Automorphisms of Partial Combinatory Algebras and Realizability Models of Constructive Set Theory

Andrew Wakelin Swan

Submitted in accordance with the requirements for the degree of Doctor of Philosophy

The University of Leeds

School of Mathematics

September 2012

The candidate confirms that the work submitted is his own and that appropriate credit has been given where reference has been made to the work of others.

Acknowledgements

I would like to thank my PhD supervisor, Prof Michael Rathjen for introducing me to this area of research and for general support and guidance.

I am grateful to the staff and students in the University of Leeds school of mathematics for helpful suggestions, interesting discussions and not least for making studying at Leeds an enjoyable experience.

I would like to thank my family for supporting and encouraging me with my studies.

This work was supported by an EPSRC Doctoral Training Grant.

Abstract

In this thesis we investigate automorphisms of partial combinatory algebras and construct realizability models of constructive set theory.

After some introductory and background material in chapters 1 and 2, we define in chapter 3 a generalisation of Kripke and realizability models of intuitionistic logic that we call Kripke realizability models. In chapters 4, 6 and 7 we then develop various realizability models of constructive set theory. We show in chapter 5 how to use these techniques to investigate the automorphisms of some partial combinatory algebras. In chapter 8 we use a Kripke realizability model to show that a property known as the existence property does not hold for the set theory **CZF**.

Contents

Chapter 1

Introduction

1.1 Constructive Mathematics

Constructive mathematics can be broadly described as mathematics carried out while avoiding certain principles accepted by mainstream mathematicians. This may be done for a variety of reasons, but the main schools of thought (as listed by Troelstra and van Dalen in the introduction to [37]) are as follows.

Finitism Finitists such as Kronecker believe that only objects that can be represented numerically are mathematically meaningful. They therefore may avoid "higher order" objects such as sets.

Predicativism Predicativists, such as Poincaré believe that definitions are not valid if they refer to objects that have not yet been defined. This means that quantifiers in definitions should range over objects that have already been defined.

Intuitionism Intuitionism was developed by Brouwer, who believed that objects studied by mathematicians are inherently mental constructions. He asserted that mathematical objects are only meaningful if they can be grasped mentally. Intuitionists are known for rejecting excluded middle (every proposition is either true or false). This is because $P \vee \neg P$ can only be known if either P is proved to be true, or a contradiction is derived from assuming P to be true. Another well known intuitionist was Heyting.

Constructive Recursive Mathematics This is also known as Russian constructive mathematics and was developed by Markov. He believed that mathematical objects are only meaningful if they can be represented numerically. This includes functions and even partial functions on the naturals, as long as they are computable.

Bishop Style Constructive Mathematics Bishop was the first constructive mathematician to put little emphasis on the philosophical basis of constructive mathematics and to instead focus on actually carrying out mathematics in a constructive style. He proved constructively a large number of theorems in analysis, and constructive mathematicians have continued this programme and expanded it to other areas of mathematics. Bishop style proofs are usually carried out in such a way that they can be accepted by intuitionists, constructive recursive mathematicians and classical mathematicians.

One of the main principles of constructive mathematics is that the meaning of formulas is given by the Brouwer-Heyting-Kolmogorov, or BHK interpretation. That is,

- to prove $P \vee Q$ is to either prove P or to prove Q
- to prove $P \wedge Q$ is to prove P and prove Q
- to prove $P \to Q$ is to possess a rule which given a proof of P returns a proof of Q
- to prove $\perp$ is impossible
- to prove $(\exists x)P(x)$ is to construct a witness a and possess a proof of $P(a)$
- to prove $(\forall x)P(x)$ is to possess a rule which given an object a returns a proof of $P(a)$

There is some variation in how this is interpreted.

For intuitionists and Bishop-style constructivists, “rule” is a primitive notion, whereas for constructive recursive mathematicians “rule” refers to computable function.

For intuitionists and some constructive recursive mathematicians, the above definition of “proof” is the only meaningful notion of mathematical truth. They deduce that it is natural to identify truth and provability. This results in beliefs contradicting classical mathematics such as Brouwer’s principle that all functions are continuous and the Russian constructivists’ axiom Church’s Thesis, stating that all functions on the naturals are computable.

A more common viewpoint is that there is some notion of truth external to provability. Many constructive mathematicians hold that classical mathematics is “true,” but that constructive proofs provide a better understanding of mathematical results.

In practice this means producing proofs that are classically valid, but where certain principles are either avoided entirely or only used with caution. The main principle to be avoided is excluded middle: that is, the axiom of classical logic stating that every proposition is either true or false. We refer to logic without excluded middle as intuitionistic logic.

1.2 The Metamathematics of Constructive Mathematics

1.2.1 Reasons for Studying

In the author’s opinion, the main reasoning for studying the metamathematics of constructive mathematics is the same as for classical mathematics: to get a better understanding of mathematical theories as they are used. This consists of identifying when and why particular axioms are needed to prove particular theorems, and finding the limitations of a theory. This includes knowing when a theory can neither prove nor disprove propositions of interest and knowing what mathematical objects are definable from within a theory.

Mathematical logic is also interesting to study as a mathematical field in its own right. Formal systems are mathematical objects themselves rich in properties worth studying and a source of challenging problems. In particular formal systems based on constructive mathematics have interesting properties not shared by classical ones. These included the disjunction property and numerical existence property, based on the BHK interpretation. We will see these in more detail in chapter 8.

Mathematical logic for constructive mathematics may even turn out to have practical benefits. Realizability allows one to extract algorithms from constructive proofs. If one has a constructive proof of a function having desired properties, instead of writing a computer program by hand, implementing the function, one may enter the proof into a proof assistant such as Coq and extract the program automatically.

1.2.2 Formal Systems

There is a very large number of formal systems that have been considered for constructive mathematics. For example, there are many intuitionistic theories based on first or higher order arithmetic that we do not consider at all in this thesis. However, there is one main system that is considered constructive and yet "general purpose" enough to provide a foundation for constructive mathematics. This is Martin-Löf type theory. Martin-Löf type theory was developed "from the ground up" to agree with the BHK interpretation of quantifiers. It is therefore very natural to constructive mathematicians as a foundation. However, this has the disadvantage that it is quite different to formal systems that classical mathematicians are used to studying.

The emphasis in this thesis is not on Martin-Löf type theory. As an alternative to Martin-Löf type theory, one may take instead constructive set theory as a foundation for constructive mathematics. This has the advantage of being the same language that classical mathematicians are used to using for formalisation. Yet there are set theories whose axioms can be justified as constructive and are still rich enough to provide a basis for most of the practice of constructive mathematics. Although many constructive set theories have been put forward, the emphasis in this thesis is very much on the most well known constructive set theory: Aczel's constructive Zermelo-Fraenkel (**CZF**). **CZF** has a natural interpretation into type theory and hence has solid constructive foundations and yet is powerful enough to develop a lot of mathematics.

1.2.3 Techniques

The techniques used to study classical mathematics are often inadequate for studying constructive mathematics. One reason for this is that excluded middle holds in models (in the sense of model theory) as well as in the more general boolean valued models. Hence these models are incapable of describing non-classical constructive theories, that is, theories where excluded middle is false. The other issue is that often the existence of these models is not proved in a constructive way.

This causes two problems. First of all constructive proofs are better here for the same reason that they are better anywhere: they tell us more about the theorem that we are proving and the objects we are constructing. Secondly, it is often useful for proving metamathematical results to be able to formalise the construction of our models inside the theory we are studying. Hence if we are studying a constructive theory it is useful to have a constructive proof of the existence of the models we are studying. In this thesis we will aim where possible to ensure that our proofs are constructively valid.

Unfortunately this is not always possible and in some instances, although we will be proving results about constructive theories, the proofs themselves will be non constructive.

There is a rich variety of models more suited to constructive theories including Kripke models, Beth models, Heyting valued models, and realizability models. These are fully described, for example in [37]. In this thesis the emphasis is very much on realizability models.

One way of looking at realizability models is that we start off with some notion of “rule” provided by a structure called a *partial combinatory algebra* (or a more general structure) and then use this notion of “rule” in the BHK interpretation. Since realizability is so closely related to the BHK interpretation, it provides very natural models for constructive mathematics.

The main aim of this thesis is to develop realizability models to help us understand better the limitations of various constructive set theories.

1.3 Outline of the Thesis

We start in chapter 2 by giving a brief introduction to combinatory algebras and constructive set theory.

In chapter 3 we define structures that we call *Kripke realizability* models. We prove that they are sound for intuitionistic logic and show that they generalise Kripke models and realizability models.

In chapter 4 we construct realizability models for constructive set theory. These generalise existing models by allowing the pca used to construct them to be a class rather than a set. We give some examples where it is a proper class and show that in this case the power set axiom can fail.

In chapter 5 we study the automorphism groups of partial combinatory algebras. In particular we show that realizability can be used as a tool to find restrictions on the automorphism groups of several examples of pcas.

In chapter 6 we develop realizability models based on automorphisms of pcas that can be used to show that choice principles are independent of $\mathbf{CZF}$. We call these symmetric realizability models. We give an example of a symmetric realizability model where countable choice fails.

In chapter 7 we adapt the models from chapter 6 to allow the order pca used to construct them to be a proper class. We use this to show that a very weak choice principle, $\mathbf{wPAx}$ is independent of $\mathbf{CZF}$.

Finally in chapter 8 we will use Kripke realizability models to show what is by far the biggest result in this thesis. A theory has the *existence property* if whenever $(\exists x)\phi(x)$ is provable, there is a formula $\chi(x)$ such that $(\exists! x)\phi(x) \wedge \chi(x)$ is provable. This property is often expected for constructive theories on the basis of the BHK interpretation, but we will show that it fails for $\mathbf{CZF}$.

1.4 Notation

We will write

$$A := B$$

to mean that A is defined to be B.

We will follow the convention that $t[x_1, \ldots, x_n/r_1, \ldots, r_n]$ means simultaneous replacement of the free variables $x_1, \ldots, x_n$ by the terms $r_1, \ldots, r_n$. However, we will always implicitly assume that when we do this any variables that occur free in r_i do not become bound after the substitution. This is always possible by relabelling bound variables. This applies both for lambda terms and for formulas.

We will often write a term with free variables amongst $x_1, \ldots, x_n$ as $t(x_1, \ldots, x_n)$. Then given terms $r_1, \ldots, r_n$, we write $t(r_1, \ldots, r_n)$ to mean $t[x_1, \ldots, x_n/r_1, \ldots, r_n]$.

We will follow the convention from constructive set theory of referring to sets that contain at least one element as *inhabited*. In intuitionistic logic this is a strictly stronger notion than not empty.

In the following table we list some remaining notational conventions.

Notation	Meaning
$\langle , \rangle$	ordered pair
$\mathrm{First}()$	first component of ordered pair
$\mathrm{Second}()$	second component of ordered pair
$H \leq G$	H is a subgroup of G
$\mathrm{mv}(A, B)$	multivalued functions from A to B
$\sup_i d_i$	the supremum of the set $\{d_i \mid i \in \omega\}$
$X^{\leq}$	$\{y \in P \mid (\exists x \in X) y \leq x\}$, where $X \subseteq P$ a poset
$\mathrm{Orb}_{\mathrm{G}}(a)$	the orbit of a under G
$\mathrm{Stab}_G(a)$	the stabiliser of a in G
$\lvert a \rvert$	cardinality of a set a
$\mathcal{P}(A)$	power set of A
$\mathcal{P}^*(A)$	set of inhabited subsets of A

Chapter 2

Background Material

In this chapter we give a brief introduction to partial combinatory algebras as used in the remainder of this thesis. A more detailed introduction to partial combinatory algebras and order partial combinatory algebras is contained in the first chapter of [39]. This material refers to definitions and results in the lambda calculus. The definitive reference text for this area is [4].

We will also define the two intuitionistic set theories **IZF** and **CZF** that will be referred to in this thesis, as well as a related theory, **CST** and will also prove a few simple lemmas that are used later.

2.1 Applicative Structures and Some Useful Notation

In this section we introduce partial combinatory algebras and the more general order partial combinatory algebras. We follow [39] and start by giving the very general definition, applicative structure.

Definition 2.1.1. An *applicative structure*, $\mathcal{A}$, is a pair $\langle A, \cdot \rangle$, where $\cdot$ (which we refer to as application) is a partial function

$$\cdot : A \times A \rightharpoonup A$$

Definition 2.1.2. 1. For $a, b \in \mathcal{A}$, we write $a.b$ or ab to mean $\cdot(a, b)$.

2. For $a_1, \ldots, a_n \in \mathcal{A}$, we write $a_1 \ldots a_n$ to mean $(\ldots(a_1.a_2).a_3). \ldots .a_n)$. That is, we take application to be left associative.

Since $\cdot$ is in general a partial operation, we will often need to use the following notation in order to make things clearer.

Definition 2.1.3. Let $f, g : A \rightharpoonup A$ be partial functions and $a, a' \in A$, then

1. We write $f(a) \downarrow$ to mean that f is defined at a.
2. We write $f(a) \simeq g(a')$ to mean that $f(a) \downarrow$ if and only if $g(a') \downarrow$, *and* that if this is the case then $f(a) = g(a')$.

When visualising applicative structures, it is often useful to consider which partial functions are *representable*.

Definition 2.1.4. Let $\mathcal{A}$ be an applicative structure, and let $a \in \mathcal{A}$. We say that a *represents* a partial function, $f : \mathcal{A} \rightharpoonup \mathcal{A}$, if for all $b \in \mathcal{A}$,

$$a.b \simeq f(b)$$

We say that $f : \mathcal{A} \rightharpoonup \mathcal{A}$ is *representable* if there is $a \in \mathcal{A}$ such that a represents f.

Definition 2.1.5. Given an applicative structure, $\mathcal{A}$, we define *terms* over $\mathcal{A}$ inductively as follows

1. There is a countable supply of free variables, x_i, each of which is a term.
2. Each element, a of $\mathcal{A}$ is a term.

3. If s and t are terms, then the ordered pair, $\langle s, t\rangle$ is also a term. We write this as $(s.t)$.

We say that a term is *open* if it contains at least one free variable, and *closed* if it contains no free variables.

It is useful to extend the notation we had before to all terms.

Definition 2.1.6. We define inductively what it means for a closed term, s, to *denote* $a \in \mathcal{A}$

1. If $a' \in \mathcal{A}$, then a' denotes a if and only if $a = a'$
2. $(s'.s'')$ denotes a if and only if there are $a', a'' \in \mathcal{A}$ such that s' denotes a', s'' denotes a'', and $a'.a'' \simeq a$.

If t is a closed term and there is an $a \in \mathcal{A}$ such that t denotes a, we write $t \downarrow$ and say that t denotes.

If $t(x_1, \ldots, x_n)$ is an *open* term with free variables amongst $x_1, \ldots, x_n$, we write $t \downarrow$ to mean that for every $a_1, \ldots, a_n \in \mathcal{A}$, $t(a_1, \ldots, a_n) \downarrow$.

Let $s(x_1, \ldots, x_n)$ and $t(x_1, \ldots, x_n)$ be terms over an applicative structure, $\mathcal{A}$, with free variables amongst $x_1, \ldots, x_n$. Then we write $s \simeq t$ to mean that for every $a_1, \ldots, a_n \in \mathcal{A}$, $s(a_1, \ldots, a_n) \downarrow$ if and only if $t(a_1, \ldots, a_n) \downarrow$ and if $s(a_1, \ldots, a_n) \downarrow$ then there is a such that $s(a_1, \ldots, a_n)$ denotes a and $t(a_1, \ldots, a_n)$ denotes a.

2.2 Partial Combinatory Algebras

We now give the definition of partial combinatory algebra.

Definition 2.2.1. A *partial combinatory algebra* (pca) is an applicative structure, $\mathcal{A}$, with distinguished elements, s and k such that,

1. for all $a, b \in \mathcal{A}$, $\mathbf{k}ab \simeq a$.

2. for all $a, b \in \mathcal{A}$, $\mathrm{s}ab \downarrow$.

3. for all $a, b, c \in \mathcal{A}$, $\mathrm{s}abc \simeq ac(bc)$.

If in addition $\mathrm{s} \neq \mathbf{k}$ then we say that $\mathcal{A}$ is a *non trivial* pca. If $\mathrm{s} = \mathbf{k}$ we say that $\mathcal{A}$ is *trivial*.

Definition 2.2.2. If $\mathcal{A}$ is a pca and the application map $\cdot : A \times A \rightharpoonup A$ is a total function we say that $\mathcal{A}$ is a *combinatory algebra*.

One of the main motivations for pcas is that they should be able to provide a basis for realizability. According to this we should be able to encode mathematical objects as elements of $\mathcal{A}$. “Rules” that transform mathematical objects into other mathematical objects should be representable in $\mathcal{A}$. If we have a term $t(x)$ with one free variable then we can easily construct a function that takes a and returns $t(a)$. Hence this function should be representable in $\mathcal{A}$. The proposition below shows that we can do this, and moreover, in the proof we can see that the pca axioms are precisely what we require to do this.

Proposition 2.2.3. *Suppose that $t(x)$ is a term. Then there is a term t^* that does not contain the free variable x such that $t^* \downarrow$ and for all $a \in \mathcal{A}$*

$$t^* a \simeq t(a)$$

Proof. We define t^* by induction on the definition of terms.

1. If t is the free variable x, we set $t^* = \mathbf{skk}$ (note that this represents the identity function on $\mathcal{A}$).

2. If t is a free variable, y distinct from x, or an element a, of $\mathcal{A}$, we set $t^* = \mathbf{k}y$ or $t^* = \mathbf{k}a$ respectively.

3. If $t = (t'.t'')$, we set $t^* = \mathbf{s}t'^*t''^*$.

One can easily check that by induction that t^* is as required. □

We write t^* as

$$(\lambda x).t(x)$$

and write

$$(\lambda x_1, \ldots, x_n).t(x_1, \ldots, x_n)$$

to mean

$$(\lambda x_1). \ldots (\lambda x_n).t(x_1, \ldots, x_n)$$

We can use lambda terms to construct fixed point elements in the following sense. This is proved, for example, in chapter 1 of [39].

Proposition 2.2.4. *Let $\mathcal{A}$ be a pca. Then,*

1. *There is $y \in \mathcal{A}$ such that for any $f \in \mathcal{A}$,*

$$(yf) \simeq f(yf)$$

2. *There is $z \in \mathcal{A}$ such that for any $e \in \mathcal{A}$, $ze \downarrow$, and for every $f \in \mathcal{A}$,*

$$(ze)f \simeq e(ze)f$$

The following theorem states formally that for any pca, we can find elements that behave like pairing and projection functions, as well as elements behaving like the natural numbers. This is a well known theorem, and a proof can be found, for example in chapter VI of [5].

Theorem 2.2.5. *Let $\mathcal{A} = \langle A, \mathbf{s}, \mathbf{k} \rangle$ be a pca. Then we can find elements $\mathbf{p}$, $\mathbf{p}_0$, $\mathbf{p}_1$, $\mathbf{0}$, $\mathbf{s}_N$, $\mathbf{p}_N$, $\mathbf{d}$, and a subset $N \subseteq A$ such that the following are satisfied.*

1. *$\forall a, b \in \mathcal{A}$, $\mathbf{p}ab \downarrow$ and $\mathbf{p}_0(\mathbf{p}ab) = a$, $\mathbf{p}_1(\mathbf{p}ab) = b$*

2. *$\mathbf{0} \in N$, whenever $n \in N$, we have $\mathbf{s}_N n \downarrow$, and $\mathbf{s}_N n \in N$, and N is the smallest set with this property*

3. *$\forall n \in N$, $\mathbf{p}_N n \downarrow$, and $\mathbf{p}_N(\mathbf{s}_N n) = n$*

4. *$\forall n, m \in N, a, b \in \mathcal{A}$, $\mathbf{d}nmab = a$ if $n = m$, and $\mathbf{d}nmab = b$ if $n \neq m$*

5. *if there is $n \in N$ such that $\mathbf{0} = \mathbf{s}_N n$, then $\mathcal{A}$ is trivial.*

For $n \in \omega$ we define $\underline{n}$ inductively by $\underline{0} = \mathbf{0}$ and $\underline{n+1} = \mathbf{s}_N \underline{n}$.

We will often write $\mathbf{p}_0 e$ as $(e)_0$ and $\mathbf{p}_1 e$ as $(e)_1$ for convenience.

The constants in theorem 2.2.5 can be constructed from $\mathbf{s}$ and $\mathbf{k}$. We will need this fact later, since it implies that these constants can be chosen so that they are fixed by any automorphism fixing $\mathbf{s}$ and $\mathbf{k}$.

However, it is often useful to explicitly give suitable constants for a particular pca. For instance this is the case in chapter 5. We will give some examples of this in section 2.4.

2.3 Order Partial Combinatory Algebras

Order partial combinatory algebras were developed by van Oosten and Hofstra in [40] as a generalisation of pcas. They are applicative structures that also have an order structure and the pca axioms are satisfied only up to the ordering. To help define this, the following notation is useful.

Definition 2.3.1. Let $\mathcal{A}$ be an applicative structure with partial ordering, $\leq$, and let s, t be terms over $\mathcal{A}$. We write

$$s \preceq t$$

to mean that if $t \downarrow$, then also $s \downarrow$, and

$$s \leq t$$

Definition 2.3.2. An *order partial combinatory algebra* (opca) is an applicative structure, $\mathcal{A}$, together with a partial ordering, $\leq$, and distinguished elements s and $\mathbf{k}$ such that

1. If $a, b, a', b' \in \mathcal{A}$ with $a \leq a'$ and $b \leq b'$, then $a.b \preceq a'.b'$.
2. For all $a, b \in \mathcal{A}$, $\mathbf{k}ab \preceq a$.
3. For all $a, b \in \mathcal{A}$, $\mathrm{s}ab \downarrow$.
4. For all $a, b, c \in \mathcal{A}$, $\mathrm{s}abc \preceq ac(bc)$.

One can easily generalise proposition 2.2.3 to the following. (This appears in chapter 1 of [39].)

Proposition 2.3.3. *Suppose that $t(x)$ is a term. Then there is a term t^* that does not contain the free variable x such that $t^* \downarrow$ and for all $a \in \mathcal{A}$*

$$t^*a \preceq t(a)$$

As noted by van Oosten in, for instance, chapter 1 of [39], proposition 2.2.4 still holds for order pcas.

Proposition 2.3.4. *Let $\mathcal{A}$ be an opca. Then,*

1. *There is $y \in \mathcal{A}$ such that for any $f \in \mathcal{A}$,*

$$(yf) \preceq f(yf)$$

2. *There is $z \in \mathcal{A}$ such that for any $e \in \mathcal{A}$, $ze \downarrow$, and for every $f \in \mathcal{A}$,*

$$(ze)f \preceq e(ze)f$$

The proof of theorem 2.2.5 can easily be adapted to give the following theorem over order pcas. This again appears in chapter 1 of [39].

Theorem 2.3.5. *Let $\mathcal{A} = \langle A, \mathbf{s}, \mathbf{k} \rangle$ be an opca. Then we can find elements $\mathbf{p}$, $\mathbf{p}_0$, $\mathbf{p}_1$, $\mathbf{0}$, $\mathbf{s}_N$, $\mathbf{p}_N$, $\mathbf{d}$, and a subset $N \subseteq A$ such that the following are satisfied.*

1. *$\forall a, b \in \mathcal{A}$, $\mathbf{p}ab \downarrow$ and $\mathbf{p}_0(\mathbf{p}ab) \leq a$, $\mathbf{p}_1(\mathbf{p}ab) \leq b$*
2. *$\mathbf{0} \in N$, whenever $n \in N$, we have $\mathbf{s}_N n \downarrow$, and $\mathbf{s}_N n \in N$, and N is the smallest set with this property*
3. *$\forall n \in N$, $\mathbf{p}_N n \downarrow$, and $\mathbf{p}_N(\mathbf{s}_N n) \leq n$*
4. *$\forall n, m \in N, a, b \in \mathcal{A}$, $\mathbf{d}nmab \leq a$ if $n = m$, and $\mathbf{d}nmab \leq b$ if $n \neq m$*

2.4 Examples of Pcas and Opcas

The canonical example of a pca is based on computable numbers as follows.

Example 2.4.1. Define a partial binary operation, $\cdot$, on $\mathbb{N}$ by $n.m = \phi_n(m)$, where we write ϕ_n for the computable function encoded by n.

Note that the representable partial functions are precisely the computable ones. We can clearly define computable functions to fulfil the roles of $\mathbf{s}$ and $\mathbf{k}$. Here, $\mathbf{k}$ would accept a number n and generate a program that returns n on any input. $\mathbf{s}$ would define a program that given input e, returns a program that given input f, returns another program that given input g runs e and f as programs with input g, then applies the result of the former to the result of the latter. This defines the pca $\mathcal{K}_1$, sometimes referred to as the *first Kleene algebra*.

For $\mathcal{K}_1$, we can explicitly prove theorem 2.2.5 by taking N to be $\mathcal{K}_1$ itself since successor, predecessor, and decider are clearly computable.

