$": Let $z \in \Gamma(\bigcup_{b\in a} K^b)$. Then there exists a set $A \subseteq \bigcup_{b\in a} K^b$ such that $\langle z, A\rangle \in \Phi$. Furthermore

$$\forall u \in A\, \exists G\, [G \texttt{ is good} \wedge \exists x \in a\, \langle x, u\rangle \in G].$$

Hence, using Strong Σ Collection, there exists a set Z such that

$$\forall u \in A\, \exists G \in Z\, [G \texttt{ is good} \wedge \exists x \in a\, \langle x, u\rangle \in G]$$

and, moreover, all sets in Z are good. Put

$$G_0 = \bigcup Z \cup \{\langle a, z\rangle\}.$$

Then $A \subseteq \bigcup_{b\in a} G_0^b$. We claim that G_0 is good. To see this let $\langle c, w\rangle \in G_0$. Then $(\exists G \in Z\, \langle c, w\rangle \in G) \vee \langle c, w\rangle = \langle a, z\rangle$. Thus $(\exists G \in Z\, w \in \Gamma(\bigcup_{x\in c} G^x) \vee w \in \Gamma(A)$, and hence $w \in \Gamma(\bigcup_{x\in c} G_0^x)$, showing that G_0 is good. Now, since $z \in G_0^a$ and G_0 is good it follows $z \in K^a$.

Using (29) one shows by set induction on a that $K^a \subseteq \mathbf{I}(\Phi)$, yielding $\bigcup_a K^a \subseteq \mathbf{I}(\Phi)$. For the reverse inclusion it suffices to show that $\bigcup_{u\in b} K^u$ is Φ-closed. So let $z \in \Gamma(\bigcup_a K^a)$. Then there exists a set $A \subseteq \bigcup_a K^a$ such that $\langle z, A\rangle \in \Phi$. Since $\forall u \in A\, \exists x\, u \in K^x$, by Σ Collection we can find a set b such that $\forall u \in A\, \exists x \in b\, u \in K^x$. Whence $A \subseteq \bigcup_{u\in b} K^b$. Consequently we have $z \in \Gamma(\bigcup_{u\in b} K^b) = K^b$ by (29), showing that $\bigcup_{u\in b} K^u$ is Φ-closed. $\Box$

The section K^b of the above class will be denoted by Γ_Φ^b.

Corollary: 18.16 (**IKP**) *If for every set x, $\Gamma_\Phi(x)$ is a set then the assignment $b \mapsto \Gamma_\Phi^b$ defines a Σ function.*

Proof: Obvious. $\Box$

19 Anti-Foundation

A very systematic toolbox for building models of various circular phenomena is set theory with the *Anti-Foundation axiom.* Theories as **ZF** outlaw sets like $\Omega = \{\Omega\}$ and infinite chains of the form $\Omega_{i+1} \in \Omega_i$ for all $i{\in}\omega$ on account of the Foundation axiom, and sometimes one hears the mistaken opinion that the only coherent conception of sets precludes such sets. The fundamental distinction between well-founded and non-well-founded sets was formulated by Mirimanoff in 1917. The relative independence of the Foundation axiom from the other axioms of Zermelo-Fraenkel set theory was announced by Bernays in 1941 but did not appear until the 1950s. Versions of axioms asserting the existence of non-well-founded sets were proposed by Finsler (1926). The ideas of Bernays' independence proof were exploited by Rieger, Hájek, Boffa, and Felgner. After Finsler, Scott in 1960 appears to have been the first person to consider an anti-foundation axiom which encapsulates a strengthening of the axiom of extensionality. The anti-foundation axiom in its strongest version was first formulated by Forti and Honsell [29] in 1983. Though several logicians explored set theories whose universes contained non-wellfounded sets (or hypersets as they are called nowadays) the area was considered rather exotic until these theories were put to use in developing rigorous accounts of circular notions in computer science (cf. [4]). It turned out that the *Anti-Foundation Axiom,* **AFA**, gives rise to a rich universe of sets and provides an elegant tool for modelling all sorts of circular phenomena. The application areas range from modal logic, knowledge representation and theoretical economics to the semantics of natural language and programming languages. The subject of hypersets and their applications is thoroughly developed in the books [4] by P. Aczel and [8] by J. Barwise and L. Moss.

[4] and [8] give rise to the question whether the material could be developed on the basis of a constructive universe of hypersets rather than a classical and impredicative one. This paper explores whether **AFA** and the most important tools emanating from it, such as the solution lemma and the co-recursion principle, can be developed on predicative grounds, that is to say, within a predicative theory of sets. The upshot is that most of the circular phenomena that have arisen in computer science don't require impredicative set existence axioms for their modelling, thereby showing that their circularity is clearly of a different kind than the one which underlies impredicative definitions.

19.1 The anti-foundation axiom

Definition: 19.1 A *graph* will consist of a set of *nodes* and a set of *edges*, each edge being an ordered pair $\langle x, y\rangle$ of nodes. If $\langle x, y\rangle$ is an edge then we will write $x \to y$ and say that y is a *child* of x.

A *path* is a finite or infinite sequence $x_0 \to x_1 \to x_2 \to \ldots$ of nodes $x_0, x_1, x_2, \ldots$ linked by edges $\langle x_0, x_1\rangle, \langle x_1, x_2\rangle, \ldots$.

A *pointed graph* is a graph together with a distinguished node x_0 called its *point*. A pointed graph is *accessible* if for every node x there is a path $x_0 \to x_1 \to x_2 \to \ldots \to x$ from the point x_0 to x.

A *decoration* of a graph is an assignment d of a set to each node of the graph in such a way that the elements of the set assigned to a node are the sets assigned to the children of that node, i.e.

$$d(a) = \{d(x) : \ a \to x\}.$$

A *picture* of a set is an accessible pointed graph (apg for short) which has a decoration in which the set is assigned to the point.

Definition: 19.2 The *Anti-Foundation Axiom*, **AFA**, is the statement that every graph has a unique decoration.

Note that **AFA** has the consequence that every apg is a picture of a unique set.

AFA is in effect the conjunction of two statements:

- $\mathbf{AFA}_1$: *Every graph has at least one decoration.*
- $\mathbf{AFA}_2$: *Every graph has a most one decoration.*

$\mathbf{AFA}_1$ is an existence statement whereas $\mathbf{AFA}_2$ is a strengthening of the Extensionalty axiom of set theory. For example, taking the graph $\mathbb{G}_0$ to consist of a single node x_0 and one edge $x_0 \to x_0$, $\mathbf{AFA}_1$ ensures that this graph has a decoration $d_0(x) = \{d_0(y) : \ x \to y\} = \{d_0(x)\}$, giving rise to a set b such that $b = \{b\}$. However, if there is another set c satisfying $c = \{c\}$, the Extensionalty axiom does not force b to be equal to c, while $\mathbf{AFA}_2$ yields $b = c$. Thus, by **AFA** there is exactly one set Ω such that $\Omega = \{\Omega\}$.

Another example which demonstrates the extensionalizing effect of $\mathbf{AFA}_2$ is provided by the graph $\mathbb{G}_\infty$ which consists of the infinitely many nodes x_i and the edges $x_i \to x_{i+1}$ for each $i{\in}\omega$. According to $\mathbf{AFA}_1$, $\mathbb{G}_\infty$ has a decoration. As $d_\infty(x_i) = \Omega$ defines such a decoration, $\mathbf{AFA}_2$ entails that this is the only one, whereby the different graphs $\mathbb{G}_0$ and $\mathbb{G}_\infty$ give rise to the same non-well-founded set.

The most important applications of **AFA** arise in connection with solving systems of equations of sets. In a nutshell, this is demonstrated by the following example. Let p and q be arbitrary fixed sets. Suppose we need sets x, y, z such that

$$\begin{aligned} x &= \{x, y\} \\ y &= \{p, q, y, z\} \\ z &= \{p, x, y\}. \end{aligned} \tag{30}$$

Here p and q are best viewed as atoms while x, y, z are the indeterminates of the system. **AFA** ensures that the system (30) has a unique solution. There is a powerful technique that can be used to show that systems of equations of a certain type have always unique solutions. In the terminology of [8] this is called the *solution lemma*. We shall prove it in the sections on applications of **AFA**.

19.1.1 The theory CZFA

We shall introduce a constructive set theory with **AFA** instead of $\in$-Induction.

Definition: 19.3 Recall that $\mathbf{CZF}^-$ is the system **CZF** without the $\in$ - Induction scheme. According to Theorem 6.21, $\mathbf{CZF}^-$ is strong enough to show the existence of any primitive recursive functions on $\mathbb{N}$ but unfortunately it has certain defects from a mathematical point of view in that this theory appears to be too limited for proving proving the existence of the transitive closure of an arbitrary set (see Definition 6.26). To remedy this we shall consider an axiom, TRANS, which ensures that every set is contained in a transitive set:

$$\text{TRANS} \qquad \forall x\, \exists y\, [x \subseteq y \wedge (\forall u{\in}y)\, (\forall v{\in}u)\, v{\in}y].$$

Let **CZFA** be the theory $\mathbf{CZF}^- + \text{TRANS} + \mathbf{AFA}$.