Example 2.4.2. Let $A = \mathbb{N}^{\mathbb{N}}$. This is can be thought of as a topological space (usually referred to as Baire space) by taking the product topology on $\mathbb{N}$ with the discrete topology. The continuous functions on A can be encoded as elements of A in the following way. Given a continuous $F : A \to A$, we can find an f such that for all $g \in A$,

$$F(g)(n) = f(\langle n \rangle * \bar{g}(m)) - 1$$

where $*$ indicates list concatenation, $\bar{g}(m)$ is a list of the first m values of g, and m is chosen to be the first number such that $f(\langle n \rangle * \bar{g}(m)) > 0$. This might suggest the following application on A.

$$f * g(n) = \begin{cases} f(\langle n \rangle * \bar{g}(m)) - 1 & \text{if there is a least } m \text{ such that } f(\langle n \rangle * \bar{g}(m)) > 0 \\ \text{undefined} & \text{otherwise} \end{cases}$$

However, note that this application might return a partial function, where A consists only of total functions. We therefore need to define application as

$$f \cdot g = \begin{cases} f * g & f * g \text{ is total} \\ \text{undefined} & \text{otherwise} \end{cases}$$

This application does give a pca, referred to as $\mathcal{K}_2$, or the *second Kleene algebra*

Example 2.4.3. In the previous example, note that **s** and **k** are both computable functions and observe that if the application of two computable functions is defined, then it is also computable. Hence there is a subpca of $\mathcal{K}_2$ consisting of the computable functions. This pca is called $\mathcal{K}_2^{\mathrm{REC}}$.

In both $\mathcal{K}_2$ and $\mathcal{K}_2^{\mathrm{REC}}$ we can take N from theorem 2.2.5 to be the constant functions with the usual zero and successor.

Example 2.4.4. We can define an application on $\mathcal{P}(\omega)$. First fix encodings of finite subsets of ω and pairs of elements of ω as elements of ω. We write $\langle , \rangle$ for the pairing function $\omega^2 \to \omega$, and write $n \subseteq A$ to mean that $n \in \omega$ encodes a finite subset of $A \in \mathcal{P}(\omega)$. We can now define application as

$$A.B = \{c \mid \langle b, c \rangle \in A, b \subseteq B\}$$

This forms a combinatory algebra known as the graph model (of the lambda calculus). As for $\mathcal{K}_2$, the representable functions are precisely the continuous ones.

Example 2.4.5. In the previous example, s and **k** can be taken to be computably enumerable sets and that if A and B are computably enumerable, then $A.B$ is also computably enumerable. Hence $\mathcal{P}(\omega)$ has a subpca $\mathcal{P}(\omega)^{\text{c.e.}}$ of the computably enumerable sets.

In both $\mathcal{P}(\omega)$ and $\mathcal{P}(\omega)^{\text{c.e.}}$ we can take N to be singletons $\{n\}$ for $n \in \omega$ with the usual successor and predecessor.

Example 2.4.6. Given a directed complete partial order (dcpo), D, we can define a dcpo, D_∞ containing D such that D_∞ is a combinatory algebra. We first define D_i recursively by $D_0 = D$ and D_{i+1} is the dcpo of homomorphisms $D_i \to D_i$. We then define maps $\varphi_i : D_i \to D_{i+1}$, $\psi_i : D_{i+1} \to D_i$ by $\varphi_0(d) = (\lambda x).d$, $\psi_0(f) = f(\bot)$, and $\varphi_{i+1}(d) = \varphi_i \circ d \circ \psi_i$, $\psi_{i+1}(f) = \psi_i \circ f \circ \varphi_i$. D_∞ is then the inverse limit of D_i, ψ_i. Application is then defined as

$$d.d' = \sup_i d_{i+1}(d'_i)$$

For more details see chapter 5 of [4].

$\mathcal{K}_1$ and $\mathcal{K}_2$ were first developed by Kleene, $\mathcal{P}(\omega)$ was developed independently by Plotkin and Scott, and D_∞ was developed by Scott.

Example 2.4.7. Let $\mathcal{A}$ be a pca. Then note that $\mathcal{A}$ is also an opca with the discrete ordering. That is $e \leq f$ if and only if $e = f$.

One might expect a converse to this wherein every opca with the discrete order is a pca. We will see some counterexamples in section 2.5.3 showing that this is not the case.

Example 2.4.8. Suppose that $\mathcal{A}$ is a pca. Then one can give an order pca structure on $\mathcal{P}(\mathcal{A})$ as follows. Given $A, B \in \mathcal{P}(\mathcal{A})$, if $a.b \downarrow$ for all $a \in A, b \in B$, then let $A.B := \{a.b \mid a \in A, b \in B\}$. Otherwise $A.B$ is undefined. The ordering of $\mathcal{P}(\mathcal{A})$ is given by inclusion. Note that we can take s to be $\{\mathbf{s}_\mathcal{A}\}$ and **k** to be $\{\mathbf{k}_\mathcal{A}\}$.

2.5 Term Models of the Lambda Calculus and Combinatory Logic

One way of viewing pcas is as models of combinatory logic and so it should not be surprising that pcas can be constructed as term models of the lambda calculus and combinatory logic.

Throughout this thesis we will often use pcas and opcas constructed in such a way and so we now briefly introduce the lambda calculus and term models.

2.5.1 The Lambda Calculus

Definition 2.5.1. The class, Λ of lambda terms is defined inductively as follows:

1. $x_i \in \Lambda$ where x_i is one of a countable supply of free variables
2. if $M \in \Lambda$ and x is a variable, then $(\lambda x).M \in \Lambda$
3. if $M, N \in \Lambda$, then $(MN) \in \Lambda$

For our purposes we will also consider the lambda calculus with a set of constants added to the language. We therefore make the following definition

Definition 2.5.2. Given a set, C the class $\Lambda(C)$ is defined inductively as follows:

1. for $c \in C$, there is a corresponding atomic term **c** $\in \Lambda(C)$
2. $x_i \in \Lambda(C)$ where x_i is one of a countable supply of free variables
3. if $M \in \Lambda(C)$ and x is a variable, then $(\lambda x).M \in \Lambda(C)$
4. if $M, N \in \Lambda(C)$, then $(MN) \in \Lambda(C)$

The lambda calculus, combinatory logic, and related systems are all based on notions of reduction.

Definition 2.5.3. A *notion of reduction* on Λ is a binary relation on Λ.

Definition 2.5.4. A notion of reduction, R is *compatible* if whenever $L, M, N \in \Lambda$ and $(M, N) \in R$, also $(LM, LN) \in R$, $(ML, NL) \in R$ and $((\lambda x).M, (\lambda x).N) \in R$.

Definition 2.5.5. For a notion of reduction, R, one step R reduction, $\rightarrow_R$ is the compatible closure of R.

$\twoheadrightarrow_R$, is the reflexive, transitive closure of $\rightarrow_R$.

$=_R$ is the reflexive, transitive, and symmetric closure of $\rightarrow_R$.

We say that a term M is in *normal form* (over R) if one cannot perform R-reduction.

The main reduction that we will be considering is that of β-reduction. That is, the following notion of reduction:

Definition 2.5.6.

$$\beta := \{((\lambda x).M)N, M[x/N])\}$$

Definition 2.5.7. A notion of reduction R has the *Church-Rosser property* if whenever $M \twoheadrightarrow_R L_1$ and $M \twoheadrightarrow_R L_2$ then there is some N such that $L_1 \twoheadrightarrow_R N$ and $L_2 \twoheadrightarrow_R N$. We write this in a diagram as follows.

$$\begin{tikzcd}
& M \arrow[dl, two heads, "R"'] \arrow[dr, two heads, "R"] & \\
L_1 \arrow[dr, two heads, dashed, "R"'] & & L_2 \arrow[dl, two heads, dashed, "R"] \\
& N &
\end{tikzcd}$$

Theorem 2.5.8 (Church-Rosser). *β has the Church Rosser property.*

Proof. A proof for Λ can be found for example in [4]. The same proof carries over to $\Lambda(C)$, but for completeness we will show explicitly that it follows from the result for Λ.

Suppose that $M \twoheadrightarrow_R L_1$ and $M \twoheadrightarrow_R L_2$. Let $c_1, \dots, c_n$ be a list of the constants appearing in M, L_1, and L_2. Let $x_1, \dots, x_n$ be free variables not occurring anywhere in M, L_1 or L_2 (free or bound). Then note that replacing $c_1, \dots, c_n$ by $x_1, \dots, x_n$ commutes with β-reduction. Hence we can get the result by replacing $c_1, \dots, c_n$ by $x_1, \dots, x_n$ throughout, applying the usual Church-Rosser theorem, and then replacing $x_1, \dots, x_n$ by $c_1, \dots, c_n$ throughout. □

2.5.2 Combinatory Logic

Definition 2.5.9. The terms of *combinatory logic*, CL are defined inductively as follows:

1. each x_i of a countable supply of free variables, x_i is a term
2. the constants $\mathbf{k}$ and $\mathbf{s}$ are terms
3. if M and N are terms, then $(M.N)$ is a term.

As for the lambda calculus, we will also consider the modified definition with a set C of constants.

Definition 2.5.10. The terms of *combinatory logic* over C, $\mathrm{CL}(C)$ are defined inductively as follows:

1. if $c \in C$ then there is a corresponding $\mathbf{c} \in \mathrm{CL}(C)$
2. for each x_i of a countable supply of free variables, $x_i \in \mathrm{CL}(C)$
3. the constants $\mathbf{k}$ and $\mathbf{s}$ are terms of $\mathrm{CL}(C)$
4. if M and N are terms, then $(M.N)$ is a term of $\mathrm{CL}(C)$.

We can then define a notion of reduction R, as well as $\rightarrow_R$ and $\twoheadrightarrow_R$ over CL in exactly the same way as for the lambda calculus.

The main notion of reduction considered over CL, and indeed over $\mathrm{CL}(C)$, is the following:

Definition 2.5.11.

$$w := \{(\mathbf{k}MN, M) \mid M, N \in \mathrm{CL}(C)\} \cup \{(\mathbf{s}MNL, ML(NL)) \mid M, N, L \in \mathrm{CL}(C)\}$$

The following theorem corresponds to theorem 2.5.8 for $\Lambda(C)$. It is a well known theorem for CL proved, for instance, in [4], and as before can be easily adapted to $\mathrm{CL}(C)$.

Theorem 2.5.12. *w has the Church-Rosser property.*

2.5.3 Examples of Term Models

The simplest term model is the open term model, defined as follows.

Note that $=_\beta$ gives an equivalence relation on $\Lambda(C)$. Let $\mathcal{T}$ be the set of equivalence classes. Note that one can take the application of M and N to be $(M.N)$, since this operation respects the equivalence relation and we have s and **k** given as follows.

$$\begin{aligned} \mathrm{s} &:= (\lambda x, y, z).xz(yz) \\ \mathbf{k} &:= (\lambda x, y).x \end{aligned}$$

Let $\Lambda_0(C)$ be the set of closed terms. Then note that s and **k** given above are closed and $(M.N)$ is closed if both M and N are. Hence $\Lambda_0(C)$ gives a term model which is a subpca of $\mathcal{T}$.

The following example appears in chapter VI of [5].

Example 2.5.13. Let $NT \subseteq \mathrm{CL}(C)$ be the set of normal forms. Then we can define application on NT as follows:

$$M.N := \begin{cases} L & \text{if } M.N \twoheadrightarrow_R L \text{ for some normal form } L \\ \text{undefined} & \text{otherwise} \end{cases}$$

Proposition 2.5.14 (Beeson). *1. NT with the discrete order is an opca*

2. NT is not a pca

Proof. Suppose that $MN(LN) \twoheadrightarrow_w K$ where K is a normal form. Then s$MLN \rightarrow_w MN(LN)$ and hence s$MLN \twoheadrightarrow_w K$. Similarly for **k**.

To show that NT is not a pca, we will show that there are situations where s$MNL \downarrow$, but $ML(NL) \uparrow$. Let $N = L = (\lambda x).xx$. Let $M = \mathbf{k}$. Then NL has no normal form. That is $NL \uparrow$. Hence $ML(NL) \uparrow$. However, s$MNL \twoheadrightarrow_w L$, and so s$MNL \downarrow$. □

Remark 2.5.15. *If we do the same thing with $\Lambda(C)$ we don't even get an opca. Let $M = N = (\lambda x).(\lambda y).yy$. Then*

$$\begin{aligned} \mathbf{s}MN &= (\lambda u, v, w).uw(vw)MN \\ &=_\beta (\lambda w).Mw(Nw) \\ &=_\beta (\lambda w).(\lambda y).yy(\lambda y).yy \end{aligned}$$

However, note that this is not a normal form since we can apply β-reduction to the subterm $(\lambda y).yy(\lambda y).yy$. We can see that in fact it is not equivalent to any normal form and hence $\mathbf{s}MN \uparrow$, so this is not even an opca.

The Term Model of Inside First Reduction

Another term model built from normal forms over $\mathrm{CL}(C)$ is the term model of *left most inner most reduction*. This is a reduction strategy, that is, a canonical way of reducing a term of $\mathrm{CL}(C)$ to normal form. We define it in the following way, essentially following the example in section 6.11 of [5]. We start by defining a partial operation on $\mathrm{CL}(C)$.

Definition 2.5.16. We define a sequence of partial operators, RED_n for each n as follows:

For $n = 0$, define RED_0 as follows:

1. if t is a normal form, $\mathrm{RED}_0(t) = t$
2. for $t = \mathbf{k}rs$ where r and s are normal forms, $\mathrm{RED}_0(\mathbf{k}rs) = r$

If RED_n has been already been defined, then we define RED_{n+1} as follows:

1. if $\mathrm{RED}_n(t) \downarrow$, then $\mathrm{RED}_{n+1}(t) = \mathrm{RED}_n(t)$

2. for $t = \mathrm{s}rsu$, where r, s, and u are normal forms,

$$\mathrm{RED}_{n+1}(\mathrm{s}rsu) \simeq \mathrm{RED}_n(\mathrm{RED}_n(ru)\,\mathrm{RED}_n(su))$$

3. if $t = rs$ and neither of previous cases apply, then

$$\mathrm{RED}_{n+1}(rs) \simeq \mathrm{RED}_n(\mathrm{RED}_n(r)\,\mathrm{RED}_n(s))$$

We then define RED as

$$\mathrm{RED} = \bigcup_{n\in\omega} \mathrm{RED}_n$$

Note that if $\mathrm{RED}(t)$ is defined, then it is a normal form.

We now define our pca, $\mathcal{T}$

Definition 2.5.17. Let $\mathcal{T}$ be the set of normal forms of $\mathrm{CL}(C)$ together with the following application:

$$s.t := \mathrm{RED}(s.t)$$

(undefined if $\mathrm{RED}(s.t)$ is undefined)

Note that since this is an applicative structure (in the sense of definition 2.1.1) we can define the notion of terms over $\mathcal{T}$. Fortunately we are free to switch between thinking of terms and terms over $\mathcal{T}$ by the following proposition.

Proposition 2.5.18. *Suppose that t is a closed term over $\mathcal{T}$ (in the sense of definition 2.1.5) and write t^* for the corresponding term (in the sense of definition 2.5.9). Then $\mathrm{RED}(t^*)$ is defined if and only if t denotes, and in this case we have*

$$\mathrm{RED}(t^*) = t$$

Proof. This appears as parts (i) and (ii) of lemma 6.1.1 in chapter VI of [5]. However, we include a proof here for completeness.

We prove this by induction on t.

First suppose that t is an element of $\mathcal{T}$. Then t^* is a normal form and so $\mathrm{RED}(t^*) = t^* = t$.

Now suppose that $t = t_1.t_2$. Then by the definition of terms over $\mathcal{T}$, $t \downarrow$ if and only if $t_1 \downarrow$, $t_2 \downarrow$, and $t_1.t_2 \downarrow$. By induction, $t_1 \downarrow$ if and only if $\mathrm{RED}(t_1^*)$ is defined and $t_2 \downarrow$ if and only if $\mathrm{RED}(t_2^*)$ is defined. Note that by the definition of RED, $\mathrm{RED}(t_1^* t_2^*) \simeq \mathrm{RED}(\mathrm{RED}(t_1^*)\,\mathrm{RED}(t_2^*))$ (split into cases where t_1^* and t_2^* are both normal forms and where one of them isn't). In particular if $\mathrm{RED}(t_1^* t_2^*)$ is defined then both $\mathrm{RED}(t_1^*)$ and $\mathrm{RED}(t_2^*)$ are defined. We can easily see that $\mathrm{RED}(t_1^* t_2^*) = t_1.t_2$ if both sides are defined, so the result follows. □

Proposition 2.5.19. *$\mathcal{T}$ is a pca.*

Proof. Note firstly that $\mathbf{s}$ and $\mathbf{k}$ are normal terms and hence elements of $\mathcal{T}$.

If r and s are normal forms, then so are $\mathbf{k}r$ and $\mathbf{s}rs$. Hence $\mathbf{k}r \downarrow$, $\mathbf{s}r \downarrow$, and $\mathbf{s}rs \downarrow$. Also $\mathrm{RED}(\mathbf{k}rs) = r$, so $\mathbf{k}rs = r$.

It remains only to check that for all r, s, t, $\mathbf{s}rst \simeq rt(st)$. However this is clear from the definition. (In fact the left hand side is defined at stage $n + 1$ if and only if the right hand side is defined at stage n.) □

Some Lemmas

Suppose that θ is a function from C to C. Then we can consider it as the following notion of reduction:

$$\Theta := \{(\mathbf{c}, \theta(\mathbf{c})) \mid c \in C\}$$

Lemma 2.5.20. *If $M \to_w L$ and $M \to_\Theta M'$, then there is L' such that $L \twoheadrightarrow_\Theta L'$ and $M' \to_w L'$. That is, we have the following diagram.*

$$\begin{tikzcd}
M \arrow[r, "w"] \arrow[d, "\Theta"'] & L \arrow[d, dashed, two heads, "\Theta"] \\
M' \arrow[r, dashed, "w"'] & L'
\end{tikzcd}$$

Proof. Suppose first that the redex in $M \to_w L$ is of the form $\mathbf{s}M_1M_2M_3$. If the redex in $M \to_\Theta M'$ occurs in none of M_1, M_2, or M_3 then the two reductions "commute," so we trivially get the result. Suppose that the redex in $M \to_\Theta M'$ occurs in M_3. Note that the contractum in the $\mathbf{s}$-reduction is $M_1M_3(M_2M_3)$, and so we can apply the same Θ-reduction to each copy of M_3 to get the result. We can similarly deal with the case when the Θ-redex occurs in M_1 or M_2.

We can do the same thing if the redex in $M \to_w L$ is of the form $\mathbf{k}M_1M_2$. □

Lemma 2.5.21.

$$\begin{tikzcd}
M \arrow[r, "w"] \arrow[d, two heads, "\Theta"'] & L \arrow[d, dashed, two heads, "\Theta"] \\
M' \arrow[r, dashed, two heads, "w"'] & L'
\end{tikzcd}$$

Proof. This follows from the previous lemma by a diagram chase. □

Lemma 2.5.22. *Suppose that $M \in \mathrm{CL}(C)$ and $a, b \in C$ are such that $a \neq b$ and $M\mathbf{a} =_w \mathbf{b}$. Then for any $c \in C$, $M\mathbf{c} =_w \mathbf{b}$.*

Proof. Let $c \in C$. Since $a \neq b$, we can define θ such that $\theta(b) = b$ and $\theta(a) = c$.

Note that since $\mathbf{b}$ is a w-normal form, we can use the Church-Rosser theorem to show that $M\mathbf{a} \twoheadrightarrow \mathbf{b}$. We can apply Θ reduction to $M\mathbf{a}$ to get $M\mathbf{c}$, and so by the previous lemma we get that $M\mathbf{c} \twoheadrightarrow_w L$ where $\mathbf{b} \twoheadrightarrow_\Theta L$. However, L must be equal to $\mathbf{b}$, since $\mathbf{b}$ itself is its only subterm and $\theta(b) = b$. Hence $M\mathbf{c} \twoheadrightarrow_w \mathbf{b}$ as required. □

Note that as long as we know for all $x, y \in C$ either $x = y$ or $x \neq y$ the above proof is valid constructively.

2.6 Class Order Partial Combinatory Algebras

In definition 2.1.1 we defined an applicative structure in terms of a *set*, A. However, in many theorems this isn't strictly necessary, and the same proofs work if we instead take A to be a class.

Definition 2.6.1. A *class applicative structure*, $\mathcal{A}$, is a class A, together with a class ternary relation, $\cdot$. Formally A is a formula with one free variable, and $\cdot$ a formula with three free variables, $\phi(x, y, z)$, such that $\phi(x, y, z) \wedge \phi(x, y, z')$ implies $z = z'$.

Formally we defined $\cdot$ as a formula with three free variables, $\phi(x, y, z)$. We view it as a partial binary operation as follows.

$x.y \downarrow$ is the formula $(\exists z)\phi(x, y, z)$ and $x.y = z$ is the formula $\phi(x, y, z)$. This allows us to treat class applicative structures as if they are (set) applicative structures and to use the same notation as before.

We can now define class order pcas.

Definition 2.6.2. A *class order partial combinatory algebra* (copca) is a class applicative structure with a class binary relation $\leq$ which is reflexive and transitive, together with distinguished elements s and $\mathbf{k}$ such that

1. If $a, b, a', b' \in \mathcal{A}$ with $a \leq a'$ and $b \leq b'$, then $a.b \preceq a'.b'$.
2. For all $a, b \in \mathcal{A}$, $\mathbf{k}ab \preceq a$.
3. For all $a, b \in \mathcal{A}$, $\mathrm{s}ab \downarrow$.
4. For all $a, b, c \in \mathcal{A}$, $\mathrm{s}abc \preceq ac(bc)$.

Proposition 2.6.3. *Suppose that $t(x)$ is a term. Then there is a term t^* that does not contain the free variable x such that $t^* \downarrow$ and for all $a \in \mathcal{A}$*

$$t^*a \preceq t(a)$$

Proof. In proposition 2.2.3 we constructed explicitly the term t^*.

This term still works as required. For example, consider the inductive step, ie $t(x) = t_1(x)t_2(x)$. Then by our definition in the proof of proposition 2.2.3 we have that $t^* =$

$\mathbf{s}t_1^*t_2^*$. Since $t_1^* \downarrow$ and $t_2^* \downarrow$, we get that $t^* \downarrow$ and for all $a \in \mathcal{A}$,

$$\begin{aligned} t^*a &= \mathbf{s}t_1^*t_2^*a \\ &\preceq (t_1^*a)(t_2^*a) \\ &\preceq t_1(a)t_2(a) \\ &= t(a) \end{aligned}$$

□

Theorem 2.6.4. *Theorem 2.3.5 still holds for class order pcas, $\mathcal{A}$.*

Proof. Let $\mathcal{A}' \subset \mathcal{A}$ be the sub order pca generated by $\mathbf{s}$ and $\mathbf{k}$. That is $\mathbf{s}, \mathbf{k} \in \mathcal{A}'$ and whenever $e, f \in \mathcal{A}$ we also have $e.f \in \mathcal{A}$. Then we can apply theorem 2.3.5 to $\mathcal{A}'$ to construct pairing and projection elements and numerals. These still function as required in $\mathcal{A}$, so we get the result. □

We will study class order pcas in more detail in chapter 4.

2.7 Constructive Set Theory

In this section we see three set theories with intuitionistic logic. The first of these, **IZF** can be regarded as "**ZF** without excluded middle."

Definition 2.7.1. **IZF** is the theory with (intuitionistic logic and) the following axioms:

1. Extensionality
2. Separation
3. Pairing
4. Union
5. Infinity

6. Power Set
7. $\in$-induction
8. Collection

Collection is the following schema:

$$(\forall c \in a)(\exists y)\phi(x, y) \to (\exists z)(\forall c \in a)(\exists y \in z)\phi(x, y)$$

Compare this with the schema (equivalent in $\mathbf{ZF}$) Replacement:

$$(\forall c \in a)(\exists! y)\phi(x, y) \to (\exists z)(\forall c \in a)(\exists y \in z)\phi(x, y)$$

Definition 2.7.2. $\mathbf{IZF}_R$ is the set theory with the axioms of $\mathbf{IZF}$ except that it has Replacement instead of Collection.

$\mathbf{IZF}$ is extremely powerful. In fact Friedman showed in [12] that it has the same consistency strength as $\mathbf{ZF}$. On the other hand, $\mathbf{IZF}$ has some pleasing metamathematical properties that we will see in chapter 8.

Often one may be doing mathematics constructively for philosophical reasons. One may be an intuitionist: one believes mathematical objects only exist if they can be "mentally constructed." One may be a predicativist: one believes that a mathematical object cannot be constructed until it is defined predicatively - that is without quantifiers whose range includes the object being constructed. In this case one needs to ensure that the axioms of the set theory are constructively justified. There are (at least) two ways to go about this:

1. Directly justify each axiom as "true" with philosophical reasoning
2. Find another theory that already has a strong constructive foundation and interpret your set theory into it

Myhill in [27] took the first approach, introducing the following theories. Both of these are over a three sorted language with sorts for numbers, sets, and partial functions.

Definition 2.7.3. $\mathbf{CST}^-$ is the theory with (intuitionistic logic and) the following axioms:

1. Extensionality (for sets)
2. Bounded Separation (that is, separation for formulas where quantifiers can only appear as bounded quantifiers)
3. Pairing
4. Union
5. Exponentiation (that is, given any sets A and B there is a set containing precisely the functions $f : A \to B$)
6. Replacement
7. Axioms of Heyting Arithmetic for the number sort

Definition 2.7.4. $\mathbf{CST}$ is the theory $\mathbf{CST}^-$ together with relativised dependent choices $\mathbf{RDC}$.

In particular Myhill rejected the power set axiom in favour of the weaker exponentiation axiom because of the more predicative nature of exponentiation. He chose bounded separation over full separation for the same reason.

$\mathbf{CZF}$ arose via the second approach in [1] where Aczel showed that set theory can be interpreted into the predicative Martin-Löf type theory. Aczel also dropped the three sorted approach of $\mathbf{CST}$ and defined the following theories over the same language as $\mathbf{ZF}$.

Definition 2.7.5. $\mathbf{CZF}$ is the theory with (intuitionistic logic and) the following axioms

1. Extensionality
2. Bounded Separation

3. Pairing

4. Union

5. Strong Infinity

6. Subset Collection: the schema

$$(\exists c)(\forall u)((\forall x \in a)(\exists y \in b)\psi(x,y,u) \to \\ (\exists d \in c)((\forall x \in a)(\exists y \in d)\psi(x,y,u) \wedge (\forall y \in d)(\exists x \in a)\psi(x,y,u)))$$

7. $\in$-induction

8. Strong Collection: the schema

$$(\forall x \in a)(\exists y)\phi(x,y) \to \\ (\exists b)((\forall x \in a)(\exists y \in b)\phi(x,y) \wedge (\forall y \in b)(\exists x \in a)\phi(x,y))$$

Subset collection implies exponentiation and is implied by power set and can be seen as an "artifact" of the interpretation of set theory into type theory. As an alternative to subset collection, one may instead assume the equivalent fullness axiom (see section 4.5 of [3]). Given sets A and B, define $\mathrm{mv}(A,B)$, the class of multivalued functions as

$$\mathrm{mv}(A,B) := \{R \subseteq A \times B \mid (\forall a \in A)(\exists b \in B)(a,b) \in R\}$$

The fullness axiom can then be stated as follows

$$(\forall A,B)(\exists C \subseteq \mathrm{mv}(A,B))(\forall R)R \in \mathrm{mv}(A,B) \to (\exists S \in C)(S \subseteq R)$$

So essentially this says that the class $\mathrm{mv}(A,B)$ is "generated" by some set C. In particular if we assume the powerset axiom, then $\mathrm{mv}(A,B)$ itself is a set, so we can see that powerset implies fullness. Also note that C has to contain every function from A to B, because if R is a function and $S \subseteq R$ is a multivalued function then we must have $S = R$. Hence fullness implies exponentiation.

One can see that the fullness axiom asserts the existence of sets for which there is no apparent definition. In chapter 8 we will see that for the case $A = \mathbb{N}^{\mathbb{N}}, B = \mathbb{N}$, in fact there is no suitable set C that is definable within $\mathbf{CZF}$.

$\mathbf{CZF}$ is stronger than $\mathbf{CST}^-$ in two respects: replacement has been strengthened to strong collection and exponentiation has been strengthened to subset collection.

$\mathbf{CZF}$ is regarded today as one of the standard set theories for formalising constructive mathematics. This is because it is constructively valid because of its interpretation into type theory and yet can be used to prove mathematically interesting results that do not hold in weaker theories. For example, in [21] Lubarsky and Rathjen showed that the theory $\mathbf{CZF}_E$ that has only exponentiation in place of subset collection does not prove that the Dedekind reals form a set.

Throughout this thesis, anytime we prove results over set theory, unless otherwise stated we will be working over $\mathbf{CZF}$.

2.7.1 The Binary Intersection Axiom

One of the axiom schemas of $\mathbf{CZF}$ and $\mathbf{CST}$ is bounded separation. This states that for each bounded formula ϕ the following holds.

$$(\forall X)(\exists S)(\forall x)(x \in S \leftrightarrow (x \in X \wedge \phi(x)))$$

However, when proving soundness theorems for $\mathbf{CZF}$, it is sometimes easier to work with the simpler axiom of binary intersection. *Binary intersection* states that for any sets a and b, the binary intersection $a \cap b$ exists. That is,

$$(\forall X, Y)(\exists Z)(\forall z)(z \in Z \leftrightarrow (z \in X \wedge z \in Y))$$

Binary intersection is equivalent to bounded separation in the following sense.

Theorem 2.7.6. *Let $\mathbf{ECST_0}$ be the theory consisting of extensionality, pairing, union, replacement, and emptyset. Then in $\mathbf{ECST_0}$, the binary intersection axiom and bounded separation are equivalent.*

Proof. This is theorem 5.6 in [3]. □

In particular binary intersection and bounded separation are equivalent in the presence of the remaining axioms of **CZF**.

2.8 Inductive Definitions

Many of the structures defined in this thesis can be defined using inductive definitions, due to Peter Aczel in [2]. We work over **CZF**.

Definition 2.8.1. An *inductive definition* is a class Φ of ordered pairs. If $(X, a) \in \Phi$, we call X/a an *inference step* of Φ.

Definition 2.8.2. We say that a class Ψ is Φ-*closed* if whenever $(X, a) \in \Phi$ and $X \subseteq \Psi$, we have $a \in \Psi$.

Theorem 2.8.3. *Let Φ be an inductive definition. Then there is a smallest Φ-closed class $I(\Phi)$.*

A proof appears in [2], as well as in chapter 13 of [3].

We say that $I(\Phi)$ is the class *inductively defined* by Φ.

Chapter 3

Kripke Realizability Models

In this chapter we define a class of structures that we call *Kripke realizability* models. These were developed as a way to understand the constructions that appear in chapter 8. They generalise realizability and Kripke models for intuitionistic logic.

Generalisations of the different models of intuitionistic logic have already been studied. Examples of this are triposes developed by Hyland, Johnstone and Pitts in [16] and applicative topologies developed by Ziegler in [41]. However, Kripke realizability models may prove easier to construct and use in practice in some situations, the result in chapter 8 perhaps being an example of this. Another related body of work is Lipton's study in [19] of the connections between realizability and Beth models.

In most of the following chapters we will use "pure" realizability models where the poset P in the definition below is trivial. However, in chapter 8 we will make essential use of the order structure.

3.1 Definition

Suppose that we are given a relational language $\mathcal{L}$ with n_i-ary relation symbols R_i for $i = 1, \ldots, n$. Then we define a Kripke realizability model over $\mathcal{L}$ as follows.

Definition 3.1.1. A *Kripke realizability model* consists of a class order pca, $\mathcal{A}$, and a poset P, together with inhabited classes $\mathcal{M}_p$ indexed by P and classes $[\![R_i]\!]_p \subset \mathcal{A} \times \mathcal{M}_p^{n_i}$ satisfying the following conditions. $[\![R_i]\!]_p$ is downwards closed with respect to the ordering on $\mathcal{A}$ and if $p \leq q$, then $[\![R_i]\!]_p \subseteq [\![R_i]\!]_q$.

We call $\mathcal{M}_p$ the *domains* of the model.

We define relations $\Vdash_p$ between $\mathcal{A}$ and formulas with parameters over $\mathcal{M}_p$, as follows. We read $e \Vdash_p \phi$ as "e realizes ϕ at p."

$$\begin{aligned}
e \Vdash_p R_i(a_1, \ldots, a_{n_i}) \quad &\text{iff} \quad \langle e, a_1, \ldots, a_{n_i} \rangle \in [\![R_i]\!]_p \\
e \Vdash_p \phi \wedge \psi \quad &\text{iff} \quad (\exists e', e'') e \leq \mathbf{p} e' e'' \wedge e' \Vdash_p \phi \wedge e'' \Vdash_p \psi \\
e \Vdash_p \phi \vee \psi \quad &\text{iff} \quad (\exists e', e'') e \leq \mathbf{p} e' e'' \ \text{ and} \\
&\qquad (e' \leq \mathbf{0} \wedge e'' \Vdash_p \phi) \vee (e' \leq \mathbf{1} \wedge e'' \Vdash_p \psi) \\
e \Vdash_p \phi \to \psi \quad &\text{iff} \quad (\forall q \geq p)(\forall f \in \mathcal{A}) f \Vdash_q \phi \text{ implies } e.f \Vdash_q \psi \\
e \Vdash_p \neg\phi \quad &\text{iff} \quad (\forall q \geq p)(\forall f \in \mathcal{A}) f \not\Vdash_q \phi \\
e \Vdash_p (\forall x)\phi(x) \quad &\text{iff} \quad (\forall q \geq p)(\forall a \in \mathcal{M}_q) e \Vdash_q \phi(a) \\
e \Vdash_p (\exists x)\phi(x) \quad &\text{iff} \quad (\exists a \in \mathcal{M}_p) e \Vdash_p \phi(a)
\end{aligned}$$

We write $[\![\phi]\!]_p$ to mean the class $\{e \in \mathcal{A} \mid e \Vdash_p \phi\}$.

Note that so far this is only defined when ϕ is closed. If ϕ has free variables then we define it as follows. Let $x_1, \ldots, x_n$ be a list of the free variables in ϕ. We then define the *universal closure*, $\overline{\forall}\phi$ as

$$\overline{\forall}\phi := (\forall x_1, \ldots, x_n)\phi$$

We can now define $[\![\phi]\!]_p$ to be $[\![\overline{\forall}\phi]\!]_p$.

3.2 Soundness Proof

In this section we aim towards the following soundness theorem. We will show the following for any Kripke realizability model.

Theorem 3.2.1. *Suppose that ϕ is an axiom of intuitionistic predicate logic, then there is some $e \in \mathcal{A}$ such that for any $p \in P$, $e \Vdash_p \phi$.*

Suppose that $\frac{\phi_1,\ldots,\phi_n}{\psi}$ is an inference rule of intuitionistic logic, and for some $p \in P$, $e_i \Vdash_p \phi_i$ for $i = 1,\ldots,n$. Then there is some $f \in \mathcal{A}$ only depending on the e_i such that $f \Vdash_p \psi$.

We first prove a few useful lemmas.

The following two lemmas state that realizability is downwards closed with respect to the ordering on $\mathcal{A}$ and upwards closed with respect to P.

Lemma 3.2.2. *For every ϕ, and every p, $[\![\phi]\!]_p$ is downwards closed with respect to the ordering on $\mathcal{A}$.*

Proof. We check by induction on ϕ

This is clear for atomics, conjunction, disjunction, and existential and universal quantifiers by definition.

It remains to check $\to$.

Suppose that $e' \leq e$ and $e \Vdash_p \phi \to \psi$. Then suppose that for $q \geq p$, $f \Vdash_q \phi$. By the opca axioms $e'.f \leq e.f$. But we know that $e.f \Vdash_q \psi$, and so by induction this implies that $e'.f \Vdash_q \psi$. Hence $e' \Vdash_p \phi \to \psi$. □

Lemma 3.2.3. *Suppose that $e \Vdash_p \phi$ and $q \geq p$. Then $e \Vdash_q \phi$.*

Proof. This is again proved by induction on ϕ. This holds at implication and universal quantification by definition, and can easily be checked in the other cases. □

Lemma 3.2.4. *To show* $e \Vdash_p \phi_1 \to (\phi_2 \to (\ldots \to (\phi_n \to \psi)\ldots)$*, it is sufficient to show that for any* $e_1, \ldots, e_{n-1} \in \mathcal{A}$*,* $ee_1 \ldots e_{n-1} \downarrow$*, and for any* $q \geq p$ *and any* $e_1, \ldots, e_n \in \mathcal{A}$ *such that* $e_i \Vdash_q \phi_i$*, we have* $ee_1 \ldots e_n \Vdash_q \psi$*.*

Proof. We will show this by induction on n.

Suppose that the condition holds. Then we aim to show

$$e \Vdash_p \phi_1 \to (\phi_2 \to (\ldots \to (\phi_n \to \psi)\ldots)$$

Note that if we set $\psi' := \phi_n \to \psi$, then this is the same as showing

$$e \Vdash_p \phi_1 \to (\phi_2 \to (\ldots \to (\phi_{n-1} \to \psi')\ldots)$$

By induction, we can show this by checking that the condition holds for $\phi_1, \ldots, \phi_{n-1}, \psi'$. We do this now.

We easily can see that for any $e_1, \ldots, e_{n-2}$ in $\mathcal{A}$, $ee_1 \ldots e_{n-2} \downarrow$. Now let $q \geq p$ and let $e_1, \ldots, e_{n-1} \in \mathcal{A}$ be such that for $i \leq n-1$, $e_i \Vdash_q \phi_i$. We need to show that $ee_1 \ldots e_{n-1} \Vdash_q \psi'$, that is $ee_1 \ldots e_{n-1} \Vdash_q \phi_n \to \psi$. Let $q' \geq q$, and suppose that $e_n \Vdash_{q'} \phi_n$. Note that by lemma 3.2.3 we know that also for $i \leq n-1$, $e_i \Vdash_{q'} \phi_i$. In particular $q' \geq p$, so by our condition we can deduce that $ee_1 \ldots e_n \Vdash_{q'} \psi$. But we have now shown that $ee_1 \ldots e_{n-1} \Vdash_q \phi_n \to \psi$ as required so we can deduce the result. □

Lemma 3.2.5. *To show* $e \Vdash_p (\forall x_1, \ldots, x_n)\phi(x_1, \ldots, x_n)$*, it is sufficient to show that for any* $q \geq p$ *and for any* $a_1, \ldots, a_n \in \mathcal{M}_q$*,* $e \Vdash_q \phi(a_1, \ldots, a_n)$*.*

Proof. We again show this by induction on n.

Suppose that the condition holds. Then note that showing

$$e \Vdash_p (\forall x_1, \ldots, x_n)\phi(x_1, \ldots, x_n)$$

is the same as showing

$$e \Vdash_p (\forall x_1)(\forall x_2, \ldots, x_n)\phi(x_1, \ldots, x_n)$$

Let $q \geq p$ and let $a_1 \in \mathcal{M}_q$. We aim to show

$$e \Vdash_q (\forall x_2, \ldots, x_n)\phi(a_1, x_2, \ldots, x_n)$$

By induction it is sufficient to check that the condition holds. We now do this.

Let $q' \geq q$, and let $a_2, \ldots, a_n \in \mathcal{M}_{q'}$. By definition we have that $a_1 \in \mathcal{M}_{q'}$. Since $q' \geq p$, we deduce from our condition that $e \Vdash_{q'} \phi(a_1, \ldots, a_n)$. Hence we do get

$$e \Vdash_q (\forall x_2, \ldots, x_n)\phi(a_1, x_2, \ldots, x_n)$$

as required. □

Proof of theorem 3.2.1 The axioms of IPL are as follows:

1. $\phi \to (\psi \to \phi)$
2. $(\phi \to (\psi \to \chi)) \to ((\phi \to \psi) \to (\phi \to \chi))$
3. $\phi \to (\psi \to \phi \wedge \psi)$
4. $\phi \wedge \psi \to \phi$
5. $\phi \wedge \psi \to \psi$
6. $\phi \to \phi \vee \psi$
7. $\psi \to \phi \vee \psi$
8. $(\phi \vee \psi) \to ((\phi \to \chi) \to ((\psi \to \chi) \to \chi))$
9. $(\phi \to \psi) \to ((\phi \to \neg\psi) \to \neg\phi)$
10. $\phi \to (\neg\phi \to \psi)$
11. $(\forall x)\phi(x) \to \phi(y)$, where y is free for x in $\phi(x)$
12. $\phi(y) \to (\exists x)\phi(x)$, where y is free for x in $\phi(x)$

Note that ϕ may have free variables, so what we actually have to check is the universal closure of each axiom.

1 We claim

$$\mathbf{k} \Vdash_p \phi \to (\psi \to \phi)$$

By lemma 3.2.4, it is enough to show that for any $q \geq p$, whenever $e \Vdash_q \phi$ and $f \Vdash_q \psi$ we have $\mathbf{k}ef \Vdash_q \phi$

However, $\mathbf{k}ef \leq e$, so this is clear.

2 We claim that

$$\mathbf{s} \Vdash_p (\phi \to (\psi \to \chi)) \to ((\phi \to \psi) \to (\phi \to \chi))$$

By lemma 3.2.4, it is enough to show that for any $q \geq p$, whenever $e \Vdash_q \phi \to (\psi \to \chi)$ $f \Vdash_q \phi \to \psi$ and $g \Vdash_q \phi$ we have $\mathbf{s}efg \Vdash_q \chi$.

However, $\mathbf{s}efg \leq eg(fg)$, so one can easily check that this is the case. (We also have that by definition $\mathbf{s}ef\downarrow$ for all e and f.)

3 Suppose that $q \geq p$, $e \Vdash_q \phi$, and $f \Vdash_q \psi$. Then

$$\mathbf{p}ef \Vdash_q \phi \wedge \psi$$

Hence

$$\mathbf{p} \Vdash_p \phi \to (\psi \to \phi \wedge \psi)$$

4 - 8 These are similar to the preceding.

9 Suppose that $q \geq p$, $e \Vdash_q \phi \to \psi$ and $f \Vdash_q \phi \to \neg\psi$.

Suppose further that for some $q' \geq q$, $g \Vdash_{q'} \phi$. Then we would get

$$\begin{aligned} e.g &\Vdash_{q'} \psi \\ f.g &\Vdash_{q'} \neg\psi \end{aligned}$$

But this gives a contradiction, so there can't be any such g. So, for instance, $\mathbf{0} \Vdash_q \neg\phi$.

Hence we can find a realizer at p for

$$(\phi \to \psi) \to ((\phi \to \neg\psi) \to \neg\phi)$$

10 Suppose $q \geq p$, $e \Vdash_q \phi$ and $f \Vdash_q \neg\phi$. Then we immediately get a contradiction and in particular we could deduce

$$\mathbf{0} \Vdash_q \psi$$

11 Let $I := \mathbf{skk}$ be the identity. Then we claim

$$I \Vdash_p (\forall x)\phi(x) \to \phi(y)$$

As mentioned above, what we actually mean is the universal closure of this axiom. Without loss of generality we can assume the universal closure is (ignoring any additional parameters) the following:

$$I \Vdash_p (\forall y)((\forall x)\phi(x) \to \phi(y))$$

Expanding this out, this means that for $q \geq p$ and $b \in \mathcal{M}_q$,

$$I \Vdash_q (\forall x)\phi(x) \to \phi(b)$$

So suppose that $q' \geq q$ and $e \Vdash_{q'} (\forall x)\phi(x)$. Then in particular, $e \Vdash_{q'} \phi(b)$.

So we have shown that $I \Vdash_q (\forall x)\phi(x) \to \phi(b)$.

So, as required we can deduce

$$I \Vdash_p (\forall y)((\forall x)\phi(x) \to \phi(y))$$

12 We claim that

$$I \Vdash_p \phi(y) \to (\exists x)\phi(x)$$

More explicitly we need to show,

$$I \Vdash_p (\forall y)(\phi(y) \to (\exists x)\phi(x))$$

So what we need is that for $q \geq p$ and $b \in \mathcal{M}_q$,

$$I \Vdash_q \phi(b) \to (\exists x)\phi(x)$$

Let $b \in \mathcal{M}_q$ and for $q' \geq q$, $e \Vdash_{q'} \phi(b)$. Then, $e \Vdash_{q'} (\exists x)\phi(x)$. So we deduce that if $b \in \mathcal{M}_q$, then

$$I \Vdash_q \phi(b) \to (\exists x)\phi(x)$$

So we can deduce

$$I \Vdash_p \phi(y) \to (\exists x)\phi(x)$$

Inference Rules

The inference rules of IPL are

1. $\frac{\phi, \phi \to \psi}{\psi}$
2. $\frac{\psi \to \phi(x)}{\psi \to (\forall x)\phi(x)}$ where $x \notin FV(\psi)$
3. $\frac{\phi(x) \to \psi}{(\exists x)\phi(x) \to \psi}$ where $x \notin FV(\psi)$

1 (Modus Ponens) Note first that we can assume that

$$\begin{aligned} e &\Vdash_p (\forall x_1, \ldots, x_n)\phi(x_1, \ldots, x_n) \\ f &\Vdash_p (\forall x_1, \ldots, x_n)\phi(x_1, \ldots, x_n) \to \psi(x_1, \ldots, x_n) \end{aligned}$$

where the free variables for ϕ and ψ are amongst $x_1, \ldots, x_n$.

Then for any $q \geq p$ and $a_1, \ldots, a_n \in \mathcal{M}_q$,

$$\begin{aligned} e &\Vdash_q \phi(a_1, \ldots, a_n) \\ f &\Vdash_q \phi(a_1, \ldots, a_n) \to \psi(a_1, \ldots, a_n) \end{aligned}$$

and hence $e.f \Vdash_q \psi(a_1, \ldots, a_n)$. So we have shown

$$e.f \Vdash_p (\forall x_1, \ldots, x_n)\psi(x_1, \ldots, x_n)$$

2 We show that if $e \Vdash_p \psi \to \phi(x)$, then

$$e \Vdash_p \psi \to (\forall x)\phi(x)$$

So suppose that $e \Vdash_p \psi \to \phi(x)$. Then, more explicitly (ignoring any additional free variables) this is

$$e \Vdash_p (\forall x)(\psi \to \phi(x))$$

So, if $q \geq p$ and $a \in \mathcal{M}_q$, then

$$e \Vdash_q \psi \to \phi(a)$$

Now suppose that $q \geq p$ and $f \Vdash_q \psi$. We need to show that for any $q' \geq q$ and $a \in \mathcal{M}_{q'}$, $e.f \Vdash_{q'} \phi(a)$. But this is clear from the above, so we can deduce

$$e.f \Vdash_q (\forall x)\phi(x)$$

and so

$$e \Vdash_p \psi \to (\forall x)\phi(x)$$

3 We claim that if $e \Vdash_p \phi(x) \to \psi$, then $e \Vdash_p (\exists x)\phi(x) \to \psi$. First note as before that what we actually assume is

$$e \Vdash_p (\forall x)(\phi(x) \to \psi)$$

Now suppose that $q \geq p$ and $f \Vdash_q (\exists x)\phi(x)$. Then there is $a \in \mathcal{M}_q$ such that $f \Vdash_q \phi(a)$. But we know from the above that

$$e \Vdash_p \phi(a) \to \psi$$

And so,

$$e.f \Vdash_q \psi$$

So we can deduce

$$e \Vdash_p (\exists x)\phi(x) \to \psi$$

3.3 Recovering Realizability Models and Kripke Models

Both Kripke models and realizability models as can be recovered from the definition of Kripke realizability models. Kripke models and realizability models are both defined in [37] in volume I, chapter 2, section 5 and volume II chapter 4, section 4 respectively.

Definition 3.3.1. A *Kripke model* is a Kripke realizability model where the opca $\mathcal{A}$ is the trivial one element pca.

Proposition 3.3.2. *Let $\mathcal{M}_p$ for $p \in P$ be a Kripke model. Denote the single element of $\mathcal{A}$ as $*$ and write $p \Vdash \phi$ to mean $* \Vdash_p \phi$. Then we have the following equivalences.*

$$\begin{aligned}
p \Vdash R_i(a_1, \ldots, a_{n_i}) \quad & \textit{iff} \quad \langle *, a_1, \ldots, a_{n_i} \rangle \in [\![R_i]\!]_p \\
p \Vdash \phi \wedge \psi \quad & \textit{iff} \quad p \Vdash \phi \wedge p \Vdash \psi \\
p \Vdash \phi \vee \psi \quad & \textit{iff} \quad p \Vdash \phi \vee p \Vdash \psi \\
p \Vdash \phi \to \psi \quad & \textit{iff} \quad \forall q \geq p, q \Vdash \phi \textit{ implies } q \Vdash \psi \\
p \Vdash \neg\phi \quad & \textit{iff} \quad \forall q \geq p, q \not\Vdash \phi \\
p \Vdash (\forall x)\phi(x) \quad & \textit{iff} \quad \forall q \geq p, (\forall a \in \mathcal{M}_q) q \Vdash \phi(a) \\
p \Vdash (\exists x)\phi(x) \quad & \textit{iff} \quad (\exists a \in \mathcal{M}_p) p \Vdash \phi(a)
\end{aligned}$$

Proof. Note that in the one element pca we have

$$\mathbf{p} = \mathbf{p}_0 = \mathbf{p}_1 = \mathbf{0} = \mathbf{1} = *$$

and also

$$*.* = *$$

Hence the two definitions agree by induction on the formula ϕ. □

Definition 3.3.3. A *realizability model* is a Kripke realizability model where P is the poset with one element.