Lemma: 19.4 *Let* $\mathbf{TC}(x)$ *stand for the smallest transitive set that contains all elements of* x*.* $\mathbf{ECST} + \mathbf{FPA} + \text{TRANS}$ *proves the existence of* $\mathbf{TC}(x)$ *for any set* x*.*

Proof: Let x be an arbitrary set. By TRANS there exists a transitive set A such that $x \subseteq A$. For $n{\in}\omega$ let

$$\begin{aligned} B_n &= \{f \in {}^{n+1}A : f(0) \in x \wedge (\forall i{\in}n)\, f(i+1) \in f(i)\}, \\ \mathbf{TC}_n(x) &= \bigcup \{\mathbf{ran}(f) : f \in B_n\}, \end{aligned}$$

where $\mathbf{ran}(f)$ denotes the range of a function f. B_n is a set owing to **FPA** and Δ_0 Separation, thus $\mathbf{TC}_n(x)$ is a set by Union. Furthermore, $C = \bigcup_{n\in\omega} \mathbf{TC}_n(x)$ is a set by Replacement and Union. Then $x = \mathbf{TC}_0(x) \subseteq C$. Let y be a transitive set such that $x \subseteq y$. By induction on n one easily verifies that $\mathbf{TC}_n(x) \subseteq y$, and hence $C \subseteq y$. Moreover, C is transitive. Thus C is the smallest transitive set which contains all elements of x. $\square$

In what follows, we will rummage through several applications of **AFA** made in [4] and [8]. In order to corroborate the claim that most applications of **AFA** require only constructive means, various sections of [4] and [8] are recast on the basis of the theory **CZFA** rather than **ZFA**.

19.2 The Labelled Anti-Foundation Axiom

In applications it is often useful to have a more general form of **AFA** at ones disposal.

Definition: 19.5 A *labelled graph* is a graph together with a labelling function ℓ which assigns a set $\ell(a)$ of *labels* to each node a.

A *labelled decoration* of a labelled graph is a function d such that

$$d(a) \quad = \quad \{d(b) : a \to b\} \cup \ell(a).$$

An unlabelled graph $(G, \rightsquigarrow)$ may be identified with the special labelled graph where the labelling function $\ell : G \to V$ always assigns the empty set, i.e. $\ell(x) = \emptyset$ for all $x \in G$.

Theorem: 19.6 (**CZFA**) (Cf. [4], Theorem 1.9) *Each labelled graph has a unique labelled decoration.*

Proof: Let $\mathbb{G} = (G, \rightsquigarrow, \ell)$ be a labelled graph. Let $\mathbb{G}' = (G', \to)$ be the graph having as nodes all the ordered pairs $\langle i, a\rangle$ such that either $i = 1$ and $a \in G$ or $i = 2$ and $a \in \mathbf{TC}(G)$ and having as edges:

- $\langle 1, a\rangle \to \langle 1, b\rangle$ whenever $a \rightsquigarrow b$,
- $\langle 1, a\rangle \to \langle 2, b\rangle$ whenever $a \in G$ and $b \in \ell(a)$,
- $\langle 2, a\rangle \to \langle 2, b\rangle$ whenever $b \in a \in \mathbf{TC}(G)$.

By **AFA**, $\mathbb{G}'$ has a unique decoration π. So for each $a \in G$

$$\pi(\langle 1, a\rangle) \ = \ \{\pi(\langle 1, b\rangle) : a \rightsquigarrow b\} \ \cup \ \{\pi(\langle 2, b\rangle) : b \in \ell(a)\}$$

and for each $a \in \mathbf{TC}(G)$,

$$\pi(\langle 2, a\rangle) \;=\; \{\pi(\langle 2, b\rangle) \;:\; b{\in}a\}.$$

Note that the set $\mathbf{TC}(G)$ is naturally equipped with a graph structure by letting its edges $x \multimap y$ be defined by $y{\in}x$. The unique decoration for $(\mathbf{TC}(G), \multimap)$ is obviously the identity function on $\mathbf{TC}(G)$. As $x \mapsto \pi(\langle 2, x\rangle)$ is also a decoration of $(\mathbf{TC}(G), \multimap)$ we can conclude that $\pi(\langle 2, x\rangle) = x$ holds for all $x \in \mathbf{TC}(G)$. Hence if we let $\tau(a) = \pi(\langle 1, a\rangle)$ for $a{\in}G$ then, for $a{\in}G$,

$$\tau(a) \;=\; \{\tau(b) \;:\; a \rightsquigarrow b\} \;\cup\; \ell(a),$$

so that τ is a labelled decoration of the labelled graph $\mathbb{G}$.

For the uniqueness of τ suppose that τ' is a labelled decoration of $\mathbb{G}$. Then π' is a decoration of the graph $\mathbb{G}'$, where

$$\begin{array}{rcl}\pi'(\langle 1, a\rangle) & = & \tau'(a) \text{ for } a{\in}G,\\ \pi'(\langle 2, a\rangle) & = & a \text{ for } a \in \mathbf{TC}(G).\end{array}$$

It follows from **AFA** that $\pi' = \pi$ so that for $a{\in}G$

$$\tau'(a) = \pi'(\langle 1, a\rangle) = \pi(\langle 1, a\rangle) = \tau(a),$$

and hence $\tau' = \tau$. □

Definition: 19.7 A relation R is a *bisimulation* between two labelled graphs $\mathbb{G} = (G, \rightsquigarrow, \ell_0)$ and $\mathbb{H} = (H, \multimap, \ell_1)$ if $R \subseteq G \times H$ and the following conditions are satisfied (where aRb stands for $\langle a, b\rangle \in R$):

1. For every $a \in G$ there is a $b \in H$ such that aRb.
2. For every $b \in H$ there is a $a \in G$ such that aRb.
3. Suppose that aRb. Then for every $x \in G$ such that $a \rightsquigarrow x$ there is a $y \in H$ such that $b \multimap y$ and xRy.
4. Suppose that aRb. Then for every $y \in H$ such that $b \multimap y$ there is an $x \in G$ such that $a \rightsquigarrow x$ and xRy.
5. If aRb then $\ell_0(a) = \ell_1(b)$.

Two labelled graphs are *bisimular* if there exists a bisimulation between them.

Theorem: 19.8 (**CZFA**) *Let $\mathbb{G} = (G, \rightsquigarrow, \ell_0)$ and $\mathbb{H} = (H, \multimap, \ell_1)$ be labelled graphs with labelled decorations d_0 and d_1, respectively.*

If $\mathbb{G}$ and $\mathbb{H}$ are bisimular then $d_0[G] = d_1[H]$.

Proof: Define a labelled graph $\mathbb{K} = (K, \rightarrow, \ell)$ by letting K be the set $\{\langle a, b\rangle : aRb\}$. For $\langle a, b\rangle, \langle a', b'\rangle \in K$ let $\langle a, b\rangle \rightarrow \langle a', b'\rangle$ iff $a \rightsquigarrow a'$ or $b \multimap b'$, and put $\ell(\langle a, b\rangle) = \ell_0(a) = \ell_1(b)$. $\mathbb{K}$ has a unique labelled decoration d. Using a bisimulation R, one easily verfies that $d_0^*(\langle a, b\rangle) := d_0(a)$ and $d_1^*(\langle a, b\rangle) := d_1(b)$ are labelled decorations of $\mathbb{K}$ as well. Hence $d = d_0^* = d_1^*$, and thus $d_0[G] = d[K] = d_1[H]$. □

Corollary: 19.9 (**CZFA**) *Two graphs are bisimular if and only if their decorations have the same image.*

Proof: One direction follows from the previous theorem. Now suppose we have graphs $\mathbb{G} = (G, \rightsquigarrow)$ and $\mathbb{H} = (H, \multimap)$ with decorations d_0 and d_1, respectively, such that $d_0[G] = d_1[H]$. The define $R \subseteq G \times H$ by aRb iff $d_0(a) = d_1(b)$. One readily verifies that R is a bisimulation. □

Here is another useful fact:

Lemma: 19.10 (**CZFA**) *If A is transitive set and $d : A \rightarrow V$ is a function such that $d(a) = \{d(x) : x \in a\}$ for all $a \in A$, then $d(a) = a$ for all $a \in A$.*

Proof: A can be considered the set of nodes of the graph $\mathbb{G}_A = (A, \multimap)$ where $a \multimap b$ iff $b \in a$ and $a, b \in A$. Since A is transitive, d is a decoration of $\mathbb{G}$. But so is the function $a \mapsto a$. Thus we get $d(a) = a$. □

19.3 Systems

In applications it is often useful to avail oneself of graphs that are classes rather than sets. By a *map* $\wp$ with domain M we mean a definable class function with domain M, and we will write $\wp : M \rightarrow V$.

Definition: 19.11 A *labelled system* is a class M of nodes together with a labelling map $\wp : M \rightarrow V$ and a class E of edges consisting of ordered pairs of nodes. Furthermore, a system is required to satisfy that for each node $a \in M$, $\{b \in M : a \multimap b\}$ is a set, where $a \multimap b$ stands for $\langle a, b\rangle \in E$.

The labelled system is said to be Δ_0 if the relation between sets x and y defined by "$y = \{b \in M : a \multimap b$ for some $a \in x\}$" is Δ_0 definable.

We will abbreviate the labelled system by $\mathbb{M} = (M, \multimap, \wp)$.