Proposition 3.3.4. *Let $\langle \mathcal{A}, \mathcal{M} \rangle$ be a realizability model. Denote the single element of P as $*$ and write $e \Vdash \phi$ for $e \Vdash_* \phi$. Then we have the following equivalences.*

$$\begin{array}{rcl}
e \Vdash R_i(a_1, \ldots, a_{n_i}) & \textit{iff} & \langle e, a_1, \ldots, a_{n_i} \rangle \in [\![R_i]\!]_* \\
e \Vdash \phi \wedge \psi & \textit{iff} & \exists e', e''\ e \leq \mathbf{p}e'e'' \wedge e' \Vdash \phi \wedge e'' \Vdash \psi \\
e \Vdash \phi \vee \psi & \textit{iff} & \exists e', e''\ e \leq \mathbf{p}e'e'' \\
 & & \qquad (e' \leq \mathbf{0} \wedge e'' \Vdash \phi) \vee (e' \leq \mathbf{1} \wedge e'' \Vdash \psi) \\
e \Vdash \phi \rightarrow \psi & \textit{iff} & \forall f \in \mathcal{A}, f \Vdash \phi \textit{ implies } e.f \Vdash \psi \\
e \Vdash \neg\phi & \textit{iff} & \forall f \in \mathcal{A}, f \not\Vdash \phi \\
e \Vdash (\forall x)\phi(x) & \textit{iff} & (\forall a \in \mathcal{M}_*) e \Vdash \phi(a) \\
e \Vdash (\exists x)\phi(x) & \textit{iff} & (\exists a \in \mathcal{M}_*) e \Vdash \phi(a)
\end{array}$$

Proof. This is again proved by induction on ϕ. □

Note that in fact this is a slight generalisation of the usual definition of realizability model, since it allows $\mathcal{A}$ to be an order pca rather than a pca.

Chapter 4

Realizability with Proper Classes

In this chapter we will see our first models of $\mathbf{CZF}$. These are broadly similar to earlier models in [24], [5] and [33] but adapted so that in place of a pca we have a class order pca. The models in this chapter are "pure" realizability in the sense that the poset P appearing in the definition of Kripke realizability models is trivial. We start by showing some examples of copcas that are proper classes. We will then show that for any such structure we get a model for all the axioms of $\mathbf{CZF}$ except for bounded separation. We then show that if $\mathcal{A}$ satisfies a condition that we call *uniformity* then bounded separation is also satisfied by the realizability models.

4.1 Uniform Class Order Pcas

Definition 4.1.1. Let $\mathcal{A}$ be a class order pca (copca). Say that $e \in \mathcal{A}$ *satisfies* $R \subseteq \mathcal{A} \times \mathcal{A}$ iff

$$\forall \langle f, g \rangle \in R \; e.f \downarrow \text{ and } e.f \leq g$$

We say that $\mathcal{A}$ is *uniform* if for every set $R \subseteq \mathcal{A} \times \mathcal{A}$, there is a set $X \subseteq \mathcal{A}$ such that

$$\{e \in \mathcal{A} \mid e \text{ satisfies } R\} = X^{\leq}$$

Proposition 4.1.2. *Suppose that $\mathcal{A}$ is a uniform copca and $S \subseteq \mathcal{A} \times \mathcal{P}\mathcal{A}$ is a set. Say that e* weakly satisfies *S if for any $\langle f, G \rangle \in S$, there is $g \in G$ such that $e.f \leq g$. Then there is a set $Y \subseteq \mathcal{A}$ such that*

$$\{e \in \mathcal{A} \mid e \textit{ weakly satisfies } S\} = Y^{\leq}$$

Proof. Let $B = \bigcup\{G \mid \langle f, G \rangle \in S\}$. Now let $C \subseteq \mathrm{mv}(S, B)$ be the set given by the fullness axiom. Let

$$C' = \{m \in C \mid (\forall x \in m)(\exists f, G, g)(x = \langle\langle f, G \rangle, g \rangle \wedge g \in G)\}$$

Suppose that $m \in \mathrm{mv}(S, B)$ is such that for all $\langle\langle f, G \rangle, g \rangle$ in m, g is in G. Then define $R_m := \{\langle f, g \rangle \mid \exists G, \langle\langle f, G \rangle, g \rangle \in m\}$.

Note that if e satisfies R_m for some $m \in C'$, then e must also weakly satisfy S, since for every $\langle f, G \rangle \in S$, there is $g \in G$ such that $\langle\langle f, G \rangle, g \rangle \in m$.

Conversely suppose that e weakly satisfies S. Then let $m = \{\langle\langle f, G \rangle, g \rangle \mid \langle f, G \rangle \in S, g \in G, \text{ and } e.f \leq g\}$. Since e weakly satisfies S, we must have that $m \in \mathrm{mv}(S, B)$ and furthermore that e satisfies R_m. Now let $m' \in C$ be such that $m' \subseteq m$. Note that we must have $m' \in C'$ and e satisfies $R_{m'}$.

By uniformity, for each $m \in C'$ we have X such that

$$\{e \in \mathcal{A} \mid e \text{ satisfies } R_m\} = X^{\leq}$$

But this means by the above and by strong collection and union we can find Y such that

$$\{e \in \mathcal{A} \mid e \text{ weakly satisfies } S\} = Y^{\leq}$$

□

4.2 Examples of Class Order pcas

Example 4.2.1. Any order pca is in particular a class order pca. In this case we automatically get uniformity, since for any $R \subseteq \mathcal{A} \times \mathcal{A}$, $\{e \mid \forall \langle f, g \rangle \in R, e.f \leq g\}$ is a set.

Example 4.2.2. Recall from chapter 2 the definition of term model obtained from $\mathrm{CL}(C)$ in example 2.5.13. Then we can easily adapt this definition to make C a proper class. Let $\mathcal{T}$ be the term model obtained by taking C to be the class of all sets.

For a set a, we will write the corresponding constant in $\mathrm{CL}(C)$ as $\mathbf{a}$.

We define an ordering on the constants by $\mathbf{a} \leq \mathbf{b}$ if $b \subseteq a$. This ordering is then extended to $\mathcal{T}$ by $t.q \leq t'.q'$ if and only if $t \leq t'$ and $q \leq q'$.

Checking that $\mathbf{s}$ and $\mathbf{k}$ have the required properties is the same as in 2.5.13.

We now show that this copca is uniform.

Define the support of t, $\mathrm{Supp}(t)$ as the set of a such that $\mathbf{a}$ appears in t.

Let $R \subseteq \mathcal{T} \times \mathcal{T}$ be a set. Now let

$$S = \bigcup_{\langle q, r \rangle \in R} \mathrm{Supp}(r)$$

Define the set, F of “finite unions” of S as

$$F = \bigcup_{n \in \omega} \{ \bigcup_{m < n} f(m) \mid f : n \to S \}$$

(Note that this set is a superset of S, by setting $n = 1$ and contains the empty set by setting $n = 0$).

We now define the set B of “relevant sets” as follows

$$B = \{ \bigcup_{\langle q, r \rangle \in R} f(\langle q, r \rangle) \mid f : R \to F \}$$

Now let $\mathcal{T}_0$ be the sub copca of $\mathcal{T}$ obtained by taking only those constants $\mathbf{b}$ such that $b \in B$.

We claim that if t satisfies R, then there is some t_0 in $\mathcal{T}_0$ such that $t \leq t_0$ and t_0 satisfies R.

We first define the (open) term t' of CL by replacing each occurrence of some $\mathbf{a}$ in t with distinct free variables $x_1, \ldots, x_n$. So we have that t' has free variables $x_1, \ldots, x_n$ each occurring exactly once and there are $a_1, \ldots, a_n$ such that we can recover t by substituting $t = t'[x_1, \ldots, x_n/\mathbf{a_1}, \ldots, \mathbf{a_n}]$.

Now for each i, we define $b_i \in B$ such that $b_i \subseteq a_i$ as follows. By the definition of B, what we require is some $f_i : R \to F$ such that $b_i = \bigcup_{\langle q,r\rangle \in R} f_i(\langle q, r\rangle)$. We define this f_i as follows

For each $\langle q, r\rangle \in R$, we know that $t.q \downarrow$, and hence as a term of combinatory logic $t.q$ must reduce to a normal form, $r' \leq r$. However, since substitutions have no effect on weak reduction, $t'.q$ must also reduce to a normal form, r'' and furthermore $r''[x_1, \ldots, x_n/a_1, \ldots, a_n] = r'$. By induction on terms we can show that x_i must occur finitely many times in r'' and each occurrence must correspond to a unique $\mathbf{c_{i,j}}$ in r such that $c_{i,j} \subseteq a_i$. We can now define $f_i(\langle q, r\rangle)$ as $\bigcup_j c_{i,j}$.

Since each $c_{i,j} \in S$, we know that $f_i(\langle q, r\rangle) \in F$, as required for f_i to be a function to F. Also, this clearly gives that for each j, $c_{i,j} \subseteq f_i(\langle q, r\rangle) \subseteq a_i$.

From the above we can see that $b_i = \bigcup_{\langle q,r\rangle \in R} f_i(\langle q, r\rangle) \subset a_i$ and so $\mathbf{a_i} \leq \mathbf{b_i}$. Hence if we define $t_0 = t'[b_1, \ldots, b_n/x_1, \ldots, x_n]$ then $t \leq t_0$. It remains to show that as claimed, t_0 satisfies R.

Therefore, let $\langle q, r\rangle \in R$. We aim to show that $t_0.q \leq r$. Let r' and r'' be the normal forms of $t.q$ and $t'.q$ as above. Note firstly, that we can apply exactly the same reduction to normal form to get a normal form r_0 of $t_0.q$. Let $\mathbf{a}$ be an occurrence of some atom in r_0. Then $\mathbf{a}$ either corresponds to some x_i in t' or it does not. (If we don't have excluded middle, we can show this by an inductive argument on the length of the reduction to normal form followed by induction on the definition of terms). If it does not, then it must correspond to an occurrence of $\mathbf{a}$ in r'. But since $r' \leq r$, we know that it must correspond to some $\mathbf{a}'$ in r with $\mathbf{a} \leq \mathbf{a}'$. On the other hand, if $\mathbf{a}$ corresponds to some x_i

in t', then we know that $a = b_i$, and that it must also correspond to some $\mathbf{c_{i,j}}$ in r. But then $c_{i,j} \subseteq f_i(\langle q, r\rangle) \subseteq b_i$, and so $\mathbf{a} = \mathbf{b_i} \leq \mathbf{c_{i,j}}$.

We can therefore deduce that $r_0 \leq r$ and hence that t_0 satisfies R.

Hence if we define $X = \{t \in \mathcal{T}_0 \mid \forall \langle r, s\rangle \in R, t.r \downarrow$ and $t.r \leq s\}$, then the class of terms satisfying R is precisely $X^{\leq}$ as required.

Proposition 4.2.3. *Let $\mathcal{A}$ be a uniform copca and $\mathcal{A}' \subseteq \mathcal{A}$ a sub copca of $\mathcal{A}$ that is upwards closed. Suppose further that either full separation holds or $\mathcal{A}'$ is definable by a bounded formula. Then $\mathcal{A}'$ is also uniform.*

Proof. Let $R \subseteq \mathcal{A}' \times \mathcal{A}'$. Then in particular $R \subseteq \mathcal{A} \times \mathcal{A}$. Let X be such that

$$\{e \in \mathcal{A} \mid e \text{ satisfies } R\} = X^{\leq}$$

Let

$$X' = X \cap \mathcal{A}'$$

Suppose $e \in \mathcal{A}'$ satisfies R. Then there is $e' \in X$ such that $e \leq e'$. However, since $\mathcal{A}'$ is upwards closed, we also have that $e' \in \mathcal{A}'$ and so $e' \in X'$.

Hence $\mathcal{A}'$ is uniform. □

Example 4.2.4. In [32], Rathjen constructs a class pca based on E-recursion (as appears in [28]). He does this by defining $\trianglerighteq$ by an inductive definition according to inference steps below. Formally, the class being defined is the class of triples $\langle e, x, y\rangle$ where $\{e\}(x) = y$. In the below, $\{e\}(x_1, \ldots, x_n) = y$ for $n > 1$ means that $\{e\}(x_1) \trianglerighteq \langle e, x_1\rangle$, for $1 < i < n$,

$$\{\langle e, x_1, \ldots, x_{i-1}\rangle\}(x_i) \trianglerighteq \langle e, x_1, \ldots, x_i\rangle$$

and that

$$\{\langle e, x_1, \ldots, x_{n-1}\rangle\}(x_n) \trianglerighteq y$$

$\mathbf{k}$, $\mathbf{s}$, $\mathbf{p}$, $\mathbf{p}_0$, $\mathbf{p}_1$, $\mathbf{s}_N$, $\mathbf{p}_N$, $\mathbf{d}_N$, $\mathbf{0}$, $\underline{\omega}$, π, σ, $\mathbf{pl}$, $\mathbf{i}$, $\mathbf{fa}$ and $\mathbf{ab}$ are constant natural numbers.

$$
\begin{aligned}
\{\mathbf{k}\}(x,y) &\trianglerighteq x\\
\{\mathbf{s}\}(x,y,z) &\trianglerighteq \{\{x\}z\}(\{y\}(z))\\
\{\mathbf{p}\}(x,y) &\trianglerighteq \langle x,y\rangle\\
\{\mathbf{p}_0\}(x) &\trianglerighteq (x)_0\\
\{\mathbf{p}_1\}(x) &\trianglerighteq (x)_1\\
\{\mathbf{s}_N\}(n) &\trianglerighteq n+1 \text{ if } n\in\mathbb{N}\\
\{\mathbf{p}_N\}(0) &\trianglerighteq 0\\
\{\mathbf{p}_N\}(n+1) &\trianglerighteq n \text{ if } n\in\mathbb{N}\\
\{\mathbf{d}_N\}(n,m,x,y) &\trianglerighteq x \text{ if } n,m\in\mathbb{N} \text{ and } n=m\\
\{\mathbf{d}_N\}(n,m,x,y) &\trianglerighteq y \text{ if } n,m\in\mathbb{N} \text{ and } n\neq m\\
\{\mathbf{0}\}(x) &\trianglerighteq 0\\
\{\underline{\omega}\}(x) &\trianglerighteq \omega\\
\{\pi\}(x,g) &\trianglerighteq \prod_{z\in x} g(z) \text{ if } g \text{ is a function with } \operatorname{dom}(g)=x\\
\{\sigma\}(x,g) &\trianglerighteq \sum_{z\in x} g(z) \text{ if } g \text{ is a function with } \operatorname{dom}(g)=x\\
\{\mathbf{pl}\}(x,y) &\trianglerighteq x+y\\
\{\mathbf{i}\}(x,y,z) &\trianglerighteq \{z\in\{0\}\mid y=z\wedge y,z\in x\}\\
\{\mathbf{fa}\}(g,x) &\trianglerighteq g(x) \text{ if } g \text{ is a function and } x\in\operatorname{dom}(g)\\
\{\mathbf{ab}\}(e,a) &\trianglerighteq h \text{ where } h \text{ is the function given by}\\
&\qquad\qquad \operatorname{dom}(h)=a \text{ and } \{e\}(x)\trianglerighteq h(x)
\end{aligned}
$$

This construction can be performed within $\mathbf{CZF}$ and gives a class pca on the universe of sets V with application given by

$$
x.y := \begin{cases} z & \text{if there exists } z \text{ such that } \{x\}(y)\trianglerighteq z\\ \text{undefined} & \text{otherwise}\end{cases}
$$

We add to this definition the constants **U** and **I** and add the following two inference steps

$$\{\mathbf{U}\}(x) \trianglerighteq \bigcup x$$
$$\{\mathbf{I}\}(x) \trianglerighteq \bigcap x$$

Call this class pca $\mathbb{E}$

$\mathbb{E}$ provides a source of non trivial examples of class order pcas that are not uniform, as demonstrated by the following proposition.

We work over **ZF**.

Proposition 4.2.5. *Suppose that $\mathbb{E}$ has been expanded to a class order pca $\mathbb{E}'$ by adding a recursive ordering (ie one whose graph is representable in $\mathbb{E}$) such that $1 \not\leq 0$. Then $\mathbb{E}'$ is not uniform.*

Proof. Let $R := \{\langle 0, 0\rangle\}$. Suppose that X is a set such that e satisfies R if and only if $e \in X^{\leq}$. Then, since $\leq$ is recursive, we can construct d such that

$$de = \bigcup_{f \in X} \{z \in \{0\} \mid e \leq f\}$$

Then using excluded middle we get that

$$d.e = \begin{cases} 0 & e \text{ does not satisfy } R \\ 1 & e \text{ does satisfy } R \end{cases}$$

However, we can now use the fixed point theorem to construct an f such that

$$f.0 = \begin{cases} 0 & f \text{ does not satisfy } R \\ 1 & f \text{ does satisfy } R \end{cases}$$

This clearly gives a contradiction. □

Note that $\mathbb{E}$ with the discrete ordering provides one such example of a suitable $\mathbb{E}'$.

4.3 Realizability over Class Order Pcas

Recall from chapter 3 the definition of realizability model (definition 3.3.3).

Given a class order pca, $\mathcal{A}$, define the class $V(\mathcal{A})$ by the following inductive definition. Let Φ be the class of pairs $\langle X, a\rangle$ where every element of a is of the form $\langle e, b\rangle$ where $e \in \mathcal{A}$ and $b \in X$. Then let $V(\mathcal{A})$ be the smallest Φ-closed class.

Define

$$\begin{aligned}
e \Vdash a \in b \quad &\text{iff} \quad (\exists e', e'', c) e \leq \mathbf{p} e' e'' \wedge \langle e', c\rangle \in b \wedge e'' \Vdash a = c \\
e \Vdash a = b \quad &\text{iff} \quad (\exists e', e'') e \leq \mathbf{p} e' e'' \wedge \\
&\qquad\qquad \forall \langle f, c\rangle \in a\ e' f \Vdash c \in b \wedge \forall \langle f, c\rangle \in b\ e'' f \Vdash c \in a \\
e \Vdash (\forall x \in a) \phi(x) \quad &\text{iff} \quad (\forall \langle f, b\rangle \in a) e.f \Vdash \phi(b) \\
e \Vdash (\exists x \in a) \phi(x) \quad &\text{iff} \quad (\exists e', e'') e \leq \mathbf{p} e' e'' \wedge (\exists \langle e', b\rangle \in a) e'' \Vdash \phi(b)
\end{aligned}$$

Since we are dealing with classes that could be proper classes, we will be a bit careful about how this definition works formally, in particular the first two lines.

Let Ψ be the following inductive definition. The elements of Ψ are $X / \langle s, e, a, b\rangle$ where one of the following two conditions holds:

1. $s = 0$ and there are e', e'' such that $e \leq \mathbf{p} e' e''$, and $\langle e', c\rangle \in b$ with $\langle 1, e'', a, c\rangle \in X$
2. $s = 1$, and there are e', e'' such that $e \leq \mathbf{p} e' e''$ and every element of a is of the form $\langle f, c\rangle$ where $\langle 0, e' f, c, b\rangle \in X$ and every element of b is of the form $\langle f, c\rangle$ where $\langle 0, e'' f, c, a\rangle \in a$

Then $e \Vdash a \in b$ means that $\langle 0, e, a, b\rangle$ is in the smallest Ψ-closed class. $e \Vdash a = b$ means that $\langle 1, e, a, b\rangle$ is in the smallest Ψ-closed class.

Formally, we deal with the last two lines by adding a predicate for each formula of the form $(\forall x \in a) \phi(x)$ and $(\exists x \in a) \phi(x)$ and defining it as given. We will show later that they relate in the correct way to unbounded quantifiers.

4.3.1 Axioms of Equality

In the following, we will need to work inductively on the definition of $V(\mathcal{A})$, so it will be useful to have a notion of rank that we can induct on.

Definition 4.3.1. The *rank*, $\mathrm{rank}(a)$ of $a \in V(\mathcal{A})$ is defined inductively as follows:

$$\mathrm{rank}(a) = \bigcup_{\langle e,b\rangle \in a} (\mathrm{rank}(b) + 1)$$

Lemma 4.3.2. *Suppose that* $a, b \in V(\mathcal{A})$*. If* $V(\mathcal{A}) \models a = b$*, then* $\mathrm{rank}(a) = \mathrm{rank}(b)$.

Proof. We show by induction that for any α, for any a, b, if $V(\mathcal{A}) \models a = b$ and $\mathrm{rank}(a) = \alpha$, then $\mathrm{rank}(b) = \alpha$.

Let $\langle e, c\rangle \in a$. Then there is $\langle e', c'\rangle \in b$ such that $V(\mathcal{A}) \models c = c'$. Then $\mathrm{rank}(c) \in \alpha$ and so we may assume by induction that $\mathrm{rank}(c) = \mathrm{rank}(c')$, and so

$$\begin{aligned} \mathrm{rank}(c) + 1 &= \mathrm{rank}(c') + 1 \\ &\leq \mathrm{rank}(b) \end{aligned}$$

Hence $\mathrm{rank}(a) \subseteq \mathrm{rank}(b)$. If $\langle e, c\rangle \in b$, then there is some $\langle e', c'\rangle \in a$ such that $V(\mathcal{A}) \models c = c'$. Then we must also have $V(\mathcal{A}) \models c' = c$ and we know that $\mathrm{rank}(c') \in \alpha$. So $\mathrm{rank}(c) = \mathrm{rank}(c')$. By the same reasoning as above $\mathrm{rank}(b) \subseteq \mathrm{rank}(a)$ and so $\mathrm{rank}(a) = \mathrm{rank}(b)$. □

Proposition 4.3.3. *Let $\mathcal{A}$ be a copca. Then $V(\mathcal{A})$ satisfies soundness for the axioms of equality.*

Proof. We first check the axioms of identity. We follow the same proof that appears in [24] and in [33]. We first check the case for atomic formula. Explicitly we find $\mathbf{i}_r, \mathbf{i}_s, \mathbf{i}_t, \mathbf{i}_0, \mathbf{i}_1$.

1. $\mathbf{i}_r \Vdash a = a$

2. $\mathbf{i}_s \Vdash a = b \to b = a$

3. $\mathbf{i}_t \Vdash a = b \wedge b = c \to a = c$

4. $\mathbf{i}_0 \Vdash a = b \wedge a \in c \to b \in c$

5. $\mathbf{i}_1 \Vdash a = b \wedge c \in a \to c \in b$

Let y be as in proposition 2.3.4. Then we define the term $\mathbf{i}_r$ as

$$\mathbf{i}_r := y((\lambda z).\mathbf{p}((\lambda x).\mathbf{p}xz)((\lambda x).\mathbf{p}xz))$$

Then

$$\mathbf{i}_r \preceq \mathbf{p}((\lambda x).\mathbf{p}x\mathbf{i}_r)((\lambda x).\mathbf{p}x\mathbf{i}_r)$$

In particular we know that $((\lambda x).\mathbf{p}x\mathbf{i}_r)\downarrow$, so we can deduce that $\mathbf{i}_r\downarrow$.

We now show by induction that for all $a \in V(\mathcal{A})$

$$\mathbf{i}_r \Vdash a = a$$

Let $\langle f, b\rangle \in a$. Then by induction we may assume that $\mathbf{i}_r \Vdash b = b$.

Hence

$$\mathbf{p}f\mathbf{i}_r \Vdash b \in a$$

But

$$((\lambda x).\mathbf{p}x\mathbf{i}_r)f \leq \mathbf{p}f\mathbf{i}_r$$

So we have that $\mathbf{i}_r \Vdash a = a$ as required.

Take

$$\mathbf{i}_s := (\lambda x).\mathbf{p}(\mathbf{p}_1 x)(\mathbf{p}_0 x)$$

Suppose that $e \Vdash a = b$. Then there is e', e'' such that $e \leq \mathbf{p}e'e''$ and for all $\langle f, c\rangle \in a$, $e'.f \Vdash c \in b$ and for all $\langle f, c\rangle \in b$, $e''.f \Vdash c \in a$. Note therefore that $\mathbf{p}e''e' \Vdash b = a$.

Then $\mathbf{i}_s.e \leq \mathbf{p}(\mathbf{p}_1 e)(\mathbf{p}_0 e)$. But also $\mathbf{p}_1 e \leq e''$ and $\mathbf{p}_0 e \leq e'$ and so $\mathbf{i}_s.e \leq \mathbf{p}e''e'$. Hence $\mathbf{i}_s.e \Vdash b = a$ and so $\mathbf{i}_s \Vdash a = b \to b = a$

To construct $\mathbf{i}_t$, we follow [24] and first consider the following four terms over $\mathcal{A}$.

$$\begin{aligned}
t_0(x,y,z) &:= ((y)_0((x)_0 z)_0)_0 \\
s_0(w,x,y,z) &:= w((x)_0 z)_1((y)_0((x)_0 z)_0)_1 \\
t_1(x,y,z) &:= ((x)_1((y)_1 z)_0)_0 \\
s_1(w,x,y,z) &:= w((y)_1 z)_1((x)_1((y)_1 z)_0)_1
\end{aligned}$$

We then construct $\mathbf{i}_t$ using the fixed point theorem so that for any e, f, $\mathbf{i}_t ef \downarrow$, and for any g,

$$\begin{aligned}
(\mathbf{i}_t ef)_0 g &\leq \mathbf{p}t_0(e,f,g)s_0(\mathbf{i}_t, e, f, g) \\
(\mathbf{i}_t ef)_1 g &\leq \mathbf{p}t_1(e,f,g)s_1(\mathbf{i}_t, e, f, g)
\end{aligned}$$

We will show by induction on b that for any $a, b, c \in V(\mathcal{A})$, and any e, f, if $e \Vdash a = b$ and $f \Vdash b = c$, then $\mathbf{i}_t ef \Vdash a = c$.

So suppose that a, b, c and e, f are as above.

Suppose further that $\langle g, d\rangle \in a$. Then we know that there must be an element of b of the form $\langle h_0, d'\rangle$ and an element of c of the form $\langle k_0, d''\rangle$ where

$$(e)_0 g \leq \mathbf{p}h_0 h_1$$
$$(f)_0 h_0 \leq \mathbf{p}k_0 k_1$$

and

$$h_1 \Vdash d = d'$$
$$k_1 \Vdash d' = d''$$

Note that d' is of strictly lower rank than b so by induction we may assume that $\mathbf{i}_t h_1 k_1 \Vdash d = d''$ and hence that

$$\mathbf{i}_t((e)_0 g)_1((f)_0((e)_0 g)_0)_1 \Vdash d = d''$$

and substituting s_0 and t_0 we get

$$\mathbf{p}t_0(e,f,g)s_0(\mathbf{i}_t,e,f,g) \Vdash d \in c$$

Similarly we can show that for any $\langle g,d\rangle \in c$,

$$\mathbf{p}t_1(e,f,g)s_1(\mathbf{i}_t,e,f,g) \Vdash d \in c$$

Hence we get

$$\mathbf{i}_t ef \Vdash a = c$$

as required.

One can easily construct $\mathbf{i}_0$ and $\mathbf{i}_1$ from $\mathbf{i}_t$.

The $\mathbf{i}_\phi$ are constructed by induction on the construction of ϕ. We will explicitly show how to do this for unbounded universal quantifiers and implication since these contain the main ideas.

We first show how to construct $\mathbf{i}_{\phi\to\psi}$.

Suppose that $a,b,c \in V(\mathcal{A})$, $e \Vdash a = b$ and $f \Vdash \phi(a,c) \to \psi(a,c)$. Suppose further that

$$g \Vdash \phi(b,c)$$

Then

$$\mathbf{i}_\phi(\mathbf{i}_s e)g \Vdash \phi(a,c)$$

and so

$$f(\mathbf{i}_\phi(\mathbf{i}_s e)g) \Vdash \psi(a,c)$$

and finally

$$\mathbf{i}_\psi e(f(\mathbf{i}_\phi(\mathbf{i}_s e)g)) \Vdash \psi(b,c)$$

Hence we can take $\mathbf{i}_{\phi\to\psi}$ to be

$$\mathbf{i}_{\phi\to\psi} := (\lambda x,y,z).\mathbf{i}_\psi x(y(\mathbf{i}_\phi(\mathbf{i}_s x)z))$$

For unbounded universal quantifiers, we show that we can take $\mathbf{i}_{(\forall z)\phi(x,z)} := \mathbf{i}_{\phi(x,z)}$. Suppose that

$$\mathbf{i}_{\phi(x,z)} \Vdash (\forall z)(x = y \to (\phi(x,z) \to \phi(y,z)))$$

and suppose that for $a, b \in V(\mathcal{A})$, $e \Vdash a = b$ and

$$f \Vdash (\forall z)\phi(a,z)$$

Then for all $c \in V(\mathcal{A})$,

$$f \Vdash \phi(a,c)$$

and so

$$\mathbf{i}_{\phi(x,z)}ef \Vdash \phi(b,c)$$

Hence

$$\mathbf{i}_{\phi(x,z)}ef \Vdash (\forall z)\phi(b,z)$$

as required.

□

4.3.2 Bounded Quantifiers

Proposition 4.3.4. *Bounded quantifiers behave correctly. That is, for each formula, ϕ we can find realizers for*

1. $(\forall x \in a)\phi(x) \to (\forall x)(x \in a \to \phi(x))$

2. $(\forall x)(x \in a \to \phi(x)) \to (\forall x \in a)\phi(x)$

3. $(\exists x \in a)\phi \to (\exists x)(x \in a \land \phi(x))$

4. $(\exists x)(x \in a \land \phi(x)) \to (\exists x \in a)\phi(x)$

1 Suppose $e \Vdash (\forall x \in a)\phi(x)$. We want to find a realizer for

$$(\forall x)(x \in a) \to \phi(x)$$

Hence let $b \in V(\mathcal{A})$ and let f be such that

$$f \Vdash b \in a$$

Then we know that there is f_0, f_1 such that $f \leq \mathbf{p} f_0 f_1$ and $\langle f_0, c\rangle \in a$ with that

$$f_1 \Vdash b = c$$

Applying e above, and noting that $(f)_0 \leq f_0$, we get

$$e(f)_0 \Vdash \phi(c)$$

Applying $\mathbf{i}_\phi$ from the previous proposition and noting that $(f)_1 \leq f_1$, we get

$$\mathbf{i}_\phi (f)_1 (e(f)_0) \Vdash \phi(b)$$

Hence

$$(\lambda y).(\mathbf{i}_\phi (y)_1 (e(y)_0)) \Vdash (\forall x)(x \in a \to \phi(x))$$

and so

$$(\lambda z).(\lambda y).(\mathbf{i}_\phi (y)_1 (z(y)_0)) \Vdash (\forall x \in a)\phi(x) \to (\forall x)(x \in a \to \phi(x))$$

2 Suppose now that

$$e \Vdash (\forall x)(x \in a \to \phi(x))$$

Now for every $\langle f, b\rangle \in a$, we know that

$$\mathbf{p} f \mathbf{i}_r \Vdash b \in a$$

and so

$$e(\mathbf{p} f \mathbf{i}_r) \Vdash \phi(b)$$

Hence

$$(\lambda y).(e(\mathbf{p} y \mathbf{i}_r)) \Vdash (\forall x \in a)\phi(x)$$

So we get

$$(\lambda z).(\lambda y).(z(\mathbf{p} y \mathbf{i}_r)) \Vdash (\forall x)(x \in a \to \phi(x) \to (\forall x \in a)\phi(x)$$

3 Suppose that

$$e \Vdash (\exists x \in a)\phi(x)$$

Then by definition we know that there are e_0, e_1 such that $e \leq \mathbf{p}e_0e_1$ and $\langle e_0, b\rangle \in a$ with

$$e_1 \Vdash \phi(b)$$

In particular, we know that $b \in V(\mathcal{A})$ and so

$$\mathbf{p}((e)_0\mathbf{i}_r)(e)_1 \Vdash (\exists x)(x \in a \wedge \phi(x))$$

4 Suppose that

$$e \Vdash (\exists x)(x \in a \wedge \phi(x))$$

Then there is some $b \in V(\mathcal{A})$ such that

$$\begin{aligned} (e)_0 &\Vdash b \in a \\ (e)_1 &\Vdash \phi(b) \end{aligned}$$

Hence there is some f_0, f_1 with $(e)_0 \leq \mathbf{p}f_0f_1$ and $\langle f_0, c\rangle \in a$ such that

$$f_1 \Vdash b = c$$

Since $((e)_0)_0 \leq f_0$ and $((e)_0)_1 \leq f_1$, we deduce

$$\mathbf{p}((e)_0)_0(\mathbf{i}_\phi((e)_0)_1(e)_1) \Vdash (\exists x \in a)\phi(x)$$

□

Proposition 4.3.5. *Suppose that $\mathcal{A}$ is uniform. Then for any $a, b \in V(\mathcal{A})$, $[\![a \in b]\!]$ and $[\![a = b]\!]$ are both generated as the downward closure of sets.*

Proof. Suppose first that ϕ is $a \in b$. Then by collection and union and induction, we may find a family P_c such that for each $\langle f, c\rangle \in b$, $[\![a = c]\!] = P_c^{\leq}$. Let $P = \{\mathbf{p}fe \mid \langle f, c\rangle \in b, e \in P_c\}$. Then one may check that $[\![a \in b]\!] = P^{\leq}$.

Now suppose that ϕ is $a = b$. Then, we can construct by collection and union a family P_c such that for every $\langle f, c\rangle \in a$, $[\![c \in b]\!] = P_c^{\leq}$. Let

$$R = \{\langle f, P_c\rangle \mid \langle f, c\rangle \in a\}$$

Since $\mathcal{A}$ is uniform, we can apply proposition 4.1.2 and find Q_0 such that $Q_0^{\leq}$ is precisely those elements weakly satisfying R.

However, one can check that this implies

$$e \in Q_0^{\leq} \text{ iff } (\forall \langle f, c\rangle \in a)(ef) \Vdash c \in b$$

One can similarly construct a Q_1. But then let

$$Q = \{\mathbf{p}q_0q_1 \mid q_0 \in Q_0, q_1 \in Q_1\}$$

But then we can easily see that

$$[\![a = b]\!] = Q^{\leq}$$

□

Theorem 4.3.6. *Let $\mathcal{A}$ be a copca. Then $V(\mathcal{A})$ satisfies soundness for all the axioms of* **CZF** *except for separation.*

The proof essentially follows that in [33].

Extensionality Let

$$e = \lambda y.\mathbf{p}(\lambda x.\mathbf{p}_0 y(\mathbf{p}x\mathbf{i_r}))(\lambda x.\mathbf{p}_1 y(\mathbf{p}x\mathbf{i_r}))$$

One can check that as in [33], this realizes the axiom of extensionality.

Strong Infinity Let $\underline{n}$ for $n \in \omega$ be numerals satisfying the conditions in theorem 2.3.5.

Define $\overline{\omega}$ as follows

$$\begin{aligned} \overline{n} &:= \{\langle \underline{m}, \overline{m}\rangle \mid m < n\} \\ \overline{\omega} &:= \{\langle \underline{n}, \overline{n} \mid n \in \omega\} \end{aligned}$$

We follow [33] in writing $\bot_v$ for the formula $(\forall x \in v)\bot$, and writing $SC(x, y)$ for $y = x \cup \{x\}$ (expressed as a bounded formula).

Note that strong infinity amounts to finding realizers for the following two sentences:

$$(\forall v \in \overline{\omega})(\bot_v \vee (\exists u \in \overline{\omega})SC(u, y))$$

$$(\forall v)((\bot_v \vee (\exists u \in \bar{\omega})SC(u, v)) \to v \in \bar{\omega})$$

The first sentence follows from the fact that the numerals $\underline{n}$ are defined so that there is some term d such that

$$d\underline{n} = \begin{cases} \mathbf{p}\underline{0}\underline{0} & \text{if } n = 0 \\ \mathbf{p}\underline{1}\underline{n-1} & \text{if } n > 0 \end{cases}$$

For the second sentence, since we can clearly find a realizer to show that the empty set is in $\bar{\omega}$, this is reduced to finding a realizer for

$$(\forall v)(\exists u \in \bar{\omega})SC(u, v) \to v \in \bar{\omega})$$

Hence we assume that there is $a \in V(\mathcal{A})$ with $e \Vdash (\exists u \in \bar{\omega})SC(u, a)$. So there must be some n such that $(e)_0 = \underline{n}$ and $(e)_1 \Vdash SC(\overline{n}, a)$.

One can clearly find a realizer for $SC(\overline{n}, \overline{n+1})$ and hence a realizer, using the soundness of extensionality (once we have checked this) for $SC(u, v) \wedge SC(u, v') \to v = v'$. We can use these to construct a realizer for $a \in \overline{\omega}$, as required.

Union Given $a \in V(\mathcal{A})$, define

$$\mathrm{Un}(a) := \{\langle \mathbf{p}ef, c\rangle \mid \exists\langle e, b\rangle \in a, \langle f, c\rangle \in b\}$$

Then

$$(\lambda x).(\lambda y).\mathbf{p}(\mathbf{p}xy)\mathbf{i}_r \Vdash (\forall x \in a)(\forall y \in x) y \in \mathrm{Un}(a)$$

and

$$(\lambda x).\mathbf{p}(x)_0(\mathbf{p}(x)_1\mathbf{i}_r) \Vdash (\forall x \in \mathrm{Un}(a))(\exists y \in a)(x \in y)$$

and so we have a realizer for the union axiom.

Pair Set Given $a, b \in V(\mathcal{A})$, define

$$\mathrm{Pair}(a, b) := \{\langle \mathbf{0}, a\rangle, \langle \mathbf{1}, b\rangle\}$$

Then by the definition of realizability of membership and disjunction, the realizers of $c = a \vee c = b$ are precisely the realizers of $c \in \mathrm{Pair}(a, b)$.

Strong Collection Suppose that

$$e \Vdash (\forall x \in a)(\exists y)\phi(x, y)$$

Then we know that for each $\langle f, b\rangle \in a$, there is some c such that $e.f \Vdash \phi(b, c)$. Using strong collection in the background universe, we can therefore find a C such that for every $\langle f, b\rangle$ in a there is $\langle f, c\rangle \in C$ such that $e.f \Vdash \phi(b, c)$ and such that for every $c \in C$, there is $f \in \mathcal{A}, b$ and c' such that $c = \langle f, c'\rangle$, $\langle f, b\rangle \in a$ and $e.f \Vdash \phi(b, c')$. In particular, C must be an element of $V(\mathcal{A})$. Now note that

$$(\lambda x).\mathbf{p}x(e.x) \Vdash (\forall x \in a)(\exists y \in C)\phi(x, y)$$

and also

$$(\lambda x).\mathbf{p}x(e.x) \Vdash (\forall y \in C)(\exists x \in a)\phi(x, y)$$

and so we can find a realizer for strong collection.

Subset Collection Fix $A, B \in V(\mathcal{A})$. Showing the soundness of subset collection amounts to finding $C \in V(\mathcal{A})$ and a realizer e for

$$\begin{aligned} e \Vdash (\forall u)((\forall x \in A)(\exists y \in B)\phi(x,y,u) \rightarrow \\ (\exists z \in C)((\forall x \in A)(\exists y \in z)\phi(x,y,u) \wedge (\forall y \in z)(\exists x \in A)\phi(x,y,u))) \end{aligned}$$

(and also the realizer should not depend on A or B)

We will show this by applying subset collection in the background universe. To this end, note firstly that we can construct $\tilde{B}$ by strong collection such that

$$\tilde{B} = \{\langle g, b\rangle \mid (\exists h)\langle h, b\rangle \in B, (\exists a)\langle g, a\rangle \in A\}$$

Now suppose that f, u are such that $f \in \mathcal{A}$, $u \in V(\mathcal{A})$, and

$$f \Vdash (\forall x \in A)(\exists y \in B)\phi(x,y,u)$$

Then in particular we know that for every $\langle g, a\rangle \in A$, there are $h_0, h_1 \in \mathcal{A}$ and $b \in V(\mathcal{A})$ such that $fg \leq \mathbf{p}h_0h_1$, $\langle h_0, b\rangle \in B$ and $h_1 \Vdash \phi(a,b,u)$. Note that we also have that $\langle g, b\rangle \in \tilde{B}$, and that since

$$\begin{aligned} \mathbf{p}_1(fg) &\leq \mathbf{p}_1(\mathbf{p}h_0h_1) \\ &\leq h_1 \end{aligned}$$

we can deduce that

$$(fg)_1 \Vdash \phi(a,b,u)$$

Hence we can apply subset collection in the background universe to find a C' such that whenever the situation above occurs, there is some $c \in C'$ such that for every $\langle g, a\rangle \in A$, there is b such that

1. $\langle k, b\rangle \in B$ for some k
2. $(fg)_1 \Vdash \phi(a,b,u)$

3. $\langle g, b\rangle \in c$

Furthermore, we know that *every* element of c is the form $\langle g, b\rangle$ such that the above conditions hold. Deduce in particular that $c \in V(\mathcal{A})$.

However, we can now deduce that

$$(\lambda x).\mathbf{p}x(fx)_1 \Vdash (\forall x \in A)(\exists y \in c)\phi(x, y, u)$$

and

$$(\lambda x).\mathbf{p}x(fx)_1 \Vdash (\forall y \in c)(\exists x \in A)\phi(x, y, u)$$

Finally, take

$$C := \{\langle \underline{0}, (c \cap \tilde{B})\rangle \mid c \in C'\}$$

Then we can see that $C \in V(\mathcal{A})$ and by the above reasoning, C is as required to show the soundness of subset collection, if we take as realizer

$$e := (\lambda x).\mathbf{p}((\lambda y).y(xy)_1)((\lambda y).y(xy)_1)$$

$\in$-induction Suppose that

$$e \Vdash (\forall y)((\forall x \in y)\phi(x) \to \phi(y))$$

Let $e' = (\lambda x, y).e.x$ and let z be the fixed point element from proposition 2.3.4 and define $f := ze'$ so we have for all g

$$f.g \preceq e'.f.g$$

We will show by induction that for all $g \in \mathcal{A}$, $f.g\downarrow$ and for all $a \in V(\mathcal{A})$, $fg \Vdash \phi(a)$.

Let $a \in V(\mathcal{A})$. By induction we can assume that for all $\langle g, b\rangle \in a$, we have

$$fg \Vdash \phi(b)$$

Therefore,

$$f \Vdash (\forall x \in a)\phi(x)$$

and so $ef \downarrow$ and

$$ef \Vdash \phi(a)$$

But then, for any $g \in \mathcal{A}$,

$$\begin{aligned} fg &\preceq e'fg \\ &\preceq ef \end{aligned}$$

and so $fg \downarrow$ and,

$$fg \Vdash \phi(a)$$

Hence,

$$(\lambda x).(z((\lambda y, w).xy))\underline{0} \Vdash ((\forall y)((\forall x \in y)\phi(x) \to \phi(y))) \to (\forall y)\phi(y)$$

□

Theorem 4.3.7. *Suppose $\mathcal{A}$ is uniform. Then $V(\mathcal{A})$ satisfies soundness for* **CZF**.

Proof. The only remaining axiom is bounded separation. It is enough to show the soundness of the binary intersection axiom.

Given $A, B \in V(\mathcal{A})$, we must have for each $\langle e, a\rangle \in A$, a set P_a such that $[\![a \in B]\!] = P_a^{\leq}$. By strong collection and union, we can assume this is a function. Define C.

$$C = \{\langle \mathbf{p}ef, a\rangle \mid \langle e, a\rangle \in A \wedge f \in P_a\}$$

Then one can clearly construct a realizer for the statement that any element of C lies in the intersection of A and B.

Now suppose that $\langle e, a\rangle \in A$ and that $f \Vdash a \in B$. Then there is some $f' \in P_a$ such that $f \leq f'$. Hence, $\mathbf{p}ef \leq \mathbf{p}ef'$ and so,

$$(\lambda x, y).\mathbf{p}(\mathbf{p}xy)\mathbf{i}_r \Vdash (\forall x \in A)(x \in B \to x \in C)$$

However, the statement above is logically equivalent to

$$A \cap B \subseteq C$$

and so we can clearly construct a realizer for binary intersection.

□

4.4 The Natural Numbers and Baire Space in $V(\mathcal{A})$

An important point worth noting about the soundness theorem is that we explicitly constructed a set witnessing the axiom of infinity. That is a set $\overline{\omega}$ with a realizer that $\overline{\omega}$ is the usual implementation of the natural numbers in set theory. Recall that we constructed $\overline{\omega}$ as follows. We start with a set $N \subseteq \mathcal{A}$ satisfying the conditions in theorem 2.2.5. That is, N consists of numerals $\underline{n}$ for $n \in \omega$ with representable successor, predecessor, and decision functions. We then define by recursion

$$\begin{aligned} \overline{n} &:= \{\langle \underline{m}, \overline{m} \rangle \mid m < n\} \\ \overline{\omega} &:= \{\langle \underline{n}, \overline{n} \rangle \mid n \in \omega\} \end{aligned}$$

We can also explicitly give a nice presentation of Baire space in $V(\mathcal{A})$ as follows. To make things clearer, we assume that $\mathcal{A}$ is a pca rather than a more general copca.

We first fix some notation that will be useful below.

In constructive set theory, as in classical set theory, we implement ordered pairs as follows:

$$\langle a, b \rangle := \{\{a\}, \{a, b\}\}$$

By following the proof in **CZF** that ordered pairs exist inside $V(\mathcal{A})$, we already know that for any $a, b \in V(\mathcal{A})$, there must be something that $V(\mathcal{A})$ believes to be the ordered pair $\langle a, b\rangle$. However, it is convenient to give an explicit witness, which we define as follows (following [24]):

$$\overline{\langle a, b\rangle} := \{\langle \underline{0}, \{\langle \underline{0}, a\rangle\}\rangle, \langle \underline{1}, \{\langle \underline{0}, a\rangle, \langle \underline{1}, b\rangle\}\rangle\}$$

One can then construct an $e \in \mathcal{A}$ such that

$$e \Vdash \overline{\langle a, b\rangle} = \{\{a\}, \{a, b\}\}$$

(and moreover e does not depend on a or b)

We now (again following [24]) give an explicit construction of the set of functions from ω to ω.

Definition 4.4.1. $f \in \mathcal{A}$ is *type 1* if for every $n \in \omega$, $f.\underline{n} \downarrow$, and there is some $m \in \omega$ such that $f.\underline{n} = \underline{m}$

Definition 4.4.2. Given a type 1 $f \in \mathcal{A}$ we construct $\overline{f}$ as follows

$$\overline{f} := \{\langle \underline{n}, \overline{\langle \overline{n}, \overline{m}\rangle}\rangle \mid n \in \omega \text{ and } f\underline{n} = \underline{m}\}$$

Proposition 4.4.3. *For every f of type 1, there is a realizer in $V(\mathcal{A})$ that $\overline{f}$ is a function from ω to ω.*

Proof. Let e be a realizer for the statement that $\overline{\langle a, b\rangle}$ is the ordered pair of a and b.

Then note that

$$(\lambda x).\mathbf{p}(fx)(\mathbf{p}xe) \Vdash (\forall n \in \overline{\omega})(\exists m \in \overline{\omega})(\exists y \in \overline{f})y = \langle n, m\rangle$$

Also see that if $\langle n, \overline{\langle \underline{n}, \underline{m}\rangle}\rangle, \langle n', \overline{\langle \underline{n'}, \underline{m'}\rangle}\rangle \in \overline{f}$ and $V(\mathcal{A}) \models \underline{n} = \underline{n'}$, then $n = n'$, and so $m = m'$. Hence we can easily construct a realizer for the statement

$$(\forall x, y \in \overline{f})\, \text{First}(x) = \text{First}(y) \to \text{Second}(x) = \text{Second}(y)$$

We can combine these realizers to get a realizer that $\overline{f}$ is a function. □

Proposition 4.4.4. *Suppose $V(\mathcal{A})$ has a realizer stating that $f \in V(\mathcal{A})$ is a function on ω. Then there is a type 1 $g \in \mathcal{A}$, such that $V(\mathcal{A}) \models f = \overline{g}$.*

Proof. Since there is a realizer stating that f is a function, we can find $a, b, c \in \mathcal{A}$ such that

$$\begin{aligned} a &\Vdash (\forall n \in \bar{\omega})(\exists m \in \bar{\omega})\langle n, m\rangle \in f \\ b &\Vdash (\forall x \in f)(\exists n, m \in \bar{\omega})x = \langle n, m\rangle \\ c &\Vdash (\forall n, m, m')\langle n, m\rangle \in f \wedge \langle n, m'\rangle \in f \rightarrow m = m' \end{aligned}$$

Let $g := (\lambda x).(ax)_0$. By the definition of realizability for bounded quantifiers and the definition of a, g must be type 1.

Now each element of $\overline{g}$ is of the form $\langle \underline{n}, \overline{\langle \overline{n}, \overline{g}\rangle}\rangle$. Then by the definition of a, $(a\underline{n})_1 \Vdash \overline{\langle \bar{n}, \overline{(a\underline{n})_0}\rangle} \in f$. Hence, $(\lambda \underline{n}).(a\underline{n})_1$ is a realizer for $g \subseteq f$.

Let $\langle l, x\rangle \in f$. Then $bl \Vdash (\exists n, m \in \bar{\omega})x = \langle n, m\rangle$. Let $n = (bl)_0, m = ((bl)_1)_0$. As before, we know that $(a\underline{n})_1 \Vdash \overline{\langle \overline{n}, \overline{(a\underline{n})_0}\rangle} \in f$. Also we have that $((bl)_1)_1 \Vdash \overline{\langle \overline{n}, \overline{m}\rangle} \in f$, so we can use c to find a realizer for $\overline{m} = \overline{(an)_0}$. This gives a realizer for $x = (\overline{n}, \overline{(an)_0})$. Hence one can construct a realizer for $f \subseteq g$.

Therefore we have $V(\mathcal{A}) \vDash f = \overline{g}$ as required. □

Proposition 4.4.5. *$V(\mathcal{A})$ realizes that the following set is the set of all functions from ω to ω:*

$$A := \{\langle f, \overline{f}\rangle | f : \omega \to \omega\}$$

Proof. This follows from the previous two propositions. □

4.5 Models where Powerset Fails

The independence of the power set axiom from **CZF** is already known and can be found for instance in [23] and [22]. However, there are few examples of realizability models where the powerset axiom does not hold.

The following proposition implies that powerset axiom can only fail in $V(\mathcal{A})$ when $\mathcal{A}$ is a proper class.