Theorem: 19.12 (**CZFA** + $\mathbf{IND}_\omega$) (Cf. [4], Theorem 1.10) *For every labelled system* $\mathbb{M} = (M, \multimap, \wp)$ *there exists a unique map* $d : M \to V$ *such that, for all* $a \in M$*:*

$$d(a) \quad = \quad \{d(b) \,:\, a \to b\} \cup \ell(a). \tag{31}$$

Proof: To each $a \in M$ we may associate a labelled graph $\mathbb{M}_a = (M_a, {}_a\!\multimap, \wp_a)$ with $M_a = \bigcup_{n\in\omega} X_n$, where $X_0 = \{a\}$ and $X_{n+1} = \{b : a \multimap b \text{ for some } a \in X_n\}$. The existence of the function $n \mapsto X_n$ is shown via recursion on ω, utilizing $\mathbf{IND}_\omega$ in combination with Strong Collection. The latter is needed to show that for every set Y, $\{b : a \multimap b \text{ for some } a \in Y\}$ is a set as well. And consequently to that M_a is a set. ${}_a\!\multimap$ is the restriction of $\multimap$ to nodes from M_a. That $E_a = \{\langle x, y\rangle \in M_a \times M_a \,:\, x \multimap y\}$ is a set requires Strong Collection, too. Further, let $\wp_a$ be the restriction of $\wp$ to M_a. Hence $\mathbb{M}_a$ is a set and we may apply Theorem 19.6 to conclude that $\mathbb{M}_a$ has a unique labelled decoration d_a. $d : M \to V$ is now obtained by patching together the function d_a with $a \in M$, that is $d = \bigcup_{a\in V} d_a$. One easily shows that two function d_a and d_b agree on $M_a \cap M_b$. For the uniqueness of d, notice that every other definable map d' satisfying (31) yields a function when restricted to M_a (Strong Collection) and thereby yields also a labelled decoration of $\mathbb{M}_a$; thus $d'(x) = \wp_a(x) = d(x)$ for all $x \in M_a$. And consequently to that, $d'(x) = d(x)$ for all $x \in M$. □

Corollary: 19.13 (**CZFA**+Σ-$\mathbf{IND}_\omega$) *For every labelled system* $\mathbb{M} = (M, \multimap, \wp)$ *that is* Δ_0 *there exists a unique map* $d : M \to V$ *such that, for all* $a \in M$*:*

$$d(a) \quad = \quad \{d(b) \,:\, a \multimap b\} \cup \ell(a). \tag{32}$$

Proof: This follows by scrutinizing the proof of Theorem 19.12 and realizing that for a Δ_0 system one only needs Σ-$\mathbf{IND}_\omega$. □

Corollary: 19.14 (**CZFA**) *Let* $\mathbb{M} = (M, \multimap, \wp)$ *be a labelled* Δ_0 *system such that for each* $a \in M$ *there is a function* $n \mapsto X_n$ *with domain* ω *such that* $X_0 = \{a\}$ *and* $X_{n+1} = \{b : a \multimap b \text{ for some } a \in X_n\}$*. Then there exists a unique map* $d : M \to V$ *such that, for all* $a \in M$*:*

$$d(a) \quad = \quad \{d(b) \,:\, a \to b\} \cup \ell(a). \tag{33}$$

Proof: In the proof of Theorem 19.12 we employed $\mathbf{IND}_\omega$ only once to ensure that $M_a = \bigcup_{n\in\omega} X_n$ is a set. This we get now from the assumptions. □

Theorem: 19.15 (**CZFA+IND**$_\omega$) (Cf. [4], Theorem 1.11) *Let* $\mathbb{M} = (M, \rightsquigarrow, \wp)$ *be a labelled system whose sets of labels are subsets of the class* Y.

1. *If* π *is a map with domain* Y *then there is a unique function* $\hat{\pi}$ *with domain* M *such that for each* $a \in M$

$$\hat{\pi}(a) \;=\; \{\hat{\pi}(b) \;:\; a \rightsquigarrow b\} \;\cup\; \{\pi(x) \;:\; x \in \wp(a)\}.$$

2. *Given a map* $\hbar : Y \to M$ *there is a unique map* π *with domain* Y *such that for all* $y \in Y$,

$$\pi(y) \;=\; \hat{\pi}(\hbar(y)).$$

Proof: For (1) let $\mathbb{M}_\pi = (M, \rightsquigarrow, \wp_\pi)$ be obtained from $\mathbb{M}$ and $\pi : Y \to V$ by redefining the sets of labels so that for each node a

$$\wp_\pi(a) \;=\; \{\pi(x) \;:\; x \in \wp(a)\}.$$

Then the required unique map $\hat{\pi}$ is the unique labelled decoration of $\mathbb{M}_\pi$ provided by Theorem 19.12

For (2) let $\mathbb{M}^* = (M, \multimap)$ be the graph having the same nodes as $\mathbb{M}$, and all edges of $\mathbb{M}$ together with the edges $a \multimap \hbar(y)$ whenever $a \in M$ and $y \in \wp(a)$. By Theorem 19.12, $\mathbb{M}^*$ has a unique decoration map ρ. So for each $a \in M$

$$\rho(a) \;=\; \{\rho(b) \;:\; a \rightsquigarrow b\} \;\cup\; \{\rho(\hbar(y)) \;:\; y \in \wp(a)\}.$$

Letting $\pi(y) := \rho(\hbar(y))$ for $y \in Y$, ρ is also a labelled decoration for the labelled system $\mathbb{M}_\pi$ so that $\rho = \hat{\pi}$ by (1), and hence $\pi(x) = \hat{\pi}(\hbar(x))$ for $x \in Y$. For the uniqueness of π let $\mu : M \to V$ satisfy $\mu(x) = \hat{\mu}(\hbar(x))$ for $x \in Y$. Then $\hat{\mu}$ is a decoration of $\mathbb{M}^*$ as well, so that $\hat{\mu} = \rho$. As a result $\mu(x) = \hat{\mu}(\hbar(x)) = \rho(\hbar(x)) = \pi(x)$ for $x \in Y$. Thus $\mu(x) = \pi(x)$ for all $x \in Y$. $\square$

Corollary: 19.16 (**CZFA** + Σ-**IND**$_\omega$) *Let* $\mathbb{M} = (M, \rightsquigarrow, \wp)$ *be a labelled system that is* Δ_0 *and whose sets of labels are subsets of the class* Y.

1. *If* π *is a map with domain* Y *then there is a unique function* $\hat{\pi}$ *with domain* M *such that for each* $a \in M$

$$\hat{\pi}(a) \;=\; \{\hat{\pi}(b) \;:\; a \rightsquigarrow b\} \;\cup\; \{\pi(x) \;:\; x \in \wp(a)\}.$$

2. *Given a map* $\hbar : Y \to M$ *there is a unique map* π *with domain* Y *such that for all* $x{\in}Y$,
$$\pi(x) \;=\; \hat{\pi}(\hbar(x)).$$

Proof: The proof is the same as for Theorem 19.15, except that one utilizes Corollary 19.13 in place of Theorem 19.12. □

Corollary: 19.17 (**CZFA**) *Let* $\mathbb{M} = (M, \rightsquigarrow, \wp)$ *be a labelled system that is* Δ_0 *and whose sets of labels are subsets of the class* Y. *Moreover suppose that for each* $a \in M$ *there is a function* $n \mapsto X_n$ *with domain* ω *such that* $X_0 = \{a\}$ *and* $X_{n+1} = \{b : a \multimap b$ *for some* $a \in X_n\}$.

1. *If* π *is a map with domain* Y *then there is a unique function* $\hat{\pi}$ *with domain* M *such that for each* $a{\in}M$
$$\hat{\pi}(a) \;=\; \{\hat{\pi}(b) \,:\, a \rightsquigarrow b\} \;\cup\; \{\pi(x) \,:\, x \in \wp(a)\}.$$

2. *Given a map* $\hbar : Y \to M$ *there is a unique map* π *with domain* Y *such that for all* $x{\in}Y$,
$$\pi(x) \;=\; \hat{\pi}(\hbar(x)).$$

Proof: The proof is the same as for Theorem 19.15, except that one utilizes Corollary 19.14 in place of Theorem 19.12. □

19.4 A Solution Lemma version of AFA

AFA can be couched in more traditional mathematical terms. The labelled Anti-Foundation Axiom provides a nice tool for showing that systems of equations of a certain type have always unique solutions. In the terminology of [8] this is called the *solution lemma*. In [8], the Anti-Foundation Axiom is even expressed in terms of unique solutions to so-called *flat systems of equations*.

Definition: 19.18 For a set Y let $\mathcal{P}(Y)$ be the class of subsets of Y. A triple $\mathcal{E} = (X, A, e)$ is said to be a *general flat system of equations* if X and A are any two sets, and $e : X \to \mathcal{P}(X \cup A)$, where the latter conveys that e is a function with domain X which maps into the class of all subsets of $X \cup A$. X will be called the set of *indeterminates* of $\mathcal{E}$, and A is called the set of *atoms* of $\mathcal{E}$. Let $e_v = e(v)$. For each $v \in X$, the set $b_v := e_v \cap X$ is called the set of indeterminates on which v immediately depends. Similarly, the set $c_v := e_v \cap A$ is called the set of atoms on which v immediately depends.

A *solution* to $\mathcal{E}$ is a function s with domain X satisfying

$$s_x = \{s_y : y \in b_x\} \cup c_x,$$

for each $x \in X$, where $s_x := s(x)$.

Theorem: 19.19 (**CZFA**) *Every generalized flat system $\mathcal{E} = (X, A, e)$ has a unique solution.*

Proof: Define a labelled graph $\mathbb{H}$ by letting X be its set of nodes and its edges be of the form $x \rightsquigarrow y$, where $y \in b_x$ for $x, y \in X$. Moreover, let $\ell(x) = c_x$ be the pertinent labelling function. By Theorem 19.6, $\mathbb{H}$ has a unique labelled decoration d. Then

$$d(x) = \{d(y) : y \in b_x\} \cup \ell(x) = \{d(y) : y \in b_x\} \cup c_x,$$

and thus d is a solution to $\mathcal{E}$. One easily verifies that every solution s to $\mathcal{E}$ gives rise to a decoration of $\mathbb{H}$. Thus there exists exactly one solution to $\mathcal{E}$. $\square$

Because of the flatness condition, i.e. $e : X \to \mathcal{P}(X \cup A)$, the above form of the Solution Lemma is often awkward to use. A much more general form of it is proved in [8]. The framework in [8], however, includes other objects than sets, namely a proper class of urelements, whose raison d'etre is to serve as an endless supply of indeterminates on which one can perform the operation of substitution. Given a set X of urelements one defines the class of X-sets which are those sets that use only urelements from X in their build up. For a function $f : X \to V$ on these indeterminates one can then define a substitution operation sub_f on the X-sets. For an X-set a, $sub_f(a)$ is obtained from a by substituting $f(x)$ for x everywhere in the build up of a.

For want of urelements, the approach of [8] is not directly applicable in our set theories, though it is possible to model an extended universe of sets with a proper class of urelements within **CZFA**. This will require a class defined as the greatest fixed point of an operator, a topic we shall intersperse now.