Proposition 4.5.1. *Suppose that $\mathcal{A}$ is a set and that the power set axiom holds in the background universe. Then it also holds in $V(\mathcal{A})$.*

Proof. Note that by lemma 4.3.2 we know that $V(\mathcal{A}) \models a \in b$ implies that the rank of a is less than the rank of b. We apply powerset and induction to show that for any α there is a set of everything with rank less than or equal to α. Hence the following is a set for any $A \in V(\mathcal{A})$.

$$P := \{\langle e, b\rangle \mid e \Vdash b \subseteq A\}$$

This is clearly an element of $V(\mathcal{A})$ and is a witness of powerset. □

Proposition 4.5.2. *Let $\mathcal{T}$ be the term model from example 4.2.2. Then the powerset axiom does not hold in $V(\mathcal{T})$.*

Proof. Assume for a contradiction that the powerset axiom does hold in $V(\mathcal{T})$.

Define $A \in V(\mathcal{T})$ as

$$A := \{\langle\emptyset, \emptyset\rangle\}$$

Then by assumption there is some $P \in V(\mathcal{A})$ and an $e \in \mathcal{A}$ such that

$$e \Vdash (\forall x)(((\forall y \in x) y \in A) \to x \in P$$

Recall that we define $\mathrm{Supp}(f)$ as the set of a such that $\mathbf{a}$ appears in f.

Let R be the set of all a such that a occurs in $\mathrm{Supp}(f)$ for some $\langle g, x\rangle \in P$ and $\langle f, y\rangle \in x$, and let S be the union of R and $\mathrm{Supp}(e)$.

Now choose a such that for any $b \in S$ we have $a \not\subseteq b$. For instance, we can take $a = S$.

Now let $B = \{\langle \mathbf{a}, \emptyset \rangle\}$ and note that

$$(\lambda x).\mathbf{p}x\mathbf{i}_r \Vdash (\forall y \in B) y \in A$$

Hence

$$e(\lambda x).\mathbf{p}x\mathbf{i}_r \Vdash B \in P$$

Then we can see that there must be $\langle (e((\lambda x).\mathbf{p}x\mathbf{i}_r))_0, z \rangle \in P$ such that

$$(e((\lambda x).\mathbf{p}x\mathbf{i}_r))_1 \Vdash B = z$$

Since B is inhabited, this implies that z is also inhabited. So let $\langle f, y \rangle$ be an element of z. Now note that if we set $g := (e((\lambda x).\mathbf{p}x\mathbf{i}_r))_1 f$ then g is a term of $\mathrm{CL}(X)$ that contains only constants that appear in S. But

$$g \Vdash \emptyset \in B$$

Hence $(g)_0$ must be some constant $\mathbf{a}'$ such that $a \subseteq a'$. But a' must occur in S so we get a contradiction. □

Chapter 5

Automorphisms and Their Effect on Realizability

In this chapter we investigate the automorphism groups of the pcas described in chapter 2. In doing this, the first point to consider is what we should take as the definition of homomorphism between pcas. For one thing, it is not clear whether or not s and k should be regarded as constants that are fixed by homomorphisms. The two alternatives give us two definitions of homomorphisms that we call *strong* and *weak*. Furthermore, Longley in [20] has suggested that the "correct" definition should be even more general in the sense that application only has to be preserved "up to realizability." Longley's definition, *applicative morphism* also has the feature of requiring only multivalued functions rather than (well defined) functions. However, we will show that when considering automorphisms we can disregard this point and work with bijective functions as usual.

In this chapter we will concentrate on more concrete aspects of some of the usual examples of pcas. The existing body of work that it is closest to is perhaps Bethke's work on a class of (strong) homomorphisms called collapses in [7], or Klop's proof in [8] that there are pcas that can't be embedded into any (total) combinatory algebra.

We will define a pca as *natural* if it can be defined within its own realizability universe $V(\mathcal{A})$. We will show that $\mathcal{K}_1$, $\mathcal{K}_2$, and $\mathcal{P}(\omega)$ satisfy the definition. These pcas all have quite tame automorphism groups even for applicative automorphisms.

We also investigate the automorphism groups of D_∞ and term models.

5.1 Homomorphisms of Pcas

Let $\mathcal{A}$ and $\mathcal{B}$ be pcas. Then one can consider the following definitions of homomorphism.

Definition 5.1.1. A *weak homomorphism* is θ is a function $\mathcal{A} \to \mathcal{B}$ such that for any e, f, if $e.f \downarrow$ then $\theta(ef) = \theta(e)\theta(f)$.

Definition 5.1.2. A *strong homomorphism*, θ is a weak homomorphism such that $\theta(\mathrm{s}) = \mathrm{s}$ and $\theta(\mathbf{k}) = \mathbf{k}$.

Definition 5.1.3 (Longley)**.** An *applicative morphism* is a function $\theta : \mathcal{A} \to \mathcal{P}^*(\mathcal{B})$, such that there is some $r \in \mathcal{B}$ such that for all $e, f \in \mathcal{A}$ and for all e', f' with $e' \in \theta(e)$ and $f' \in \theta(f)$, $re'f' \in \theta(ef)$.

For each of these definitions, there is a corresponding notion of isomorphism, defined as a homomorphism that has a (2-sided) inverse. Observe that applicative morphisms need not be functions from $\mathcal{A}$ to $\mathcal{B}$. However, when we switch to automorphisms, we can disregard this issue by the following proposition.

Proposition 5.1.4. *Suppose that $\theta : \mathcal{A} \to \mathcal{P}^*(\mathcal{B})$ is an applicative isomorphism. Then there is a bijection $\theta' : \mathcal{A} \to \mathcal{B}$ such that for all $e \in \mathcal{A}$, $\theta(e) = \{\theta'(e)\}$.*

Proof. Let $\theta^{-1} : \mathcal{B} \to \mathcal{P}^*(\mathcal{A})$ be the inverse of θ. Now suppose that $e \in \mathcal{A}$ and $f, f' \in \theta(e)$. Then $\theta \circ \theta^{-1}(f) = \{f\}$. But $\theta^{-1}(f) \subseteq \theta^{-1} \circ \theta(e) = \{e\}$. Hence $\theta^{-1}(f) = \{e\} = \theta^{-1}(f')$. Therefore we get $\{f\} = \theta \circ \theta^{-1}(f) = \theta \circ \theta^{-1}(f') = \{f'\}$, and so $f = f'$.

We deduce that for every $e \in \mathcal{A}$, $\theta(e)$ is a singleton. So we can take $\theta'(e)$ such that $\theta(e) = \{\theta'(e)\}$. □

In future we will refer to applicative automorphisms of a pca, $\mathcal{A}$ as bijections $\mathcal{A} \to \mathcal{A}$.

Definition 5.1.5. We say that an applicative morphism $\theta : \mathcal{A} \to \mathcal{P}^*(\mathcal{B})$ is *decidable* if there is an element $d \in \mathcal{B}$ such that defining $T := (\lambda x, y)y$ and $F := (\lambda x, y)x$, we have that for $e \in \theta(T)$, $de = T$, and for $f \in \theta(F)$, $df = F$.

Proposition 5.1.6. *Any applicative isomorphism is decidable.*

Proof. Note that

$$\theta^{-1}(F) = F\theta^{-1}(F)\theta^{-1}(T)$$

and hence, applying θ to both sides,

$$\begin{aligned} F &= \theta(F\theta^{-1}(F)\theta^{-1}(T)) \\ &= r\theta(F\theta^{-1}(F))T \qquad \text{by the definition of applicative morphism} \\ &= r(r\theta(F)F)T \end{aligned}$$

However, we can similarly show that

$$T = r(r\theta(T)F)T$$

Hence we can take

$$d := (\lambda x).r(rxF)T$$

□

5.2 Preservation of Realizability by Homomorphisms

Note that if $\theta : \mathcal{A} \to \mathcal{B}$ is an applicative morphism, then we can lift it to an operation $\tilde{\theta}$ from $V(\mathcal{A})$ to $V(\mathcal{B})$ by the following inductive definition.

$$\tilde{\theta}(a) := \{\langle e', \tilde{\theta}(b)\rangle \mid \langle e, b\rangle \in a, e' \in \theta(e)\}$$

For convenience we will write $\tilde{\theta}$ as θ.

Given a formula ϕ over $V(\mathcal{A})$, we write ϕ^θ to mean the formula over $V(\mathcal{B})$ resulting from replacing each parameter a in ϕ by $\theta(a)$.

5.2.1 Applicative Morphisms

The preservation of realizability by applicative morphisms was first studied by Longley in [20] in a category theoretic context. We show in this section that similar results hold in this context.

Theorem 5.2.1. *Suppose that ϕ is a formula over $V(\mathcal{A})$, without negation, implication, disjunction, or unbounded universal quantification. Let $\mathcal{A}$ and $\mathcal{B}$ be pcas. Then there is $r_\phi \in \mathcal{B}$ such that for any applicative morphism $\theta : \mathcal{A} \to \mathcal{B}$ with r a realizer for θ, $\mathbf{p}_0' \in \theta(\mathbf{p}_0)$ and $\mathbf{p}_1' \in \theta(\mathbf{p}_1)$, and $e' \in \theta(e)$ where $e \Vdash \phi$, we have*

$$r_\phi r \mathbf{p}_0' \mathbf{p}_1' e' \Vdash \phi^\theta$$

Furthermore, r_ϕ does not depend on any parameters appearing in ϕ.

Proof. We will show this by induction on the complexity of ϕ.

Assume first that ϕ is atomic.

Construct by the fixed point theorem $r_\in$ and $r_=$ satisfying for every $e' \in \mathcal{B}$,

$$\begin{aligned} r_\in r \mathbf{p}_0' \mathbf{p}_1' e' &= \mathbf{p}(r\mathbf{p}_0' e')(r_= r \mathbf{p}_0' \mathbf{p}_1'(r\mathbf{p}_1' e')) \\ r_= r \mathbf{p}_0' \mathbf{p}_1' e' &= \mathbf{p}((\lambda x).r_\in r \mathbf{p}_0' \mathbf{p}_1'(r(r\mathbf{p}_0' e')x))((\lambda x).r_\in r \mathbf{p}_0' \mathbf{p}_1'(r(r\mathbf{p}_1' e')x)) \end{aligned}$$

We now show that the theorem holds for atomic formulas by simultaneous induction on rank.

Suppose that $e \Vdash a \in b$, that $e' \in \theta(e)$ and that r, $\mathbf{p}_0'$ and $\mathbf{p}_1'$ are as in the statement of the theorem. Then we know that there is some c such that $\langle (e)_0, c\rangle \in b$ and $(e)_1 \Vdash a = c$. Since $e' \in \theta(e)$, we know that $r\mathbf{p}_0' e' \in \theta((e)_0)$, and and $r\mathbf{p}_1' e' \in \theta((e)_1)$. We deduce that $\langle r\mathbf{p}_0' e', \theta(c)\rangle \in \theta(b)$, and by induction we can assume also that $r_= r\mathbf{p}_0'\mathbf{p}_1'(r\mathbf{p}_1' e') \Vdash \theta(a) = \theta(c)$. Therefore $\mathbf{p}(r\mathbf{p}_0' e')(r_= r\mathbf{p}_0'\mathbf{p}_1'(r\mathbf{p}_1' e')) \Vdash \theta(a) \in \theta(b)$. But by this is equal to $r_\in r\mathbf{p}_0'\mathbf{p}_1' e'$ by construction.

Now suppose that $e \Vdash a = b$. We aim to show that for any $\langle f', c' \rangle \in \theta(a)$,

$$r_\in r\mathbf{p}'_0\mathbf{p}'_1(r(r\mathbf{p}'_0e')f')) \Vdash c' \in \theta(b)$$

First note that there must be some $\langle f, c \rangle \in a$ such that $f' \in \theta(f)$ and $c' = \theta(c)$. We know that $(e)_0 f \Vdash c \in b$. Furthermore, note that $r\mathbf{p}'_0 e \in \theta((e)_0)$ and hence $r(r\mathbf{p}'_0e)f' \in \theta((e)_0 f)$.

By induction we can deduce that $r_\in\mathbf{p}'_0\mathbf{p}'_1(r(r\mathbf{p}'_0e)f') \Vdash \theta(c) \in \theta(b)$. We can similarly show that for any $\langle f', c' \rangle \in \theta(b)$, $r_\in\mathbf{p}'_0\mathbf{p}'_1(r(r\mathbf{p}'_1e)f') \Vdash c' \in \theta(a)$. Therefore $\mathbf{p}((\lambda x).r_\in\mathbf{p}'_0\mathbf{p}'_1(r(r\mathbf{p}'_0e)x))((\lambda x).r_\in\mathbf{p}'_0\mathbf{p}'_1(r(r\mathbf{p}'_1e)x)) \Vdash \theta(a) = \theta(b)$ as required.

Now suppose that ϕ is of the form $\phi_0 \wedge \phi_1$ and that $e \Vdash \phi_0 \wedge \phi_1$. Then we know that $(e)_0 \Vdash \phi_0$ and $(e)_1 \Vdash \phi_1$. Furthermore, if $e' \in \theta(e)$, we know that $r\mathbf{p}'_0e' \in \theta((e)_0)$ and $r\mathbf{p}'_1e' \in \theta((e)_1)$. By induction we can assume that we have constructed r_{ϕ_0} and r_{ϕ_1} such that $r_{\phi_0}r\mathbf{p}'_0\mathbf{p}'_1(r\mathbf{p}'_0e') \Vdash \phi_0^\theta$ and $r_{\phi_1}r\mathbf{p}'_0\mathbf{p}'_1(r\mathbf{p}'_1e') \Vdash \phi_1^\theta$. We deduce that $\mathbf{p}(r_{\phi_0}r\mathbf{p}'_0\mathbf{p}'_1(r\mathbf{p}'_0e'))(r_{\phi_1}r\mathbf{p}'_0\mathbf{p}'_1(r\mathbf{p}'_1e')) \Vdash \phi^\theta$. Hence we can take

$$r_\phi := (\lambda x, y, z, w).\mathbf{p}(r_{\phi_0}xyz(xyw))(r_{\phi_1}xyz(xzw))$$

Now suppose that ϕ is of the form $(\forall x \in a)\psi(x)$. Let $\langle f', c' \rangle \in \theta(a)$. Then we know that there is some $\langle f, c \rangle \in a$ such that $c' = \theta(c)$ and $f' \in \theta(f)$. If $e \Vdash (\forall x \in a)\phi(x)$, we know that $ef \Vdash \psi(c)$. Furthermore, we know that $re'f' \in \theta(ef)$. By induction we can assume that there is r_ψ such that $r_\psi r\mathbf{p}'_0\mathbf{p}'_1(re'f') \Vdash \psi^\theta(c')$. Hence we can take

$$r_\phi\mathbf{p}'_0\mathbf{p}'_1re' := (\lambda x).(r_\psi r\mathbf{p}'_0\mathbf{p}'_1(re'x))$$

Bounded and unbounded existential quantifiers can be handled similarly. □

We now show that if we add in the condition that θ is decidable, then we can also get the result for disjunctions.

Theorem 5.2.2. *Suppose that ϕ is a formula over $V(\mathcal{A})$, without negation, implication, or unbounded universal quantification. Let $\mathcal{A}$ and $\mathcal{B}$ be pcas. Then there is $r_\phi \in \mathcal{B}$ such* *that for any* decidable *applicative morphism* $\theta : \mathcal{A} \to \mathcal{B}$ *with* r *a realizer and* d *a decider for* θ*,* $\mathbf{p}_0' \in \theta(\mathbf{p}_0)$ *and* $\mathbf{p}_1' \in \theta(\mathbf{p}_1)$*, and* $e' \in \theta(e)$ *where* $e \Vdash \phi$*, we have*

$$r_\phi r d \mathbf{p}_0' \mathbf{p}_1' e' \Vdash \phi^\theta$$

Furthermore, r_ϕ *does not depend on any parameters appearing in* ϕ*.*

Proof. We show this by induction on the complexity of ϕ. All the induction steps except for disjunction are covered by the previous proof.

Assume that $\phi = \phi_0 \vee \phi_1$. Let $e \Vdash \phi$ and $e' \in \theta(e)$. Then either $(e)_0 = F$ and $(e)_1 \Vdash \phi_0$, or $(e)_0 = T$ and $(e)_1 \Vdash \phi_1$. Note that $r\mathbf{p}_0'e' \in \theta((e)_0)$ and that $d(r\mathbf{p}_0'e')$ is equal to T if $(e)_0$ is equal to T and is equal to F if $(e)_0$ is equal to F. Also we know that $r\mathbf{p}_1'e' \in \theta((e)_1)$. By induction we can assume that we have r_{ϕ_0} and r_{ϕ_1} such that if $(e)_1 \Vdash \phi_0$, then $r\mathbf{p}_1'e' \Vdash \phi_0^\theta$ and if $(e)_1 \Vdash \phi_1$ then $r\mathbf{p}_1'e' \Vdash \phi_1^\theta$. Let $\mathbf{d}$ be defined using theorem 2.2.5 so that for all $b, b' \in \mathcal{B}$,

$$\mathbf{d}\underline{0}bb' = b$$
$$\mathbf{d}\underline{1}bb' = b'$$

Then we can take

$$r_\phi := (\lambda v, w, x, y, z).(\mathbf{p}(y(vwz))((\mathbf{d}r_{\phi_0}r_{\phi_1}(y(vwz)))(v(xz))))$$

□

In the following theorem we apply proposition 5.1.4 so that we think of an isomorphism, θ, as a bijection.

Theorem 5.2.3. *Suppose that* ϕ *is a formula over* $V(\mathcal{A})$*. Let* $\mathcal{A}$ *and* $\mathcal{B}$ *be pcas. Then there is* $r_\phi \in \mathcal{B}$ *such that for any applicative isomorphism* $\theta : \mathcal{A} \to \mathcal{B}$ *with* r *a realizer and* d *a decider for* θ*,* r' *a realizer and* d' *a decider for* θ^{-1}*, and* $e \Vdash \phi$*, we have*

$$r_\phi r d \theta(\mathbf{p}_0)\theta(\mathbf{p}_1) r' d' \theta^{-1}(\mathbf{p}_0)\theta^{-1}(\mathbf{p}_1)\theta(e) \Vdash \phi^\theta$$

Furthermore, r_ϕ *does not depend on any parameters appearing in* ϕ*.*

Proof. It only remains to check the induction steps for negation, implication and unbounded quantification. We will show implication; the other two cases are similar.

Suppose that $\phi = \phi_0 \to \phi_1$. By induction assume that we have r_{ϕ_0} and r_{ϕ_1} as before. Now suppose that $f \Vdash \phi_0^\theta$. By applying the inductive hypothesis to θ^{-1}, if we set

$$f' = r_{\phi_0} r' d' \theta^{-1}(\mathbf{p}_0)\theta^{-1}(\mathbf{p}_1) r d \theta(\mathbf{p}_0)\theta(\mathbf{p}_1)\theta^{-1}(f)$$

Then

$$f' \Vdash (\phi_0^\theta)^{\theta^{-1}} = \phi_0$$

Hence $e.f' \Vdash \phi_1$ and so

$$r_{\phi_1} r d r d \theta(\mathbf{p}_0)\theta(\mathbf{p}_1) r' d' x \theta^{-1}(\mathbf{p}_0)\theta^{-1}(\mathbf{p}_1)\theta(e.f') \Vdash \phi_1^\theta$$

However note that we have $\theta(e.f') = r\theta(e).\theta(f')$ and we can express $\theta(f')$ in terms of f, and so we can write down a lambda term that realizes $\phi_0^\theta \to \phi_1^\theta$. □

5.2.2 Strong Homomorphisms

In this section we suppose that the constants used in the definition of realizability $\mathbf{p}$, $\mathbf{p}_0$, $\mathbf{p}_1$, $\underline{0}$ and $\underline{1}$ are constructed from $\mathbf{s}$ and $\mathbf{k}$. We can hence assume that they are fixed by any strong homomorphism.

Theorem 5.2.4. *Suppose that ϕ is a formula over $V(\mathcal{A})$ without negation, implication, or unbounded universal quantification. Let $\theta : \mathcal{A} \to \mathcal{B}$ be a strong homomorphism. If $e \Vdash \phi$ then $\theta(e) \Vdash \phi^\theta$.*

Proof. We first show by induction that $\in$ and $=$ are preserved.

Suppose that $e \Vdash a \in b$. That is, there is some $e', e'' \in \mathcal{A}$ and some $\langle e', c\rangle \in b$ such that

$$e'' \Vdash a = c$$

Then by induction, we may assume that

$$\theta(e'') \Vdash \theta(a) = \theta(c)$$

But we also have that $\langle \theta(e'), \theta(c) \rangle \in \theta(b)$ and

$$\begin{aligned} \theta(e) &= \theta(\mathbf{p}e'e'') \\ &= \theta(\mathbf{p})\theta(e')\theta(e'') \\ &= \mathbf{p}\theta(e')\theta(e'') \end{aligned}$$

Hence we can deduce that

$$\theta(e) \Vdash \theta(a) \in \theta(b)$$

Now suppose that $e \Vdash a = b$. Then there is some $e', e'' \in \mathcal{A}$ such that for every $\langle f, c \rangle \in a$, we have $e'f \Vdash c \in b$ and for every $\langle f, c \rangle \in b$ we have $e''f \Vdash c \in a$.

Then any element of $\theta(a)$ is of the form $\langle \theta(f), \theta(c) \rangle$, where $\langle f, c \rangle \in a$. Hence $e'f \Vdash c \in b$ and by induction, we may deduce that

$$\theta(e'f) \Vdash \theta(c) \in \theta(b)$$

But $\theta(e')\theta(f) = \theta(e'f)$

Similarly, we know that any element of $\theta(b)$ is of the form $\langle \theta(f), \theta(c) \rangle$ and that

$$\theta(e''f) \Vdash \theta(c) \in \theta(a)$$

As before, we also know that

$$\theta(e) = \mathbf{p}\theta(e')\theta(e'')$$

and so

$$\theta(e) \Vdash \theta(a) = \theta(b)$$

We now proceed by induction on the structure of formulas. Conjunction and disjunction are clear from the fact that $\mathbf{p}$, $\underline{0}$ and $\underline{1}$ are fixed by θ. It remains to check bounded quantifiers and unbounded existential quantifiers.

Suppose that

$$e \Vdash (\exists x)\phi(x)$$

Then there is some $a \in V(\mathcal{A})$ such that $e \Vdash \phi(a)$. But then $\theta(e) \Vdash \phi^{\theta}(\theta(a))$, and so

$$\theta(e) \Vdash (\exists x)\phi^{\theta}(x)$$

Now suppose that $e \Vdash (\exists x \in a)\phi(x)$. Then there is some element $\langle (e)_0, c\rangle$ of a such that $(e)_1 \Vdash \phi(c)$. But then

$$\langle (\theta(e))_0, \theta(c)\rangle \in \theta(a)$$

and

$$(\theta(e))_1 \Vdash \phi^{\theta}(\theta(c))$$

and so

$$\theta(e) \Vdash (\exists x \in \theta(a))\phi^{\theta}(x)$$

Now suppose that $e \Vdash (\forall x \in a)\phi(x)$.

Then we aim to show $\theta(e) \Vdash (\forall x \in \theta(a))\phi^{\theta}(x)$.

Every element of $\theta(a)$ is of the form $\langle \theta(f), \theta(c)\rangle$ where $\langle f, c\rangle \in a$. Hence

$$ef \Vdash \phi(c)$$

and so by induction we may assume $\theta(ef) \Vdash \phi^{\theta}(\theta(c))$. □

Theorem 5.2.5. *Suppose that ϕ is a formula over $V(\mathcal{A})$ and $\theta : \mathcal{A} \to \mathcal{B}$ is an isomorphism. If $e \Vdash \phi$, then $\theta(e) \Vdash \phi^{\theta}$.*

Proof. We proceed by induction on the construction of formulas. Every case has already been done in the proof of the previous theorem except for implication and unbounded universal quantification.

Suppose that

$$e \Vdash \phi \to \psi$$

Then we aim to show that

$$\theta(e) \Vdash \phi^{\theta} \to \psi^{\theta}$$

To show this, suppose that $f \Vdash \phi^\theta$. Then since θ^{-1} is also an isomorphism, we know by induction that

$$\theta^{-1}(f) \Vdash \phi$$

Hence

$$e\theta^{-1}(f) \Vdash \psi$$

But $\theta(e)f = \theta(e\theta^{-1}(f))$, so we deduce that

$$\theta(e)f \Vdash \psi^\theta$$

and so

$$\theta(e) \Vdash \phi \to \psi$$

as required.

Now suppose that

$$e \Vdash (\forall x)\phi(x)$$

Then for any $b \in V(\mathcal{B})$ we have $\theta^{-1}(b) \in V(\mathcal{A})$, and so

$$e \Vdash \phi(\theta^{-1}(b))$$

We deduce that

$$\theta(e) \Vdash \phi^\theta(b)$$

and so

$$\theta(e) \Vdash (\forall x)\phi^\theta(x)$$

as required. □

5.3 Natural Pcas

For any pca, $\mathcal{A}$ we can consider the realizability model $V(\mathcal{A})$, as defined in section 4.3. Informally, a pca $\mathcal{A}$ is natural if it can be defined inside $V(\mathcal{A})$. Before we show the formal definition of natural, we first recursively define the following operation on $V(\mathcal{A})$

$$\hat{a} := \{\hat{b} \mid (\exists e \in \mathcal{A})\langle e, b\rangle \in a\}$$

Definition 5.3.1. A pca, $\mathcal{A}$, is *natural*, if there is some $A \in V(\mathcal{A})$ and some $\phi(x)$ a formula over $V(\mathcal{A})$ such that

1. for all $e \in \mathcal{A}$ there is a such that $\langle e, a\rangle \in A$
2. for all $\langle e, a\rangle, \langle e', a'\rangle \in A$, $\hat{a} = \hat{a'}$ implies that $e = e'$
3. $V(\mathcal{A}) \models (\exists! x)\phi(x)$
4. $V(\mathcal{A}) \models \phi(A)$
5. any parameters in $\phi(x)$ are fixed by all applicative automorphisms

Theorem 5.3.2. *Suppose that $\mathcal{A}$ is a natural pca. Then there are $e, e_0, e_1, e_2 \in \mathcal{A}$ such that for any applicative automorphism, α, with realizer r, and realizer r' for α^{-1} we have that for any $f \in \mathcal{A}$*

$$err'\alpha(e_0)\alpha(e_1)\alpha(e_2)\alpha^{-1}(e_0)\alpha^{-1}(e_1)\alpha^{-1}(e_2)f = \alpha(f)$$

Proof. Fix $e_0, h \in \mathcal{A}$ such that

$$\begin{aligned} e_0 &\Vdash \phi(A) \\ h &\Vdash \phi(x) \wedge \phi(y) \to x = y \end{aligned}$$

By proposition 5.2.3 we have some r_ϕ such that for any applicative automorphism α with realizer r and realizer r' for α^{-1}, and any f such that $f \Vdash \phi(a)$,

$$r_\phi rr'\alpha(\mathbf{p}_0)\alpha(\mathbf{p}_1)\alpha^{-1}(\mathbf{p}_0)\alpha^{-1}(\mathbf{p}_1)\alpha(f) \Vdash \phi(\alpha(a))$$

(Note that $(\phi(a))^\alpha = \phi(\alpha(a))$ since any parameters in ϕ are fixed by α).

Let

$$g := r_\phi rr'\alpha(\mathbf{p}_0)\alpha(\mathbf{p}_1)\alpha^{-1}(\mathbf{p}_0)\alpha^{-1}(\mathbf{p}_1)$$

We have in particular that

$$g\alpha(e_0) \Vdash \phi(\alpha(A))$$

and so

$$he_0(g\alpha(e_0)) \Vdash A = \alpha(A)$$

Let $g' = he_0(g\alpha(e_0))$. Then for any $\langle f, a\rangle \in A$ there is $\langle (g'f)_0, b\rangle \in \alpha(A)$ such that $(g'f)_1 \Vdash a = b$. Since $\langle (g'f)_0, b\rangle \in \alpha(A)$, we know that there is some $\langle f', a'\rangle \in A$ such that $(g'f)_0 = \alpha(f')$ and $b = \alpha(a')$. Then $\hat{a} = \hat{b} = \alpha(\hat{a'})$. But $\alpha(\hat{a'}) = \hat{a'}$ and so $\hat{a'} = \hat{a}$. By condition 2 of the definition of natural this means that $f' = f$. But we have now shown that $\alpha(f) = (g'f)_0$. But by condition 1 in the definition of natural we have this for any $f \in \mathcal{A}$.

Hence we can take

$$\begin{aligned} e_1 &:= \mathbf{p}_0 \\ e_2 &:= \mathbf{p}_1 \end{aligned}$$

and define e so that

$$err'\alpha(e_0)\alpha(e_1)\alpha(e_2)\alpha^{-1}(e_0)\alpha^{-1}(e_1)\alpha^{-1}(e_2) = (\lambda x).(g'x)_0$$

(Note that we defined g and g' so that they depend only on r, r', $\alpha(e_0)$, $\alpha(e_1)$, $\alpha(e_2)$, $\alpha^{-1}(e_0)$, $\alpha^{-1}(e_1)$ and $\alpha^{-1}(e_2)$.)

□

We immediately get the following corollaries.

Corollary 5.3.3. *The applicative automorphisms of a natural pca are precisely the representable permutations.*

So in particular, any automorphism of $\mathcal{K}_1$ is computable, and any automorphism of $\mathcal{K}_2$ or $\mathcal{P}(\omega)$ is continuous. The following proposition shows that for natural pcas, automorphisms, since they are representable, have little effect on realizability structure.

Proposition 5.3.4. *Suppose that $\alpha : \mathcal{A} \to \mathcal{A}$ is an automorphism and both α and α^{-1} are representable. Then for any $a \in V(\mathcal{A})$ we have $V(\mathcal{A}) \models a = \alpha(a)$. Moreover, the same realizer works for any $a \in V(\mathcal{A})$.*

Proof. Let $a \in V(\mathcal{A})$ and suppose that $e \in \mathcal{A}$ is such that for any $\langle f, b\rangle \in a$,

$$e \Vdash b = \alpha(b)$$

Then for any $\langle f, b\rangle \in a$,

$$\mathbf{p}\alpha(f)e \Vdash b \in \alpha(a)$$

and for $\langle \alpha(f), \alpha(b)\rangle \in \alpha(a)$,

$$\mathbf{p}f(\mathbf{i}_s e) = \mathbf{p}\alpha^{-1}(\alpha(f))(\mathbf{i}_s e) \Vdash \alpha(b) \in a$$

Now note that by the fixed point theorem and the representability of α and α^{-1}, we can construct $e \in \mathcal{A}$ such that for any $f \in \mathcal{A}$,

$$\begin{aligned} (e)_0 f &\simeq \mathbf{p}\alpha(f)e \\ (e)_1 f &\simeq \mathbf{p}\alpha^{-1}(f)(\mathbf{i}_s e) \end{aligned}$$

However, note that we can now use $\in$-induction and the above argument to show that for any $a \in V(\mathcal{A})$,

$$e \Vdash a = \alpha(a)$$

□

Corollary 5.3.5. *The group of applicative automorphisms of a natural pca, $\mathcal{A}$ (and hence also of weak and strong automorphisms) has cardinality less than or equal to that of $\mathcal{A}$.*

Corollary 5.3.6. *Let $\mathcal{A}$ be a natural pca. Then there is some finite set $e_1, \ldots, e_n \in \mathcal{A}$ with the following property.*

Suppose that α and β are weak automorphisms of $\mathcal{A}$ such that for each i $\alpha(e_i) = \beta(e_i)$ and $\alpha^{-1}(e_i) = \beta^{-1}(e_i)$. Then $\alpha = \beta$.

Proof. Note that weak automorphisms are precisely applicative automorphisms where the identity, $I := \mathbf{skk}$ is a realizer.

Hence using the same notation as in the statement of theorem 5.3.2, for every $f \in \mathcal{A}$,

$$\begin{aligned}\alpha(f) &= eII\alpha(e_0)\alpha(e_1)\alpha(e_2)\alpha^{-1}(e_0)\alpha^{-1}(e_1)\alpha^{-1}(e_2)f \\ &= eII\beta(e_0)\beta(e_1)\beta(e_2)\beta^{-1}(e_0)\beta^{-1}(e_1)\beta^{-1}(e_2)f \\ &= \beta(f)\end{aligned}$$

□

5.4 Automorphisms of $\mathcal{K}_1$

Theorem 5.4.1. *$\mathcal{K}_1$ is natural.*

Proof. Let $\overline{\omega} = \{\langle \underline{n}, \overline{n}\rangle \mid n \in \omega\}$. We saw in section 4.4 that this appears as the natural numbers in $V(\mathcal{A})$. Hence take $A = \overline{\omega}$ and $\phi(x)$ to be the formula stating that x is the natural numbers. This clearly satisfies the necessary conditions. □

5.4.1 Weak Automorphisms of $\mathcal{K}_1$

The definition of weak homomorphism is much more restrictive than that of applicative morphism. One might ask therefore whether any non trivial weak automorphisms of $\mathcal{K}_1$ even exist. We will show that the group of weak automorphisms is nontrivial.

We will adapt the proof of the following theorem due to Blum. (This appears in [29].)

Theorem 5.4.2 (Blum)**.** *Let $A = \langle \mathbb{N}, ._A\rangle, B = \langle \mathbb{N}, ._B\rangle$ be $\mathcal{K}_1$ under different encodings. Then there is a $\theta : \mathbb{N} \to \mathbb{N}$ such that θ is bijective and $\forall m, n \in \mathbb{N}$, $\theta(m._A n) = \theta(m)._B\theta(n)$.*

Proof. We first construct for each $\alpha : \mathbb{N} \to \mathbb{N}$ recursive, θ_α such that

$$\alpha(m._A n) \simeq \theta_\alpha(m)._B\alpha(n) \tag{5.4.1}$$

Define α^{-1} such that $\alpha^{-1}(m)$ is the least n with $\alpha(n) = m$. Since there is an algorithm to find this, α^{-1} is partial recursive, and it can be found recursively from α.

Note that if α is a bijection, then the above condition is equivalent to either of the two below

$$\begin{aligned} \alpha(m._A\alpha^{-1}(n)) &\simeq \theta_\alpha(m)._B n \qquad (5.4.2) \\ \alpha^{-1}(\theta_\alpha(m)._B\alpha(n)) &\simeq m._A n \qquad (5.4.3) \end{aligned}$$

We define θ_α in stages, θ^s_α, so that $\theta_\alpha = \bigcup_s \theta^s_\alpha$. At each stage we add an extra element to the domain, ensuring that θ^s_α is injective. At odd stages, we ensure that at some point every element of $\mathbb{N}$ is in the domain of θ_α, and that equation (5.4.2) holds for every n, for m the element added to the domain. At even stages we ensure that at some point every element of $\mathbb{N}$ is in the image of θ_α, and that equation (5.4.3) holds for every n for m the element added to the domain.

For $s + 1$ odd, let m be the least element of $\mathbb{N}$ not in the domain of θ^s_α. Note that there are infinitely many m' encoding in B the recursive function $\alpha \circ (m._A) \circ \alpha^{-1}$. Furthermore, it can be shown that it is possible to recursively enumerate infinitely many of these m'. Hence we can find recursively such an m' that is not in the image of θ^s_α. Let $\theta^{s+1}_\alpha(m) = m'$.

For $s + 1$ even, let m be the least element of $\mathbb{N}$ not in the image of θ^s_α. Note that there are infinitely many m' encoding in A the function $\alpha^{-1} \circ m._B \circ \alpha$. Similarly to before we can find recursively one such m' that is not in the domain of θ^s_α. Let $\theta^{s+1}_\alpha(m') = m$.

Since θ_α can be found recursively from (an encoding of) α, it must have a fixed point, θ. We know by construction that θ_θ is bijective satisfying (5.4.2) for numbers added at odd stages and (5.4.3) for numbers added at even stages. But this means equation (5.4.1) applies everywhere, as required.

□

Corollary 5.4.3. *Let $m_1, \ldots, m_k$ and $n_1, \ldots, n_k$ be finite lists of integers. Then there is some weak automorphism θ such that for each i, $\theta(m_i) \neq n_i$.*

Proof. First note we can take $A = B$.

Note that for $s+1$ odd we constructed θ^s_α by enumerating an infinite list of m' such that m' encodes the function $\alpha^{-1} \circ m. \circ \alpha$ and choosing one that not in the image of θ^s_α. We can simply require that in addition, if there is some i such that $m = m_i$, then m' is not equal to n_i. We can then carry through the rest of the proof to construct a suitable automorphism. □

5.5 $\mathcal{K}_2$ is Natural

We will now show that $\mathcal{K}_2$ is natural, in fact that $\mathcal{K}_2$ is definable in $V(\mathcal{K}_2)$ as $\mathbb{N}^\mathbb{N}$.

The idea here is that functions from $\mathbb{N}$ to $\mathbb{N}$ in the realizability model correspond to type 1 elements (definition 4.4.1) of $\mathcal{K}_2$, so we need to show that we can switch between type 1 elements and actual functions in a representable way. We do this with the following two lemmas.

Lemma 5.5.1. *There is an element, f, of $\mathcal{K}_2$ such that for every $h \in \mathcal{K}_2$, and every $n \in \omega$*

$$fh\underline{n} = \underline{h(n)}$$

where $\underline{n}$ is the function constantly equal to n

Proof. Define f as follows

$$f(l) = \begin{cases} h_n + 2 & \exists k, n, h_i \; l = \langle \langle k, n \rangle, h_1, \ldots, h_n \rangle \\ 0 & \exists k, n, h_i, n' \; n' < n \text{ and } l = \langle \langle k, n \rangle, h_1, \ldots, h_{n'} \rangle \\ 1 & \text{otherwise} \end{cases}$$

Then

$$fh(l) = \begin{cases} h(n) + 1 & \exists k, n \; l = \langle k, n \rangle \\ 0 & \text{otherwise} \end{cases}$$

and so

$$fh\underline{n}(k) = h(n)$$

That is

$$fh\underline{n} = \underline{h(n)}$$

□

Lemma 5.5.2. *There is an element, g, of $\mathcal{K}_2$ with the following property. Let $h \in \mathcal{K}_2$ be such that for every n, $h\underline{n}$ is defined and of the form $\underline{h_n}$ for $h_n \in \omega$. Then $(gh)(n) = h_n$.*

Proof. Define g as follows

$$g(l) = \begin{cases} h_k & \exists n, k, h_i l = \langle n, h_1, \ldots, h_k \rangle k = \langle 0, n, \ldots, n \rangle \\ 0 & \text{otherwise} \end{cases}$$

Then

$$\begin{aligned} gh(n) &= h\underline{n}(0) \\ &= h_n \end{aligned}$$

□

Definition 5.5.3. Recall from section 4.4 that given g of type 1 we can define $\overline{g}$. If f is as above, then for any $h \in \mathcal{K}_2$, fh is of type 1. Hence we can define

$$\hat{h} := \overline{fh}$$

Theorem 5.5.4. *$\mathcal{K}_2$ is natural, with A given by*

$$A = \{\langle h, \hat{h} \rangle | h : \omega \to \omega\}$$

where $\bar{f} \in V(\mathcal{K}_2)$ is as in section 4.4.

Proof. Recall that in proposition 4.4.5 we showed that if

$$B := \{\langle h, \overline{h} \rangle | h : \omega \to \omega\}$$

then there is a realizer that B is the set of all functions from ω to ω.

However, note that by the definition of $\hat{h}$ we can use lemmas 5.5.1 and 5.5.2 to construct a realizer for $A = B$. But then by substitution this gives us a realizer for the statement that A is the set of functions ω to ω. □

Theorem 5.5.5. $\mathcal{K}_2^{\mathrm{REC}}$ *is natural.*

Proof. Note that all the functions we used in the proof were computable, so exactly the same proof applies to $\mathcal{K}_2^{\mathrm{REC}}$. □

5.6 Automorphisms of $\mathcal{P}(\omega)$

Firstly note that since weak automorphisms are only required to preserve the applicative structure $\mathcal{P}(\omega)$ we don't know a priori that they also fix the order structure, ie that they are order preserving with respect to $\subseteq$. We will first establish that this is the case and in fact even applicative automorphisms must be order preserving.

Unfortunately we require excluded middle in order to prove this.

Proposition 5.6.1. *The empty set, $X = \emptyset$ is the unique $X \in \mathcal{P}(\omega)$ such that there exists $D, Z \in \mathcal{P}(\omega)$ such that $Z \neq X$ and for all $Y \in \mathcal{P}(\omega)$*

$$DY = \begin{cases} X & Y = X \\ Z & Y \neq X \end{cases}$$

Proof. If $X = \emptyset$, then take

$$\begin{aligned} Z &= \omega \\ D &= \{\langle s, n\rangle \mid s \text{ is inhabited}, n \in \omega\} \end{aligned}$$

One can easily check that these work as required.

For the converse, we first show that $X \neq \omega$, so assume for a contradiction that $X = \omega$. Since $Z \neq X$, we therefore know that there is some $n \in X \setminus Z$. Since $DX = X$, we deduce that there must be some $\langle s, n \rangle \in D$. Now if we regard s as a set, we know that since it is finite we must have $s \neq \omega = X$, so $Ds = Z$. But we also have that $n \in Ds$ giving a contradiction.

Now that we have established that $X \neq \omega$, we know that there is some X' with $X \subsetneq X'$. Now assume further for a contradiction that there is also some X'' such that $X'' \subsetneq X$. Then $DX'' \subseteq DX \subseteq DX'$ and so $Z \subseteq X \subseteq Z$, giving $Z = X$, a contradiction. Therefore $X = \emptyset$. □

Proposition 5.6.2. *Suppose that α is an applicative automorphism. Then $\alpha(\emptyset) = \emptyset$.*

Proof. Let D be as in the first part of the proof of the previous proposition, and let R be a realizer for α as an applicative morphism. Let $D' = (\lambda x).R\alpha(D)x$. Then for any $Y \in \mathcal{P}(\omega)$,

$$\begin{aligned} D'Y &= R\alpha(D)Y \\ &= R\alpha(D)\alpha(\alpha^{-1}(Y)) \\ &= \alpha(D\alpha^{-1}(Y)) \\ &= \begin{cases} \alpha(\emptyset) & \alpha^{-1}(Y) = \emptyset \\ \alpha(\omega) & \alpha^{-1}(Y) \neq \emptyset \end{cases} \\ &= \begin{cases} \alpha(\emptyset) & Y = \alpha(\emptyset) \\ \alpha(\omega) & Y \neq \alpha(\emptyset) \end{cases} \end{aligned}$$

Also, since α is a bijection, we know that $\alpha(\omega) \neq \alpha(\emptyset)$. We deduce from proposition 5.6.1 that $\alpha(\emptyset) = \emptyset$. □

Proposition 5.6.3. *Let $X, Y \in \mathcal{P}(\omega)$. Then $X \subseteq Y$ if and only if there is some $S \in \mathcal{P}(\omega)$ such that $S\emptyset = X$ and $SX = Y$.*

Proof. Assume first that $X \subseteq Y$. Then note that we can take

$$S = \{\langle \emptyset, n\rangle \mid n \in X\} \cup \{\langle \{n\}, m\rangle \mid n \in X, m \in Y\}$$

This is clearly as required.

For the converse assume that S is such that $S\emptyset = X$ and $SX = Y$. Then $\emptyset \subseteq X$ and so $S\emptyset \subseteq SX$, giving that $X \subseteq Y$. □

Proposition 5.6.4. *Suppose that α is an applicative automorphism. Then α is order preserving.*

Proof. Let $X, Y \in \mathcal{P}(\omega)$ be such that $X \subseteq Y$. Then there is some $S \in \mathcal{P}(\omega)$ such that $S\emptyset = X$ and $SX = Y$. Let R be a realizer for α as an applicative morphism and let

$$S' := (\lambda x).RSx$$

Then

$$\begin{aligned} S'\emptyset &= R\alpha(S)\emptyset \\ &= R\alpha(S)\alpha(\emptyset) \\ &= \alpha(S\emptyset) \\ &= \alpha(X) \end{aligned}$$

and

$$\begin{aligned} S'\alpha(X) &= R\alpha(S)\alpha(X) \\ &= \alpha(SX) \\ &= \alpha(Y) \end{aligned}$$

Hence $\alpha(X) \subseteq \alpha(Y)$. □

In particular, since ω is uniquely defined as the top element of $\mathcal{P}(\omega)$, we now know that for any applicative automorphism, α, $\alpha(\omega) = \omega$.

Lemma 5.6.5. *There is an $E \in \mathcal{P}(\omega)$ such that given $X \subseteq \omega$,*

$$EX\{n\} = \begin{cases} \emptyset & n \notin X \\ \omega & n \in X \end{cases}$$

Proof. Let $E = \{\langle\{n\}, \langle\{n\}, m\rangle\rangle | n, m \in \omega\}$ □

Lemma 5.6.6. *There is an $F \in \mathcal{P}(\omega)$ such that for any $Y \subseteq \omega$,*

$$FY = \{n \in \omega | Y\{n\} \neq \emptyset\}$$

Proof. Let $F = \{\langle\{\langle\{n\}, m\rangle\}, n\rangle | n, m \in \omega\} \cup \{\langle\{\langle\emptyset, m\rangle\}, n\rangle | n, m \in \omega\}$.

Suppose first that for some m $\langle\emptyset, m\rangle \in Y$. Then for every n, $m \in Y\{n\}$, so $Y\{n\} \neq \emptyset$. Also we have that for every n, $\langle\{\langle\emptyset, m\rangle\}, n\rangle \in F$ and hence $n \in FY$. But then the result follows.

Now suppose that for every m, $\langle\emptyset, m\rangle \notin Y$.

Assume that there is some $m \in Y\{n\}$. Then we know that $\langle s, m\rangle \in Y$ for some $s \subseteq \{n\}$. But the only such subsets are $\emptyset$ and $\{n\}$, and we have ensured $\langle\emptyset, m\rangle \notin Y$. Hence, $\langle\{n\}, m\rangle \in Y$. This implies that $n \in FY$.

Now assume that $n \in FY$. Then, since we have ensured $\langle\emptyset, m\rangle \notin Y$ for any m, we must have that $\langle\{n\}, m\rangle \in Y$ for some m. But this implies that $Y\{n\} \neq \emptyset$.

Therefore the result also follows in this case, as required. □

Theorem 5.6.7. *The graph model, $\mathcal{P}(\omega)$ is natural.*

Proof. Define

$$\Sigma := \{\langle\emptyset, \emptyset\rangle, \langle\omega, \{\langle\emptyset, \emptyset\rangle\}\rangle\}$$

and let

$$A = \{\langle X, \bar{X}\rangle \mid X \in \mathcal{P}(\omega)\}$$

where $\bar{X}$ is the (standard) function from ω to Σ in $V(\mathcal{P}(\omega))$ given by

$$\bar{X}(n) = \begin{cases} \langle\emptyset,\emptyset\rangle & n \notin X \\ \langle\omega,\{\langle\emptyset,\emptyset\rangle\}\rangle & n \in X \end{cases}$$

Let $\phi(x)$ be the formula over $V(\mathcal{P}(\omega))$ stating that x is the set of functions from ω to Σ. Then we clearly have $V(\mathcal{P}(\omega)) \vDash (\exists! x)\phi(x)$. Also, A clearly satisfies the first two parts of the definition of natural. It remains only to show that $V(\mathcal{P}(\omega)) \vDash \phi(A)$.

Let $b \in V(\mathcal{P}(\omega))$ and suppose that there is a realizer showing that b is a function from ω to Σ. Then, reasoning inside $V(\mathcal{P}(\omega))$, we can find a realizer, e, for $(\forall n \in \bar{\omega})\exists x(x \in \Sigma) \wedge b(n) = x$. But then we must have

$$(e\{n\})_0 = \begin{cases} \emptyset & b(n) = \emptyset \\ \omega & b(n) = \{\langle\emptyset,\emptyset\rangle\} \end{cases}$$

Now we can apply lemma 5.6.6 to find the set $X = \{n | (e\{n\})_0 = \omega\}$. Then we must have $\widehat{\bar{X}} = \hat{b}$, and so we can easily find a realizer for $\bar{X} = b$, and hence for $b \in a$. This gives a realizer for b is a function $\omega \to \Sigma$ implies $b \in A$.

Now let $\bar{X} \in A$. Then if E is as in lemma 5.6.5, we have

$$EX\{n\} = \begin{cases} \emptyset & n \notin X \\ \omega & n \in X \end{cases}$$

But we can clearly use this to construct a realizer showing that $\bar{X}$ is indeed a function from ω to Σ.

Therefore we have a realizer for the statement that the elements of A are precisely the functions from ω to Σ, and noting that Σ is fixed by all automorphisms, we deduce that $\mathcal{P}(\omega)$ is natural. □

Theorem 5.6.8. *$\mathcal{P}(\omega)^{\text{c.e.}}$ is natural.*

Proof. Note that any sets we constructed in the above proofs were computably enumerable, and hence we can apply exactly the same proof as before to show that $\mathcal{P}(\omega)^{\text{c.e.}}$ is natural. □

5.6.1 The Automorphisms of $\mathcal{P}(\omega)$ in More Detail

For the case of $\mathcal{P}(\omega)$ we can in fact characterise the weak automorphisms exactly as those that lift in a canonical way from permutations of ω.

Definition 5.6.9. We say that $Y \in \mathcal{P}(\omega)$ is a *successor* of $X \in \mathcal{P}(\omega)$ if $X \subseteq Y$ and there is no $Z \in \mathcal{P}(\omega)$ such that $X \subsetneq Z \subsetneq Y$.