19.5 Greatest fixed points of operators

The theory of greatest operators was initiated by Aczel in [4].

Definition: 19.20 Let Φ be a class operator, i.e. $\Phi(X)$ is a class for each class X. Φ is *set continuous* if for each class X

$$\Phi(X) \;=\; \bigcup\{\Phi(x) : \; x \textit{ is a set with } x \subseteq X\}. \tag{34}$$

Note that a set continuous operator is monotone, i.e., if $X \subseteq Y$ then $\Phi(X) \subseteq \Phi(Y)$.

In what follows, I shall convey that x is a set by $x{\in}V$. If Φ is a set continuous operator let

$$J_\Phi \;=\; \bigcup\{x{\in}V : \; x \subseteq \Phi(x)\}.$$

A set continuous operator Φ is Δ_0 if the relation "$y \in \Phi(x)$" between sets x and y is Δ_0 definable. Notice that J_Φ is a Σ_1 class if Φ is a Δ_0 operator.

Theorem: 19.21 ($\mathbf{CZF}^- + \mathbf{RDC}$) (Cf. [4], Theorem 6.5) *If Φ is a set continuous operator and $J = J_\Phi$ then*

1. $J \subseteq \Phi(J)$,
2. *If $X \subseteq \Phi(X)$ then $X \subseteq J$,*
3. *J is the largest fixed point of Φ.*

Proof: (1): Let $a{\in}J$. Then $a{\in}x$ for for some set x such that $x \subseteq \Phi(x)$. It follows that $a \in \Phi(J)$ as $x \subseteq J$ and Φ is monotone.

(2): Let $X \subseteq \Phi(X)$ and let $a{\in}X$. We like to show that $a{\in}J$. We first show that for each set $x \subseteq X$ there is a set $c_x \subseteq X$ such that $x \subseteq \Phi(c_x)$. So let $x \subseteq X$. Then $x \subseteq \Phi(X)$ yielding

$$\forall y{\in}x\; \exists u\; [y{\in}\Phi(u) \;\wedge\; u \subseteq X].$$

By Strong Collection there is a set A such that

$$\forall y{\in}x\; \exists u{\in}A\; [y{\in}\Phi(u) \;\wedge\; u \subseteq X] \;\wedge\; \forall u{\in}A\; \exists y{\in}x\; [y{\in}\Phi(u) \;\wedge\; u \subseteq X].$$

Letting $c_x = \bigcup A$, we get $c_x \subseteq X \;\wedge\; x \subseteq \Phi(c_x)$ as required.

Next we use **RDC** to find an infinite sequence $x_0, x_1, \ldots$ of subsets of X such that $x_0 = \{a\}$ and $x_n \subseteq \Phi(x_{n+1})$. Let $x^* = \bigcup_n x_n$. Then x^* is a set and if $y{\in}x^*$ then $y{\in}x_n$ for some n so that $y \in x_n \subseteq \Phi(x_{n+1}) \subseteq \Phi(x^*)$. Hence $x^* \subseteq \Phi(x^*)$. As $a{\in}x_0 \subseteq x^*$ it follows that $a{\in}J$.

(3): By (1) and the monotonicity of Φ

$$\Phi(J) \subseteq \Phi(\Phi(J)).$$

Hence by (2) $\Phi(J) \subseteq J$. This and (1) imply that J is a fixed point of Φ. By (2) it must be the greatest fixed point of Φ. $\square$

If it exists and is a set, the largest fixed point of an operator Φ will be called the set *coinductively defined* by Φ.

Theorem: 19.22 ($\mathbf{CZF}^- + \Delta_0$-**RDC**) *If Φ is a set continuous Δ_0 operator and $J = J_\Phi$ then*

1. *$J \subseteq \Phi(J)$,*
2. *If X is a Σ_1 class and $X \subseteq \Phi(X)$ then $X \subseteq J$,*
3. *J is the largest Σ_1 fixed point of Φ.*

Proof: This is the same proof as for Theorem 19.21, noticing that Δ_0-**RDC** suffices here. $\square$

In applications, set continuous operators Φ often satisfy an additional property. Φ will be called *fathomable* if there is a partial class function q such that whenever $a \in \Phi(x)$ for some set x then $q(a) \subseteq x$ and $a \in \Phi(q(a))$. For example, deterministic inductive definitions are given by fathomable operators.

If the graph of q is also Δ_0 definable we will say that Φ is a fathomable set continuous Δ_0 operator.

For fathomable operators one can dispense with **RDC** and Δ_0-**RDC** in Theorems 19.21 and 19.22 in favour of $\mathbf{IND}_\omega$ and Σ-$\mathbf{IND}_\omega$, respectively.

Corollary: 19.23 ($\mathbf{ECST} + \mathbf{IND}_\omega$) *If Φ is a set continuous fathomable operator and $J = J_\Phi$ then*

1. *$J \subseteq \Phi(J)$,*
2. *If $X \subseteq \Phi(X)$ then $X \subseteq J$,*
3. *J is the largest fixed point of Φ.*

Proof: In the proof of Theorem 19.21, **RDC** was used for (2) to show that for every class X with $X \subseteq \Phi(X)$ it holds $X \subseteq J$. Now, if $a \in X$, then $a \in \Phi(u)$ for some set $u \subseteq X$, as Φ is set continuous, and thus $a \in \Phi(q(a))$ and $q(a) \subseteq X$. Using $\mathbf{IND}_\omega$ and Replacement one defines a sequence $x_0, x_1, \ldots$ by $x_0 = \{a\}$ and $x_{n+1} = \bigcup\{q(v) : v {\in} x_n\}$. We use induction on ω to show $x_n \subseteq X$. Obviously $x_0 \subseteq X$. Suppose $x_n \subseteq X$. Then $x_n \subseteq \Phi(X)$. Thus for every $v{\in}x_n$, $q(v) \subseteq X$, and hence $x_{n+1} \subseteq X$. Let $x^* = \bigcup_n x_n$. Then $x^* \subseteq X$. Suppose $u \in x^*$. Then $u \in x_n$ for some n, and hence as $u \in \Phi(X)$, $u \in \Phi(q(u))$. Thus $q(u) \subseteq x_{n+1} \subseteq x^*$, and so $u \in \Phi(x^*)$. As a result, $a \in x^* \subseteq \Phi(x^*)$, and hence $a \in J$. $\square$

Corollary: 19.24 (**ECST** + Σ_1-**IND**$_\omega$) *If Φ is a set continuous fathomable Δ_0 operator and $J = J_\Phi$ then*

1. *$J \subseteq \Phi(J)$,*
2. *If X is Σ_1 and $X \subseteq \Phi(X)$ then $X \subseteq J$,*
3. *J is the largest Σ_1 fixed point of Φ.*

Proof: If the graph of q is Δ_0 definable, Σ_1-**IND**$_\omega$ is sufficient to define the sequence $x_0, x_1, \ldots$. $\square$

For special operators it is also possible to forgo Σ_1-**IND**$_\omega$ in favour of TRANS.

Corollary: 19.25 (**CZF**$^-$ + **EXP** + TRANS) *Let Φ be a set continuous fathomable Δ_0 operator such that q is a total map and $q(a) \subseteq$ **TC**$(\{a\})$ for all sets a. Let $J = J_\Phi$. Then*

1. *$J \subseteq \Phi(J)$,*
2. *If X is Δ_0 and $X \subseteq \Phi(X)$ then $X \subseteq J$,*
3. *J is the largest Δ_0 fixed point of Φ.*

Proof: (1) is proved as in Theorem 19.21. For (2), suppose that X is a class with $X \subseteq \Phi(X)$. Let $a \in X$. Define a sequence of sets $x_0, x_1, \ldots$ by $x_0 = \{a\}$ and $x_{n+1} = \bigcup\{q(v) : v{\in}x_n\}$ as in Corollary 19.23. But without Σ-**IND**$_\omega$, how can we ensure that the function $n \mapsto x_n$ exists? This can be seen as follows. Define

$$\begin{array}{rcl} D_n & = & \{f \in {}^{n+1}\mathbf{TC}(\{a\}) : f(0) = a \wedge \forall i \in n\,[f(i+1) \in q(f(i))]\}, \\ E_n & = & \{f(n) : f \in D_n\}. \end{array}$$

The function $n \mapsto E_n$ exists by **FPA** and Replacement. Moreover, $E_0 = \{a\}$ and $E_{n+1} = \bigcup\{q(v) : v \in E_n\}$ as can be easily shown by induction on n; thus $x_n = E_n$. The remainder of the proof is as in Corollary 19.23.

For (3), note that $J = \{a : a \in \Phi(q(a))\}$ and thus J is Δ_0. $\square$

19.6 Generalized systems of equations in an expanded universe

Before we can state the notion of a general systems of equations we will have to emulate urelements and the sets built out of them in the set theory **CZFA** with pure sets. To this end we employ the machinery of greatest fixed points of the previous subsection. We will take the sets of the form $\langle 1, x\rangle$ to be the urelements and call them $*$-*urelements*. The class of $*$-urelements will be denoted by $\mathcal{U}$. Certain sets built from them will be called the $*$-*sets*. If $a = \langle 2, u\rangle$ let $a^* = u$. The elements of a^* will be called the $*$-elements of a. Let the $*$-sets be the largest class of sets of the form $a = \langle 2, u\rangle$ such that each $*$-element of a is either a $*$-urelement or else a $*$-set. To bring this under the heading of the previous subsection, define

$$\Phi^*(X) \;=\; \{\langle 2, u\rangle : \forall x{\in}u\,[(x{\in}X \;\wedge\; x \in \mathrm{TWO}) \;\vee\; x \text{ is a } *\text{-urelement}]\},$$

where TWO is the class of all ordered pairs of the form $\langle 2, v\rangle$. Obviously, Φ^* is a set-continuous operator. That Φ^* is fathomable can be seen by letting

$$q(a) \;=\; \{v \in a^* : v \in \mathrm{TWO}\}.$$

Notice also that Φ^* has a Δ_0 definition.

The $*$-sets are precisely the elements of J_{Φ^*}. Given a class Z of $*$-urelements we will also define the class of Z-*sets* to be the largest class of $*$-sets such that every $*$-urelement in a Z-set is in Z. We will use the notation $V[Z]$ for the class of Z-sets.

Definition: 19.26 A *general system of equations* is a pair $\mathcal{E} = (X, e)$ consisting of a set $X \subseteq \mathcal{U}$ (of indeterminates) and a function

$$e : X \to V[X].$$

The point of requiring e to take values in $V[X]$ is that thereby e is barred from taking $*$-urelements as values and that all the values of e are sets which use only $*$-urelements from X in their build up. In consequence, one can define a substitution operation on the values of e.

Theorem: 19.27 (**CZFA**) (Substitution Lemma) *Let Y be a Δ_0 class such that $Y \subseteq \mathcal{U}$. For each map $\rho : Y \to V$ there exists a unique operation sub_ρ that assigns to each $a \in V[Y]$ a set $sub_\rho(a)$ such that*

$$sub_\rho(a) \;=\; \{sub_\rho(x) : x \in a^* \cap V[Y]\} \;\cup\; \{\rho(x) : x \in a^* \cap Y\}. \quad (35)$$

Proof: The class $V[Y]$ forms the nodes of a labelled Δ_0 system $\mathbb{M}$ with edges $a \multimap b$ for $a, b \in V[Y]$ whenever $b \in a^*$, and labelling map $\wp(a) = a^* \cap Y$. By Corollary 19.17 there exists a unique map $\hat{\rho} : V[Y] \to V$ such that for each $a \in V[Y]$,

$$\hat{\rho}(a) \;=\; \{\hat{\rho}(x) : x \in a^* \cap V[Y]\} \;\cup\; \{\rho(x) : x \in a^* \cap Y\}. \tag{36}$$

Put $sub_\rho(a) := \hat{\rho}(a)$. Then sub_ρ satisfies (35). Since the equation (36) uniquely determines $\hat{\rho}$ it follows that sub_ρ is uniquely determined as well. □

Definition: 19.28 Let $\mathcal{E}$ be a general system of equations as in Definition 19.26. A *solution* to $\mathcal{E}$ is a function $s : X \to V$ satisfying, for all $x \in X$,

$$s(x) \;=\; sub_s(e_x), \tag{37}$$

where $e_x := e(x)$.

Theorem: 19.29 (**CZFA**) (Solution Lemma) *Let $\mathcal{E}$ be a general system of equations as in Definition 19.26. Then $\mathcal{E}$ has a unique solution.*

Proof: The class $V[X]$ provides the nodes for a labelled Δ_0 system $\mathbb{M}$ with edges $b \multimap c$ for $b, c \in V[X]$ whenever $c \in b^*$, and with a labelling map $\wp(b) = b^* \cap X$. Since $e : X \to V[X]$, we may employ Corollary 19.17 (with $Y = X$). Thus there is a unique function π and a unique function $\hat{\pi}$ such that

$$\pi(x) \;=\; \hat{\pi}(e_x) \tag{38}$$

for all $x \in X$, and

$$\hat{\pi}(a) \;=\; \{\hat{\pi}(b) :: b \in a^*\} \;\cup\; \{\pi(x) : x \in a^* \cap X\}. \tag{39}$$

In view of Theorem 19.27, we get $\hat{\pi} = sub_\pi$ from (39). Thus letting $s := \pi$, (38) then yields the desired equation $s(x) = sub_s(e_x)$ for all $x \in X$. Further, s is unique owing to the uniqueness of π in (38). □

Remark: 19.30 The framework in which **AFA** is studied in [8] is a set theory with a proper class of urelements $\mathcal{U}$ that also features an *axiom of plenitude* which is the conjunction of the following sentences:

$$\forall a \forall b\, \mathsf{new}(a,b) \in \mathcal{U},$$
$$\forall a \forall a' \forall b \forall b'\, [\mathsf{new}(a,b) = \mathsf{new}(a',b') \to a = a' \,\wedge\, b = b'],$$
$$\forall a \forall b\, [b \subseteq \mathcal{U} \to \mathsf{new}(a,b) \notin b],$$

where new is a binary function symbol. It is natural to ask whether a version of **CZFA** with urelements and an axiom of plenitude would yield any extra strength. That such a theory is not stronger than **CZFA** can be easily seen by modelling the urelements and sets of [8] inside **CZFA** by the $*$-urelements and the $*$-sets, respectively. To interpret the function symbol new define

$$\mathsf{new}^*(a,b) := \langle 1, \langle a, \langle b, b^r \rangle\rangle\rangle,$$

where $b^r = \{r \in \mathbf{TC}(b) : r \notin r\}$. Obviously, $\mathsf{new}^*(a,b)$ is a $*$-urelement and new^* is injective. Moreover, $\mathsf{new}^*(a,b) \in b$ would imply $\mathsf{new}^*(a,b) \in \mathbf{TC}(b)$ and thus $b^r \in \mathbf{TC}(b)$. The latter yields the contradiction $b^r \notin b^r \wedge b^r \in b^r$. As a result, $\mathsf{new}^*(a,b) \notin b$. Interpreting new by new^* thus validates the axiom of plenitude, too.

19.7 Streams, coinduction, and corecursion

In the following we shall demonstrate the important methods of coinduction and corecursion in a setting which is not too complicated but still demonstrates the general case in a nutshell. The presentation closely follows [8].

Let A be some set. By a *stream* over A we mean an ordered pair $s = \langle a, s' \rangle$ where $a \in A$ and s' is another stream. We think of a stream as being an element of A followed by another stream. Two important operations performed on streams s are taking the first element $1^{st}(s)$ which gives an element of A, and taking its second element $2^{nd}(s)$, which yields another stream. If we let A^∞ be the streams over A, then we would like to have

$$A^\infty \;=\; A \times A^\infty. \tag{40}$$

In set theory with the foundation axiom, equation (40) has only the solution $A = \emptyset$. With **AFA**, however, not only can one show that (40) has a solution different from $\emptyset$ but also that it has a largest solution, the latter being the largest fixed point of the operator $\Gamma_A(Z) = A \times Z$. This largest solution to Γ_A will be taken to be the set of streams over A and be denoted by A^∞, thus rendering A^∞ a *coinductive* set. Moreover, it will be shown that A^∞ possesses a "recursive" character despite the fact that there is no "base case". For instance, it will turn out that one can define a function

$$zip : A^\infty \times A^\infty \;\to\; A^\infty$$

such that for all $s, t \in A^\infty$

$$zip(s,t) \;=\; \langle 1st(s), \langle 1^{st}(t), zip(2^{nd}(s), 2^{nd}(t))\rangle\rangle. \tag{41}$$

As its name suggests, *zip* acts like a zipper on two streams. The definition of *zip* in (41) is an example for definition by *corecursion* over a coinductive set.

Theorem: 19.31 (**CZFA**) *For every set A there is a largest set Z such that $Z \subseteq A \times Z$. Moreover, Z satisfies $Z = A \times Z$, and if A is inhabited then so is Z.*

Proof: Let F be the set of functions from $\mathbb{N} := \omega$ to A. For each such f, we define another function $f^+ : \mathbb{N} \to \mathbb{N}$ by

$$f^+(n) \;=\; f(n+1).$$

For each $f \in F$ let x_f be an indeterminate. We would like to solve the system of equations given by

$$x_f \;=\; \langle f(0), x_{f^+} \rangle.$$

Solving these equations is equivalent to solving the equations

$$\begin{aligned} x_f &= \{y_f, z_f\}; \\ y_f &= \{f(0)\} \\ z_f &= \{f(0), x_{f^+}\}, \end{aligned} \tag{42}$$

where y_f and z_f are further indeterminates. Note that $f(0)$ is an element of A. To be precise, let $x_f = \langle 0, f \rangle$, $y_f = \langle 1, f \rangle$, and $z_f = \langle 2, f \rangle$. Solving (42) amounts to the same as finding a labelled decoration for the labelled graph

$$\mathbb{S}_A = (S, \rightsquigarrow, \ell)$$

whose set of nodes is

$$S = \{x_f \,:\, f \in F\} \cup \{y_f \,:\, f \in F\} \cup \{z_f \,:\, f \in F\}$$

and whose edges are given by $x_f \rightsquigarrow y_f$, $x_f \rightsquigarrow z_f$, $z_f \rightsquigarrow x_{f^+}$. Moreover, the labelling function ℓ is defined by $\ell(x_f) = \emptyset$, $\ell(y_f) = \{f(0)\}$, $\ell(z_f) = \{f(0)\}$ for all $f \in F$. By the labelled Anti-Foundation Axiom, Theorem 19.6, $\mathbb{S}_A$ has a labelled decoration d and we thus get

$$d(x_f) \;=\; \langle f(0), d(x_{f^+}) \rangle. \tag{43}$$

Let $A^\infty = \{d(x_f) \,:\, f \in F\}$. By (43), we have $A^\infty \subseteq A \times A^\infty$. Thus A^∞ solves the equation $Z \subseteq A \times Z$.

To check that $A \times A^\infty \subseteq A^\infty$ holds also, let $a \in A$ and $t \in A^\infty$. By the definition of A^∞, $t = d(x_f)$ for some $f \in F$. Let $g : \mathbb{N} \to A$ be defined by

$g(0) = a$ and $g(n+1) = f(n)$. Then $g^+ = f$, and thus $d(x_g) = \langle a, d(x_f)\rangle = \langle a, t\rangle$, so $\langle a, t\rangle \in A^\infty$.

If A contains an element a, then $f_a \in F$, where $f_a : \mathbb{N} \to A$ is defined by $f_a(n) = a$. Hence $d(x_{f_a}) \in A^\infty$, so A^∞ is inhabited, too.

Finally it remains to show that A^∞ is the largest set Z satisfying $Z \subseteq A \times Z$. So suppose that W is a set so that $W \subseteq A \times W$. Let $v \in W$. Define $f_v : \mathbb{N} \to A$ by

$$f_v(n) \;=\; 1^{st}(sec^n(v)),$$

where $sec^0(v) = v$ and $sec^{n+1}(v) = 2^{nd}(sec^n(v))$. Then $f_v \in F$, and so $d(x_{f_v}) \in A^\infty$. We claim that for all $v \in W$, $d(x_{f_v}) = v$. Notice first that for $w = 2^{nd}(v)$, we have $sec^n(w) = sec^{n+1}(v)$ for all $n \in \mathbb{N}$, and thus $f_w = (f_v)^+$. It follows that

$$\begin{aligned} d(x_{f_v}) &= \langle 1^{st}(v), d(x_{(f_v)^+})\rangle \\ &= \langle 1^{st}(v), d(x_{f_w})\rangle \\ &= \langle 1^{st}(v), d(x_{f_{2^{nd}(v)}})\rangle. \end{aligned} \tag{44}$$

W gives rise to a labelled subgraph $\mathbb{T}$ of $\mathbb{S}$ whose set of nodes is

$$T := \{x_{f_v} : v \in W\} \cup \{y_{f_v} : v \in W\} \cup \{z_{f_v} : v \in W\},$$

and wherein the edges and the labelling function are obtained from $\mathbb{S}$ by restriction to nodes from T. The function d' with $d'(x_{f_v}) = v$, $d'(y_{f_v}) = \{1^{st}(v)\}$, and $d'(z_{f_v}) = \{1^{st}(v), 2^{nd}(v)\}$ is obviously a labelled decoration of $\mathbb{T}$. By (44), d restricted to T is a labelled decoration of $\mathbb{T}$ as well. So by Theorem 19.6, $v = d'(x_{f_v}) = d(x_{f_v})$ for all $v \in W$, and thus $W \subseteq A^\infty$. □

As a corollary one gets the following *coinduction principle* for A^∞.

Remark: 19.32 Rather than applying the labelled Anti-Foundation Axiom one can utilize the solution lemma for general systems of equations (Theorem 19.29) in the above proof of Theorem 19.31. To this end let $B = \mathbf{TC}(A)$, $x_f = \langle 1, \langle 0, f\rangle\rangle$ for $f \in F$ and $x_b = \langle 1, \langle 1, b\rangle\rangle$ for $b \in B$. Set $X := \{x_f : f \in F\} \cup \{x_b : b \in B\}$. Then $X \subseteq \mathcal{U}$ and $\{x_f : f \in F\} \cap \{x_b : b \in B\} = \emptyset$.

Next define the unordered $*$-pair by $\{c, d\}^* = \langle 2, \{c, d\}\rangle$ and the ordered $*$-pair by $\langle c, d\rangle^* = \{\{c\}^*, \{c, d\}^*\}^*$. Note that with $c, d \in V[X]$ one also has $\{c, d\}^*, \langle c, d\rangle^* \in V[X]$.

Let $\mathcal{E} = (X, e)$ be the general system of equations with $e(x_f) = \langle x_{f(0)}, x_{f^+}\rangle^*$ for $f \in F$ and $e(x_b) = \langle 2, \{x_u \;\; u \in b\}\rangle$ for $b \in B$. Then $e : X \to V[X]$. By Theorem 19.29 there is a unique function $s : X \to V$ such that

$$s(x_b) \;=\; sub_s(e(x_b)) \;=\; \{s(x_u) : u \in b\} \quad \text{for } b \in B, \tag{45}$$

$$s(x_f) \;=\; sub_s(e(x_f)) \;=\; \langle s(x_{f(0)}), s(x_{f^+})\rangle \quad \text{for } f \in F. \tag{46}$$

From (45) and Lemma 19.10 it follows $s(x_b) = b$ for all $b \in B$, and thus from (46) it ensues that $s(x_f) = \langle f(0), s(x_{f+}) \rangle$ for $f \in F$. From here on one can proceed further just as in the proof of Theorem 19.29.

Corollary: 19.33 (**CZFA**) *If a set Z satisfies $Z \subseteq A \times Z$, then $Z \subseteq A^\infty$.*

Proof: This follows from the fact that A^∞ is the largest such set. $\square$

The pivotal property of inductively defined sets is that one can define functions on them by structural recursion. For coinductively defined sets one has a dual principle, *corecursion*, which allows one to define functions mapping into the coinductive set.

Theorem: 19.34 (**CZFA**) (Corecursion Principle for Streams). *Let C be an arbitrary set. Given functions $g : C \to A$ and $h : C \to C$ there is a unique function $f : C \to A^\infty$ satisfying*

$$f(c) \;=\; \langle g(c), f(h(c)) \rangle \tag{47}$$

for all $c \in C$.

Proof: For each $c \in C$ let x_c, y_c, z_c be different indeterminates. To be precise, let $x_c = \langle 0, c \rangle$, $y_c = \langle 1, c \rangle$, and $z_c = \langle 2, c \rangle$ for $c \in C$. This time we would like to solve the system of equations given by

$$x_c \;=\; \langle g(c), x_{h(c)} \rangle.$$

Solving these equations is equivalent to solving the equations

$$\begin{aligned} x_c &= \{y_c, z_c\}; \\ y_c &= \{g(c)\} \\ z_c &= \{g(c), x_{h(c)}\}. \end{aligned} \tag{48}$$

Solving (48) amounts to the same as finding a labelled decoration for the labelled graph

$$\mathbb{S}_C = (S_C, \rightsquigarrow, \ell_C)$$

whose set of nodes is

$$S_C = \{x_c : c \in C\} \cup \{y_c : c \in C\} \cup \{z_c : c \in C\}$$

and whose edges are given by $x_c \rightsquigarrow y_c$, $x_c \rightsquigarrow z_c$, $z_c \rightsquigarrow x_{h(c)}$. Moreover, the labelling function ℓ_C is defined by $\ell_C(x_b) = \emptyset$, $\ell_C(y_b) = \{g(b)\}$, $\ell_C(z_b) =$

$\{g(b)\}$ for all $b \in C$. By the labelled Anti-Foundation Axiom, Theorem 19.6, $\mathbb{S}_C$ has a labelled decoration $\jmath$ and we thus get

$$\jmath(x_c) \;=\; \langle g(c), \jmath(x_{h(c)})\rangle. \tag{49}$$

Letting the function f with domain C be defined by $f(c) := \jmath(x_c)$, we get from (49) that

$$f(c) \;=\; \langle g(c), f(h(c))\rangle \tag{50}$$

holds for all $c \in C$. As $\mathbf{ran}(f) \subseteq A \times \mathbf{ran}(f)$, Corollary 19.33 yields $\mathbf{ran}(f) \subseteq A^{\infty}$, thus $f : C \to A^{\infty}$.

It remains to show that f is uniquely determined by (50). So suppose $f' : C \to A^{\infty}$ is another function satisfying $f'(c) = \langle g(c), f'(h(c))\rangle$ for all $c \in C$. Then the function $\jmath'$ with $\jmath'(x_c) = f'(c)$, $\jmath'(y_c) = \{g(c)\}$, and $\jmath'(z_c) = \{g(c), f'(h(c))\}$ would give another labelled decoration of $\mathbb{S}_C$, hence $f(c) = \jmath(x_c) = \jmath'(x_c) = f'(x_c)$, yielding $f = f'$. □

Example 1. Let $k : A \to A$ be arbitrary. Then k gives rise to a unique function $map_k : A^{\infty} \to A^{\infty}$ satisfying

$$map_k(s) \;=\; \langle k(1^{st}(s)), map_k(2^{nd}(s))\rangle. \tag{51}$$

For example, if $A = \mathbb{N}$, $k(n) = 2n$, and $s = \langle 3, \langle 6, \langle 9, \ldots\rangle\rangle\rangle$, then $map_k(s) = \langle 6, \langle 12, \langle 18, \ldots\rangle\rangle\rangle$. To see that map_k exists, let $C = A^{\infty}$ in Theorem 19.34, $g : A^{\infty} \to A$ be defined by $g(s) = k(1^{st}(s))$, and $h : A^{\infty} \to A^{\infty}$ be the function $h(s) = 2^{nd}(s)$. Then map_k is the unique function f provided by Theorem 19.34.

Example 2. Let $\nu : A \to A$. We want to define a function

$$iter_{\nu} \,:\, A \to A^{\infty}$$

which "iterates" ν such that $iter_{\nu}(a) = \langle a, iter_{\nu}(\nu(a))\rangle$ for all $a \in A$. If, for example $A = \mathbb{N}$ and $\nu(n) = 2n$, then $iter_{\nu}(7) = \langle 7, \langle 14, \langle 28, \ldots\rangle\rangle\rangle$. To arrive at $iter_{\nu}$ we employ Theorem 19.34 with $C = A^{\infty}$, $g : C \to A$, and $h : C \to C$, where $g(s) = \nu(1^{st}(s))$ and $h = map_{\nu}$, respectively.

Outlook. It would be desirable to develop the theory of corecursion of [8] (in particular Theorem 17.5) and the final coalgebra theorem of [4] in full generality within **CZFA** and extensions. It appears that the first challenge here is to formalize parts of category theory in constructive set theory.

19.8 Predicativism

Hermann Weyl rejected the platonist philosophy of mathematics as manifested in impredicative existence principles of Zermelo-Fraenkel set theory. In his book *Das Kontinuum*, he initiated a predicative approach to the the real numbers and gave a viable account of a substantial chunk of analysis. What are the ideas and principles upon which his "predicative view" is supposed to be based? A central tenet is that there is a fundamental difference between our understanding of the concept of natural numbers and our understanding of the set concept. As the French predicativists, Weyl accepts the completed infinite system of natural numbers as a point of departure. He also accepts classical logic but just works with sets that are of level one in Russell's ramified hierarchy, in other words only with the principle of arithmetical definitions.

Logicians such as Wang, Lorenzen, Schütte, and Feferman then proposed a foundation of mathematics using layered formalisms based on the idea of predicativity which ventured into higher levels of the ramified hierarchy. The idea of an autonomous progression of theories $RA_0, RA_1, \ldots, RA_\alpha, \ldots$ was first presented in Kreisel [43] and than taken up by Schütte and Feferman to determine the limits of predicativity. The notion of autonomy therein is based on introspection and should perhaps be viewed as a 'boot-strap' condition. One takes the structure of natural numbers as one's point of departure and then explores through a process of active reflection what is implicit in accepting this structure, thereby developing a growing body of ever higher layers of the ramified hierarchy. Schütte and Feferman (cf. [70, 71, 23, 24]) showed that the ordinal Γ_0 is the first ordinal whose well-foundedness cannot be proved in autonomous progressions of theories. It was also argued by Feferman that the whole sequence of autonomous progressions of theories is coextensive with predicativity and on these grounds Γ_0 is often referred to as the proper limit of all predicatively provable ordinals. In this paper I shall only employ the "lower bound" part of this analysis, i.e., that every ordinal less than Γ_0 is a predicatively provable ordinal. In consequence, every theory with proof-theoretic ordinal less than Γ_0 has a predicative consistency proof and is moreover conservative over a theory RA_α for arithmetical statements for some $\alpha < \Gamma_0$. As a shorthand for the above I shall say that a theory is *predicatively justifiable.*

As a scale for measuring the proof-theoretic strength of theories one uses traditionally certain subsystems of second order arithmetic (see [26, 73]). Relevant to the present context are systems based on the Σ^1_1 axiom of choice and the Σ^1_1 axiom of dependent choices. The theory $\mathbf{\Sigma^1_1}$-$\mathbf{AC}$ is a subsystem of second order arithmetic with the Σ^1_1 axiom of choice and induction over the natural numbers for all formulas while $\mathbf{\Sigma^1_1}$-$\mathbf{DC}_0$ is a subsystem of second order arithmetic with the Σ^1_1 axiom of dependent choices and induction over the natural numbers restricted to formulas without second order quantifiers (for precise definitions see [26, 73]). The proof theoretic ordinal of $\mathbf{\Sigma^1_1}$-$\mathbf{AC}$ is $\varphi\varepsilon_0 0$ while $\mathbf{\Sigma^1_1}$-$\mathbf{DC}_0$ has the smaller proof-theoretic ordinal $\varphi\omega 0$ as was shown by Cantini [15]. Here φ denotes the Veblen function (see [72]).

Theorem: 19.35 *(i) The theories* $\mathbf{CZF}^-$+Σ_1-$\mathbf{IND}_\omega$, $\mathbf{CZFA}$+$\Sigma_1\mathbf{IND}_\omega$+$\Delta_0$-$\mathbf{RDC}$, $\mathbf{CZFA}$+Σ_1-$\mathbf{IND}_\omega$+$\mathbf{DC}$, *and* $\mathbf{\Sigma^1_1}$-$\mathbf{DC}_0$ *are proof-theoretically equivalent. Their proof-theoretic ordinal is* $\varphi\omega 0$.

(ii) The theories $\mathbf{CZF}^-$+$\mathbf{IND}_\omega$, $\mathbf{CZFA}$+$\mathbf{IND}_\omega$+$\mathbf{RDC}$, $\widehat{\mathbf{ID}}_\mathbf{1}$, *and* $\mathbf{\Sigma^1_1}$-$\mathbf{AC}$ *are proof-theoretically equivalent. Their proof-theoretic ordinal is* $\varphi\varepsilon_0 0$.

(iii) $\mathbf{CZFA}$ *has at least proof-theoretic strength of Peano arithmetic and so its proof-theoretic ordinal is at least* ε_0. *An upper bound for the proof-theoretic ordinal of* $\mathbf{CZFA}$ *is* $\varphi 20$. *In consequence,* $\mathbf{CZFA}$ *is proof-theoretically weaker than* $\mathbf{CZFA} + \Delta_0$-$\mathbf{RDC}$.

Proof: (ii) follows from [59], Theorem 3.15.

As to (i) it is important to notice that the scheme dubbed Δ_0-$\mathbf{RDC}$ in [59] is not the same as Δ_0-$\mathbf{RDC}$ in the present paper. In [59], Δ_0-$\mathbf{RDC}$ asserts for Δ_0 formulas ϕ and ψ that whenever $(\forall x{\in}a)[\phi(x) \rightarrow (\exists y{\in}a)(\phi(y) \wedge \psi(x,y))]$ and $b_0{\in}a \wedge \phi(b_0)$, then there exists a function $f : \omega \rightarrow a$ such that $f(0) = b_0$ and $(\forall n{\in}\omega)[\phi(f(n)) \wedge \psi(f(n), f(n{+}1))]$. The latter principle is weaker than our Δ_0-$\mathbf{RDC}$ as all quantifiers have to be restricted to a given set a. However, the realizability interpretation of constructive set theory in $\mathbf{PA}^r_\Omega + \Sigma^\Omega$-$\mathbf{IND}$ employed in the proof of [59], Theorem 3.15 (i) also validates the stronger Δ_0-$\mathbf{RDC}$ of the present paper (the system $\mathbf{PA}^r_\Omega$ stems from [37]).

Theorem 3.15 (i) of [59] and Lemma 10.6 also imply that $\mathbf{CZF}^-$+Δ_0-$\mathbf{RDC}$ is not weaker than $\mathbf{CZF}^- + \Sigma_1$-$\mathbf{IND}_\omega$. Thus proof-theoretic equivalence of all systems in (i) ensues.

(iii) is a consequence of the fact that Heyting Arithmetic can be easily interpreted in $\mathbf{CZF}^-$ and hence in $\mathbf{CZFA}$. At present the exact proof-theoretic strength of $\mathbf{CZFA}$ is not known, however, it can be shown that the proof-theoretic ordinal of $\mathbf{CZFA}$ is not bigger than $\varphi 20$. The latter bound can be obtained by inspecting the interpretation of $\mathbf{CZFA}$ in $\mathbf{PA}^r_\Omega + \Sigma^\Omega$-$\mathbf{IND}$ employed in the proof of [59], Theorem 3.15. A careful inspection reveals that a subtheory T of $\mathbf{PA}^r_\Omega + \Sigma^\Omega$-$\mathbf{IND}$ suffices. To be more precise, T can be taken to be the theory

$$\mathbf{PA}^r_\Omega + \forall\alpha\,\exists\lambda\,[\alpha < \lambda \;\wedge\; \lambda \text{ is a limit ordinal}].$$

Using cut elimination techniques and asymmetric interpretation, T can be partially interpreted in $\mathbf{RA}_{<\omega^2}$. The latter theory is known to have proof-theoretic ordinal $\varphi 20$. $\square$

References

[1] P. Aczel: *The type theoretic interpretation of constructive set theory.* In: MacIntyre, A. and Pacholski, L. and Paris, J, editor, *Logic Colloquium '77* (North Holland, Amsterdam 1978) 55–66.

[2] P. Aczel: *The type theoretic interpretation of constructive set theory: Choice principles.* In: A.S. Troelstra and D. van Dalen, editors, *The L.E.J. Brouwer Centenary Symposium* (North Holland, Amsterdam 1982) 1–40.

[3] P. Aczel: *The type theoretic interpretation of constructive set theory: Inductive definitions.* In: R.B. et al. Marcus, editor, *Logic, Methodology and Philosophy of Science VII* (North Holland, Amsterdam 1986) 17–49.

[4] P. Aczel: *Non-well-founded sets.* CSLI Lecture Notes 14 (CSLI Publications, Stanford, 1988).

[5] P. Aczel, M. Rathjen: *Notes on constructive set theory*, Technical Report 40, Institut Mittag-Leffler (The Royal Swedish Academy of Sciences, 2001). *http://www.ml.kva.se/preprints/archive2000-2001.php*

[6] H.P. Barendregt: *The Lambda Calculus: It's Syntax and Semantics* (North Holland, Amsterdam,, 1981).

[7] J. Barwise: *Admissible Sets and Structures* (Springer-Verlag, Berlin, Heidelberg, New York, 1975).

[8] J. Barwise, L. Moss: *Vicious circles.* CSLI Lecture Notes 60 (CSLI Publications, Stanford, 1996).

[9] M. Beeson: *Continuity in intuitionistic set theories*, in: M Boffa, D. van Dalen, K. McAloon (eds.): *Logic Colloquium '78* (North-Holland, Amsterdam, 1979).

[10] M. Beeson: *Foundations of Constructive Mathematics.* (Springer-Verlag, Berlin, Heidelberg, New York, Tokyo, 1985).

[11] E. Bishop and D. Bridges: *Constructive Analysis.* (Springer-Verlag, Berlin, Heidelberg, New York, Tokyo, 1985).

[12] A. Blass: *Injectivity, projectivity, and the axiom of choice.* Transactions of the AMS 255 (1979) 31–59.

[13] É. Borel: *Œuvres de Émil Borel* (Centre National de la recherche Scientifique, Paris, 1972).

[14] L.E.J. Brouwer: *Weten, willen, spreken* (Dutch). Euclides 9 (1933) 177-193.

[15] A. Cantini: *On the relation etween choice and comprehension principles in second order arithmetic.* Journal of Symbolic Logic, vol. 51 (1986) 360-373.

[16] L. Crosilla and M. Rathjen: *Inaccessible set axioms may have little consistency strength* Annals of Pure and Applied Logic 115 (2002) 33–70.

[17] R. Diaconescu: *Axiom of choice and complementation.* Proc. Amer. Math. Soc. 51:176–178, 1975.

[18] T. Dodd and R. Jensen: *The core model.* Annals of Mathematical Logic 20 (1981) 43-75.

[19] M. Dummett: *Elements of intuitionism.* Second edition (Clarendon Press,Oxford,2000)

[20] S. Feferman: *Formal theories for transfinite iterations of generalized inductive definitions and some subsystems of analysis.* In: J. Myhill, A. Kino, R.E. Vesley (eds.): *Intuitionism and Proof Theory.* (North-Holland, Amsterdam, 1970) 303-325.

[21] S. Feferman: *Iterated inductive fixed-point theories: application to Hancock's conjecture*, in: Patras Logic Symposium (Patras, 1980)Studies in Logic and the Foundations of Mathematics, 109 (North–Holland, Amsterdam 1982) 171–196.

[22] S. Feferman, W. Sieg: *Theories of inductive definitions.* In: W. Buchholz, S. Feferman, W. Pohlers, W. Sieg: *Iterated inductive definitions and subsystems of analysis* (Springer, Berlin, 1981) 16-142.

[23] S. Feferman: *Systems of predicative analysis*, Journal of Symbolic Logic 29 (1964) 1–30.

[24] S. Feferman: *Systems of predicative analysis II. Representations of ordinals*, Journal of Symbolic Logic 33 (1968) 193–220.

[25] S. Feferman: *A language and axioms for explicit mathematics.* In: J.N. Crossley (ed.): *Algebra and Logic*, Lecture Notes in Math. 450 (Springer, Berlin 1975) 87–139.

[26] S. Feferman: *Theories of finite type related to mathematical practice.* In: J. Barwise (ed.): *Handbook of Mathematical Logic* (North Holland, Amsterdam, 1977) 913–971.

[27] S. Feferman: *Constructive theories of functions and classes* in: Boffa, M., van Dalen, D., McAloon, K. (eds.), *Logic Colloquium '78* (North-Holland, Amsterdam 1979) 159–224.

[28] S. Feferman and A. Levy: *Independence results in set theory by Cohen's method. II.* (abstract) Notices of the american Mathematical Society 10 (1963) 593.

[29] M. Forti, F. Honsell: *Set theory with free construction principles.* Annali Scuola Normale Supeiore di Pisa, Classe di Scienze 10 (1983) 493-522.

[30] H. Friedman: *Set-theoretic foundations for constructive analysis.* Annals of Mathematics 105 (1977) 868-870.

[31] H. Friedman, S. Ščedrov: *The lack of definable witnesses and provably recursive functions in intuitionistic set theory*, Advances in Mathematics 57 (1985) 1–13.

[32] N. Gambino: *Types and sets: a study on the jump to full impredicativity*, Laurea Dissertation, Department of Pure and Applied Mathematics, University of Padua (1999).

[33] N. Gambino: *Heyting-valued interpretations for constructive set theory*, Department of Computer Science, Manchester University (2002) 42 pages.

[34] M. Gitik: *All uncountable cardinals can be singular.* Israel Journal of Mathematics 35 (1980) 61–88.

[35] P.G. Hinman: *Recursion-theoretic hierarchies* (Springer, Berlin, 1978).

[36] P. Howard, J.E. Rubin: *Consequences of the axiom of choice.* Mathematical Surveys and Mongraphs 59 (American Mathematical Society, providence, 1998).

[37] G. Jäger: *Fixed points in Peano arithmetic with ordinals.* Annals of Pure and Applied Logic 60 (1993) 119–132.

[38] T. Jech: *The axiom of choice.* (North-Holland, Amsterdam, 1973).

[39] T. Jech: *On hereditarily countable sets.* Journal of symbolic Logic (1982) 43–47.

[40] R.B. Jensen: *Independence of the axiom of dependent choices from the countable axiom of choice (abstract).* Journal of symbolic logic 31 (1966) 294.

[41] H. Jervell: *From the axiom of choice to choice sequences*, Nordic Journal of Philosophical Logic 1 (1996) 95-98.

[42] A. Kanamori: *The higher infinite.* (Springer, Berlin, 1995).

[43] G. Kreisel: *Ordinal logics and the characterization of informal concepts of proof.* In: *Proceedings of the 1958 International Congress of Mathematicians*, (Edinburgh,1960) 289–299.

[44] K. Kunen: *Set Theory: An introduction to independence proofs.* (North-Holland, Amsterdam, 1980).

[45] J. Lindström: *A construction of non-well-founded sets within Martin-Löf type theory.* Journal of Symbolic Logic 54 (1989) 57–64.

[46] P. Mahlo: *Über lineare transfinite Mengen*, Berichte über die Verhandlungen der Königlich Sächsischen Gesellschaft der Wissenschaften zu Leipzig, Mathematisch-Physische Klasse, 63 (1911) 187–225.

[47] P. Martin-Löf: *An intuitionistic theory of types: predicative part*, in: H.E. Rose and J. Sheperdson (eds.): *Logic Colloquium '73* (North-Holland, Amsterdam, 1975) 73–118.

[48] P. Martin-Löf: *Intuitionistic Type Theory*, (Bibliopolis, Naples, 1984).

[49] D.C. McCarty: *Realizability and recursive mathematics*, PhD thesis, Oxford University (1984), 281 pages.

[50] I. Moerdijk, E. Palmgren: *Type theories, toposes and constructive set theory: predicative aspects of AST*, Annals of Pure and Applied Logic 114 (2002) 155-201.

[51] L. Moss: *Power set recursion*, Annals of Pure and Applied Logic 71 (1995) 247–306.

[52] J. Myhill: *"Embedding classical type theory in intuitionistic type theory" a correction.* Axiomatic set theory. Proceedings of Symposia in 185– 188, 1974.

[53] J. Myhill: *Constructive set theory.* Journal of Symbolic Logic, 40:347–382, 1975.

[54] W. Pohlers: *Proof theory.* Lecture Notes in Mathematics 1407 (Springer, Berlin, 1989).

[55] W. Pohlers: *A short course in ordinal analysis,* in: P. Aczel, H. Simmons, S. Wainer (eds.): *Proof Theory* (Cambridge University Press, Cambridge, 1992) 27–78.

[56] M. Rathjen: *Fragments of Kripke-Platek set theory with infinity,* in: P. Aczel, H. Simmons, S. Wainer (eds.): *Proof Theory* (Cambridge University Press, Cambridge, 1992) 251–273.

[57] M. Rathjen: *The strength of some Martin-Löf type theories.* Archive for Mathematical Logic 33 (1994) 347–385.

[58] M. Rathjen: *The realm of ordinal analysis.* In: S.B. Cooper and J.K. Truss (eds.): *Sets and Proofs.* (Cambridge University Press, 1999) 219–279.

[59] M. Rathjen: *The anti-foundation axiom in constructive set theories.* In: G. Mints, R. Muskens (eds.): *Games, Logic, and Constructive Sets.* (CSLI Publications, Stanford, 2003).

[60] M. Rathjen: *Kripke-Platek set theory and the anti-foundation axiom.* Mathematical Logic Quarterly 47 (2001) 435–440.

[61] M. Rathjen, E. Palmgren: *Inaccessibility in constructive set theory and type theory.* Annals of Pure and Applied Logic 94 (1998) 181–200.

[62] M. Rathjen, R. Lubarsky: *On the regular extension axioms and its variants.* Mathematical Logic Quarterly 49, No. 5 (2003) 1-8.

[63] M. Rathjen *Realizability for constructive Zermelo-Fraenkel set theory.* In: J. Väänänen, V. Stoltenberg-Hansen (eds.): *Logic Colloquium 2003.* Lecture Notes in Logic 24 (A.K. Peters, 2006) 282–314.

[64] M. Rathjen: *Choice principles in constructive and classical set theories.* In: Z. Chatzidakis, P. Koepke, W. Pohlers (eds.): *Logic Colloquium 02*, Lecture Notes in Logic 27 (A.K. Peters, 2006) 299–326.

[65] M. Rathjen, Sergei Tupailo: *Characterizing the interpretation of set theory in Martin-Löf type theory.* Annals of Pure and Applied Logic 141 (2006) 442–471.

[66] M. Rathjen: *Replacement versus collection in constructive Zermelo-Fraenkel set theory.* Annals of Pure and Applied Logic 136 (2005) Pages 156–174.

[67] M. Rathjen: *Generalized Inductive Definitions in Constructive Set Theory.* In: L. Crosilla, P. Schuster (eds.): *From Sets and Types to Topology and Analysis Towards Practicable Foundations for Constructive Mathematics* (Clarendon Press, Oxford, 2005) 23–40.

[68] M. Rathjen: *The formulae-as-classes interpretation of constructive set theory.* In: H. Schwichtenberg, K. Spies (eds.): *Proof Technology and Computation* (IOS Press, Amsterdam,2006) 279–322.

[69] B. Russell: *Mathematical logic as based on the theory of types.* American Journal of Mathematics 30 (1908) 222–262.

[70] K. Schütte: *Eine Grenze für die Beweisbarkeit der transfiniten Induktion in der verzweigten Typenlogik*, Archiv für Mathematische Logik und Grundlagenforschung 67 (1964) 45–60.

[71] K. Schütte: *Predicative well-orderings*, in: Crossley, Dummett (eds.), Formal systems and recursive functions (North Holland, Amsterdam, 1965) 176–184.

[72] K. Schütte: *Proof theory* (Springer, Berlin, 1977).

[73] S. Simpson: *Subsystems of second order arithmetic* (Springer, Berlin, 1999).

[74] A.S. Troelstra: *A note on non-extensional operations in connection with continuity and recursiveness.* Indagationes. Math. 39 (1977) 455–462.

[75] A.S. Troelstra and D. van Dalen: *Constructivism in Mathematics, Volumes I, II.* (North Holland, Amsterdam, 1988).

[76] H. Weyl: *Die Stufen des Unendlichen.* (Verlag von Gustav Fischer, Jena, 1931).

[77] H. Weyl: *Philosophy of Mathematics and Natural Sciences.* (Princeton University Press, Princeton, 1949)