Theorem 5.6.10. *For every applicative automorphism, α, of $\mathcal{P}(\omega)$, there is some permutation $\pi : \omega \to \omega$ such that for all $X \in \mathcal{P}(\omega)$, $\alpha(X) = \{\pi(n) \mid n \in X\}$.*

Proof. Firstly note that the singleton sets are precisely the successors of the empty set. Therefore, since α is order preserving and fixes the empty set, we know that α must also preserve the singletons. Therefore there is some permutation π such that $\alpha(\{n\}) = \{\pi(n)\}$ for all n. Now note that for any n, and any $X \in \mathcal{P}(\omega)$ we have that $n \in X$ if and only if $\{n\} \subseteq X$. Since α and α^{-1} are order preserving we know that $\alpha(\{n\}) \subseteq \alpha(X)$ if and only if $\{n\} \subseteq X$. Then $n \in X$ iff $\{n\} \subseteq X$ iff $\alpha(\{n\}) \subseteq \alpha(X)$ iff $\{\pi(n)\} \subseteq \alpha(X)$ iff $\pi(n) \in \alpha(X)$. So the result follows. □

Note that any such permutation lifts uniquely to a continuous bijection of $\mathcal{P}(\omega)$ and that any representable bijection of a pca gives an applicative automorphism. Hence the group of applicative automorphisms of $\mathcal{P}(\omega)$ is precisely the symmetric group of ω, with action given as in the theorem.

Theorem 5.6.11. *Let π be a permutation of ω such that for every $s, n \in \omega$, $\langle \pi s, \pi(n) \rangle = \pi(\langle s, n \rangle)$ (here πs means think of s as encoding a finite subset of ω and apply π pointwise). Then π lifts to a weak automorphism, α, of $\mathcal{P}(\omega)$.*

Proof. Let π be a permutation satisfying the given condition, with $\alpha : \mathcal{P}(\omega) \to \mathcal{P}(\omega)$

given by $\alpha(X) = \pi X$. Then for any $X, Y \in \mathcal{P}(\omega)$,

$$\begin{aligned}
\alpha(X).\alpha(Y) &= \{n|\langle s,n\rangle \in \alpha(X), s \subseteq \alpha(Y)\} \\
&= \{n|\langle s,n\rangle \in \pi X, s \subseteq \pi Y\} \\
&= \{n|\pi^{-1}(\langle s,n\rangle) \in X, \pi^{-1}s \subseteq Y\} \\
&= \{n|\langle \pi^{-1}s, \pi^{-1}(n)\rangle \in X, \pi^{-1}s \subseteq Y\} \\
&= \{\pi(n)|\langle s,n\rangle \in X, s \subseteq Y\} \\
&= \alpha(X.Y)
\end{aligned}$$

□

In fact this the same condition is necessary for π to lift to an weak automorphism.

Theorem 5.6.12. *Let π be a permutation of ω such that π lifts to a weak automorphism of $\mathcal{P}(\omega)$. Then for any $s, n \in \omega$, $\langle \pi s, \pi(n)\rangle = \pi(\langle s,n\rangle)$.*

Proof. Let π be a permutation of ω that lifts to a weak automorphism of $\mathcal{P}(\omega)$, and let $s, n \in \omega$.

Note that for any m,

$$\{\langle s,n\rangle\}.\{m\} = \begin{cases} \{n\} & m \in s \\ \emptyset & m \notin s \end{cases}$$

Since π lifts to a weak automorphism we know that

$$\{\pi(\langle s,n\rangle)\}.\{\pi(m)\} = \begin{cases} \{\pi(n)\} & m \in s \\ \emptyset & m \notin s \end{cases}$$

Since pairing is surjective there must be $s', n' \in \omega$ such that $\pi(\langle s,n\rangle) = \langle s', n'\rangle$. Hence,

$$\{\pi(\langle s,n\rangle)\}.\{\pi(m)\} = \begin{cases} \{n'\} & \pi(m) \in s' \\ \emptyset & \pi(m) \notin s' \end{cases}$$

But this implies that $n' = \pi(n)$ and $s' = \pi s$ and so $\pi(\langle s,n\rangle) = \langle \pi s, \pi(n)\rangle$.

□

In [4] the following encodings of finite sets and pairs are chosen and fixed throughout:

A finite set of naturals $a_1, \ldots, a_n$ is encoded as $\sum_{i=1}^{n} 2^{a_i}$ (ie the number whose binary expansion has 1 precisely at the digits a_i).

A pair $\langle n, m \rangle$ is encoded as $\frac{1}{2}(n+m)(n+m+1)+m$.

Proposition 5.6.13. *For any a, b, we have $a' < \langle a, b \rangle$ for all $a' \in a$ and $b \leq \langle a, b \rangle$ with equality iff $a = \emptyset$ and $b = 0$ (in which case $\langle a, b \rangle = 0$).*

Proof. Let $a' \in a$. Then $a \geq 2^{a'} > a'$. Note in particular that this implies $a \geq 1$.

$$\begin{aligned}
\langle a, b \rangle &= \frac{1}{2}(a+b)(a+b+1)+b \\
&\geq \frac{1}{2}a(a+1) \\
&\geq \frac{1}{2}a(1+1) \\
&\geq a \\
&> a'
\end{aligned}$$

As mentioned above, if $a \neq \emptyset$, then $a \geq 1$, and so

$$\begin{aligned}
\langle a, b \rangle &= \frac{1}{2}(a+b)(a+b+1)+b \\
&\geq 1+b \\
&> b
\end{aligned}$$

If $b \geq 1$, then

$$\begin{aligned}
\langle a, b \rangle &= \frac{1}{2}(a+b)(a+b+1)+b \\
&\geq 1+b \\
&> b
\end{aligned}$$

But the only case remaining is $a = \emptyset$ and $b = 0$, as required. □

Theorem 5.6.14. *For the encodings given above, there are no nontrivial permutations of the naturals satisfying the condition given in theorem 5.6.12.*

Proof. Let $\pi : \omega \to \omega$ be a bijection such that for all $n, m \in \omega$, $\pi(\langle n, m\rangle) = \langle \pi n, \pi(m)\rangle$ (where πn means think of n as a finite subset and apply π pointwise).

Note that $\langle \emptyset, 0\rangle = 0$. Hence, $\pi(0) = \pi(\langle \emptyset, 0\rangle) = \langle \emptyset, \pi(0)\rangle$. Therefore, if $\pi(0) = m$, then we know that

$$\begin{aligned} m &= \frac{1}{2}(0+m)(0+m+1)+m \\ &= \frac{1}{2}m(m+3) \end{aligned}$$

and so either $m = 0$, or

$$\begin{aligned} \frac{1}{2}(m+3) &= 1 \\ m+1 &= 0 \end{aligned}$$

but this gives a contradiction since $m \in \omega$. So $\pi(0) = 0$.

Now, for $n > 0$, by proposition 5.6.13, we have that $n = \langle a, b\rangle$ with $b < n$ and for each $a' \in a$, $a < n$. By induction we can therefore assume that $\pi(b) = b$ and for each $a' \in a$, $\pi(a') = a'$. But then it follows $\pi(n) = \pi(\langle a, b\rangle) = \langle \pi a, \pi(b)\rangle = \langle a, b\rangle = n$.

Hence by induction we can see that π must be the identity.

□

However, if we carefully construct the encoding of pairs, we can ensure that there are plenty of permutations satisfying the condition required.

Theorem 5.6.15. *There is a (computable) encoding of pairs, $(,)$, such that for any permutation σ of ω, there is a permutation, π satisfying the condition given in 5.6.12 such that $\pi((\emptyset, \langle n, 0\rangle)) = (\emptyset, \langle \sigma(n), 0\rangle)$, where $\langle , \rangle$ is the usual encoding.*

Proof. We define $(,)$ in stages. Let $I_n = \{\langle i, j\rangle | i \leq n, j \in \omega\}$

We first decide which pairs, (a, b), will have value in I_0

Let $(\{\langle 0, a_1\rangle, \ldots, \langle 0, a_n\rangle\}, \langle 0, b\rangle)$ be encoded by the value $\langle 0, \langle\{a_1, \ldots, a_n\}, b\rangle\rangle$.

Now at stage n, we assume by induction that we have found pairs (a, b) for values in I_n. We now find pairs that will have values in $I_{n+1} \setminus I_n$.

Note that we can (computably) enumerate pairs (a, b) such that $a \subseteq I_{n+1}$, $b \in I_{n+1}$, and either $a \nsubseteq I_n$ or $b \notin I_n$. Note further that we can ensure each such pair is listed only once, such that $(a_0, b_0) = (\emptyset, \langle n+1, 0\rangle)$, and such that $a_{k+1} \subseteq I_n \cup \{\langle n+1, i\rangle | i \leq k\}$ and $b_k \in I_n \cup \{\langle n+1, i\rangle | i \leq k\}$. Let (a_k, b_k) be such an enumeration. Now assign (a_k, b_k) the value $\langle n+1, k\rangle$.

We can see that this does define a computable bijective encoding of pairs.$\{\langle n+1, i\rangle | i < k\}$

If we are given a permutation $\sigma : \omega \to \omega$, then note that we can define a permutation π, as required by first ensuring $\pi((\emptyset, \langle n, 0\rangle)) = (\emptyset, \langle \sigma(n)\rangle)$, and then extending by induction.

□

As an immediate corollary we get the following result noted before, eg in [5].

Corollary 5.6.16. *There are versions of the graph model, $\mathcal{P}(\omega)$, (using different encodings of pairs) that are non-isomorphic*

Proof. We have shown that one encoding gives a graph model with no weak automorphisms, and one gives a graph model with uncountably many weak automorphisms. There clearly can be no weak isomorphisms between these copies of the graph model.

□

5.7 Some Automorphisms of D_∞

We show that automorphisms (in the topological sense) of a directed complete partial order (dcpo) D lift in a canonical way to automorphisms (in the pca sense) of D_∞.

Theorem 5.7.1. *Let $\alpha : D \to D$ be an automorphism of a directed complete partial order, D. Then there is a pca automorphism $\tilde{\alpha} : D_\infty \to D_\infty$ such that $\tilde{\alpha}$ restricted to D is equal to α.*

Proof. We first define automorphisms $\alpha_i : D_i \to D_i$ $i \in \mathbb{N}$.

Let $\alpha_0 = \alpha$.

If α_i is already defined, let $\alpha_{i+1}(d) = \alpha_i \circ d \circ \alpha_i^{-1}$.

We can clearly see that each α_i is an automorphism of D_i.

We now show by induction that for each i, $\psi_{i+1}(\alpha_{i+1}) = \alpha_i$.

For $i = 0$, and for any $d \in D_0$

$$\begin{aligned}
\psi_1(\alpha_1)(d) &= \psi_0 \circ \alpha_1 \circ \varphi_0(d) \\
&= \psi_0 \circ \alpha_1(\varphi_0(d)) \\
&= \psi_0(\alpha_0 \circ \varphi_0(d) \circ \alpha_0^{-1}) \\
&= \alpha_0 \circ \varphi_0(d) \circ \alpha_0^{-1}(\perp) \\
&= \alpha_0(\varphi_0(d)(\alpha_0^{-1}(\perp))) \\
&= \alpha_0(d)
\end{aligned}$$

Now assume that $\psi_{i+1}(\alpha_{i+1}) = \alpha_i$ and note that we can also assume $\psi_{i+1}(\alpha_{i+1}^{-1}) = \alpha_i^{-1}$. Then for any $d \in D_i$,

$$\begin{aligned}
\psi_{i+2}(\alpha_{i+2})(d) &= \psi_{i+1} \circ \alpha_{i+2} \circ \varphi_{i+1}(d) \\
&= \psi_{i+1} \circ \alpha_{i+2}(\varphi_{i+1}(d)) \\
&= \psi_{i+1}(\alpha_{i+1} \circ \varphi_{i+1}(d) \circ \alpha_{i+1}^{-1}) \\
&= \psi_i \circ \alpha_{i+1} \circ \varphi_{i+1}(d) \circ \alpha_{i+1}^{-1} \circ \varphi_i \\
&= \psi_i \circ \alpha_{i+1} \circ \varphi_i \circ d \circ \psi_i \circ \alpha_{i+1}^{-1} \circ \varphi_i \\
&= \psi_{i+1}(\alpha_{i+1}) \circ d \circ \psi_{i+1}(\alpha_{i+1}^{-1}) \\
&= \alpha_i \circ d \circ \alpha_i^{-1} \\
&= \alpha_{i+1}(d)
\end{aligned}$$

But this implies that $\tilde{\alpha} = (\perp, \alpha_1, \alpha_2, \ldots)$ is an element of D_∞. We can therefore consider it as a function on D_∞ by application.

Note that this operation preserves composition in the sense that if β is also an automorphism on D, then for any $(d_i)_{i\in\mathbb{N}} \in D_\infty$,

$$\begin{array}{rcl}\tilde{\alpha}.(\tilde{\beta}.d) & = & \tilde{\alpha}.(\sup\limits_i \beta_i(d_i)) \\ & = & \sup\limits_i(\tilde{\alpha}.\beta_i(d_i))) \\ & = & \sup\limits_i(\sup\limits_j \alpha_j(\beta_i(d_i))_j) \\ & = & \sup\limits_i \alpha_i(\beta_i(d_i)) \\ & = & \sup\limits_i(\alpha \circ \beta)_i(d_i) \\ & = & \widetilde{(\alpha \circ \beta)}.d\end{array}$$

This then implies that $\widetilde{\alpha^{-1}}$ is the inverse of $\tilde{\alpha}$, and hence $\tilde{\alpha}$ is a bijection.

We finally need to show that $\tilde{\alpha}$ preserves application. Let $d, d' \in D_\infty$. Then,

$$\begin{array}{rcl}(\tilde{\alpha}.d).(\tilde{\alpha}.d') & = & \sup\limits_i(\tilde{\alpha}.d)_{i+1}(\tilde{\alpha}.d')_i \\ & = & \sup\limits_i(\alpha_{i+1}(d_{i+1})(\alpha_i(d'_i))) \\ & = & \sup\limits_i(\alpha_i \circ d_{i+1} \circ \alpha_i^{-1}(\alpha_i(d'_i))) \\ & = & \sup\limits_i(\alpha_i(d_{i+1}(d'_i))) \\ & = & \sup\limits_i(\alpha_i(\sup\limits_j d_{j+1}(d'_j))_i) \\ & = & \tilde{\alpha}.(d.d')\end{array}$$

So $\tilde{\alpha}$ is an automorphism, as required. □

5.8 Automorphisms of Term Models

Recall from chapter 2 the term models built from $\Lambda(C)$ and $\mathrm{CL}(C)$.

Let $\alpha : C \to C$ be a permutation of C. Then α lifts to a permutation of $\Lambda(C)$ and $\mathrm{CL}(C)$ via induction (say that α fixes λ-terms in $\Lambda(C)$ and s and k in $\mathrm{CL}(C)$). Since the constants play no role in β-reduction or w-reduction this implies that α lifts to a strong automorphism of the term models defined in section 2.5.3.

This gives us an example of a pca that is *not* natural.

Proposition 5.8.1. *The term model $\mathcal{T}$ defined by quotienting* $\mathrm{CL}(\mathbb{N})$ *by w-equivalence is not natural.*

Proof. There are uncountably many permutations on $\mathbb{N}$ but $\mathcal{T}$ is countable, so we get a contradiction by corollary 5.3.5. □

In fact even very simple strong automorphisms fail to be representable.

Proposition 5.8.2. *Given $n, m \in \mathbb{N}$ such that $n \neq m$ the transposition of m and n is not representable in $\mathcal{T}$.*

Proof. This follows from lemma 2.5.22. □

This gives another proof of proposition 5.8.1 since we get a contradiction with corollary 5.3.3.

Chapter 6

Symmetric Models

6.1 Introduction

Permutation models were introduced by Fraenkel and Mostowski to show that a variation of **ZF**, **ZFA** does not prove the axiom of choice. **ZFA** differs from **ZF** in that it allows a set of *atoms* in addition to sets. In Fraenkel-Mostowski models there is an infinite set of atoms that are indistinguishable, resulting in the failure of the axiom of choice.

On developing forcing, Cohen in [11] produced a proof based on similar techniques showing that the axiom of choice is independent of **ZF** itself. A variation of Cohen's proof based on boolean valued models was developed by Scott and Solovay and Vopěnka and is described in [6].

In this chapter we show that like boolean valued models, realizability models can also be adapted to give *symmetric realizability models*. We will also demonstrate the use of these symmetric models by giving a proof that countable choice is independent of **CZF** (and in fact **IZF**).

We will use strong automorphisms (definition 5.1.2) throughout this chapter. Since the other definitions aren't used in this chapter, we will often refer to them just as automorphisms. We will also assume that the constants $\mathbf{p}$, $\mathbf{p}_0$, $\mathbf{p}_0$, $\underline{0}$ and $\underline{1}$ are constructed from

$\mathbf{s}$ and $\mathbf{k}$ and so are preserved by strong automorphisms. Hence theorem 5.2.5 applies throughout.

6.2 Definitions

Let G be a group. Then we have the following definitions.

Definition 6.2.1. A class, Γ, is a *filter* if

1. $G \in \Gamma$
2. whenever H and K are in Γ, we have $H \cap K \in \Gamma$
3. whenever $H \in \Gamma$ and $H \leq K$, we have $K \in \Gamma$

Definition 6.2.2. A filter Γ is *set generated* if there is some set S such that for every $H \subseteq G$, $H \in \Gamma$ if and only if there is some $K \in S$ such that $K \leq H$.

Definition 6.2.3. A class Γ is a *normal filter* if it is a filter and if in addition, whenever $H \in \Gamma$ and $g \in G$, we have $gHg^{-1} \in \Gamma$.

Example 6.2.4. Let G be a group acting on a set X. Let S be the set of subgroups of the form $\mathrm{Stab}_G(x_1) \cap \ldots \mathrm{Stab}_G(x_n)$, where $x_1, \ldots, x_n \in X$. Then S is closed under binary intersection, and generates a normal filter, called the filter of *finite support relative to* X. If G also acts on another set Y, then we say $X' \subseteq X$ is a *support* for $y \in Y$ if every $g \in G$ that fixes X' pointwise also fixes y. If there is a finite such X', we say y is of *finite support* relative to X. $y \in Y$ is of finite support relative to X if and only if $\mathrm{Stab}_G(y) \in \Gamma$.

Remark 6.2.5. *If we are working constructively then it is important to clarify what we mean by finite. For finite support, the correct notion is referred to in [3] as* finitely enumerable. *A set is finitely enumerable if it is the image of a set of size n for some $n \in \omega$.*

Example 6.2.6. For any group, G, the set Γ containing only G is a filter. Now if G acts on a set, X, we can see that $\mathrm{Stab}_G(x) \in \Gamma$ precisely when x is invariant, ie fixed by all elements of G.

Let $\mathcal{A}$ be a pca, and let G be a subgroup of the group of (strong) automorphisms of $\mathcal{A}$.

Then recall that G acts on $V(\mathcal{A})$ by the following inductive definition. Given $\alpha \in G$, and $a \in V(\mathcal{A})$,

$$\alpha(a) = \{\langle \alpha(e), \alpha(b) \rangle \mid \langle e, b \rangle \in a\}$$

Given a group G, and a normal filter Γ we can now define the subclass $V^\Gamma(\mathcal{A})$ of $V(\mathcal{A})$ consisting of hereditarily symmetric sets. That is, define $V^\Gamma(\mathcal{A})$ using an inductive definition so that it is the smallest class satisfying the following.

$$V^\Gamma(\mathcal{A}) := \{a \in V(\mathcal{A}) \mid \mathrm{Stab}_G(a) \in \Gamma \wedge a \subseteq \mathcal{A} \times V^\Gamma(\mathcal{A})\}$$

$V^\Gamma(\mathcal{A})$ inherits realizability for atomic formulas from $V(\mathcal{A})$. That is, $V^\Gamma(\mathcal{A})$ is the realizability model with the following relations:

$$\begin{aligned}
e \Vdash a \in b \quad &\text{iff} \quad (\exists e', e'', c)\; e \leq \mathbf{p}e'e'' \wedge \langle e', c \rangle \in b \;\wedge e'' \Vdash a = c \\
e \Vdash a = b \quad &\text{iff} \quad (\exists e', e'')e \leq \mathbf{p}e'e'' \wedge (\forall \langle f, c \rangle \in a)e'f \Vdash c \in b \wedge \\
&\qquad\qquad (\forall \langle f, c \rangle \in b)e''f \Vdash c \in a \\
e \Vdash (\forall x \in a)\phi(x) \quad &\text{iff} \quad (\forall \langle f, b \rangle \in a)e.f \Vdash \phi(b) \\
e \Vdash (\exists x \in a)\phi(x) \quad &\text{iff} \quad (\exists e', e'')e \leq \mathbf{p}e'e'' \wedge (\exists \langle e', b \rangle \in a)e'' \Vdash \phi(b)
\end{aligned}$$

Also note the following proposition

Proposition 6.2.7. *G acts on $V^\Gamma(\mathcal{A})$*

Proof. It is enough to show that for every $\alpha \in G$ and $a \in V^\Gamma(\mathcal{A})$,

$$\alpha(a) \in V^\Gamma(\mathcal{A})$$

Note firstly that for every $\langle e, b\rangle \in \alpha(a)$, we have that $\langle \alpha^{-1}(e), \alpha^{-1}(b)\rangle \in a$. Hence $\alpha^{-1}(b) \in V^\Gamma(\mathcal{A})$. By induction we may assume therefore that $b = \alpha(\alpha^{-1}(b)) \in V^\Gamma(\mathcal{A})$. It remains to show that $\mathrm{Stab}_G(\alpha(a)) \in \Gamma$.

Let $\mathrm{Stab}_G(a) = H$. Then since Γ is normal we know that $H' := \alpha H \alpha^{-1} \in \Gamma$. Let $\beta' \in H'$. Then $\beta' = \alpha \circ \beta \circ \alpha^{-1}$, where $\beta \in H$. Therefore

$$\begin{aligned} \beta'(\alpha(a)) &= \alpha \circ \beta\alpha^{-1}(\alpha(a)) \\ &= \alpha(\beta(a)) \\ &= \alpha(a) \end{aligned}$$

We have shown that $H' \subseteq \mathrm{Stab}_G(\alpha(a))$. Hence $\mathrm{Stab}_G(\alpha(a)) \in \Gamma$ as required. □

It is also important to note that realizability is preserved by automorphisms (theorem 5.2.5).

6.3 Soundness Theorem

We aim towards the following theorem.

Theorem 6.3.1. *Suppose that ϕ is an axiom of* **CZF**. *Then $V^\Gamma(\mathcal{A}) \models \phi$.*

Definition 6.3.2. If $H \in \Gamma$ and $a \in V(\mathcal{A})$, we define the closure $\mathrm{Cl}_H(a)$ of a over H as follows.

$$\mathrm{Cl}_H(a) := \{\langle \alpha(e), \alpha(b)\rangle \mid \langle e, b\rangle \in a, \alpha \in H\}$$

Lemma 6.3.3. *Suppose that $a \in V(\mathcal{A})$, and that for every $\langle e, b\rangle \in a$ we have $b \in V^\Gamma(\mathcal{A})$. Then for any $H \in \Gamma$, $\mathrm{Cl}_H(a) \in V^\Gamma(\mathcal{A})$.*

Proof. Note that every element of $\mathrm{Cl}_H(a)$ is of the form $\langle \alpha(e), \alpha(b)\rangle$ where $\langle e, b\rangle \in a$. We know by assumption that $b \in V^\Gamma(\mathcal{A})$ and hence also that $\alpha(b) \in V^\Gamma(\mathcal{A})$. It remains only to show therefore that $\mathrm{Stab}_G(\mathrm{Cl}_H(a)) \in \Gamma$. We will do this by showing that $H \leq \mathrm{Stab}_G(\mathrm{Cl}_H(a))$.

Let $\beta \in H$. Any element of $\mathrm{Cl}_H(a)$ is of the form $\langle \alpha(e), \alpha(b) \rangle$ where $\langle e, b \rangle \in a$ and $\alpha \in H$. Then

$$\langle \beta(\alpha(e)), \beta(\alpha(b)) \rangle = \langle \beta \circ \alpha(e), \beta \circ \alpha(b) \rangle$$

Since H is a subgroup, $\alpha \circ \beta \in H$ and hence $\langle \beta(\alpha(e)), \beta(\alpha(b)) \rangle \in \mathrm{Cl}_H(a)$. We have shown therefore that $\beta(\mathrm{Cl}_H(a)) \subseteq \mathrm{Cl}_H(a)$, but similarly $\mathrm{Cl}_H(a) \subseteq \beta(\mathrm{Cl}_H(a))$. Hence $\mathrm{Cl}_H(a) = \beta(\mathrm{Cl}_H(a))$ and so $\beta \in \mathrm{Stab}_G(\mathrm{Cl}_H(a))$ as required. □

Proof of theorem 6.3.1 We now show that the axioms of **CZF** hold in $V^\Gamma(\mathcal{A})$ and that power set and full separation hold if they do so in the background universe.

Firstly note that the proof of extensionality and $\in$-induction carry through the same as in chapter 4. It remains to check infinity, bounded separation, strong collection, subset collection and union.

Binary Intersection As in theorem 4.3.7 we show the soundness of the binary intersection axiom rather than bounded separation. Following the proof of theorem 4.3.7 we construct a set B such that every element of B is of the form $\langle \mathbf{p}ef, x \rangle$ where $\langle e, x \rangle \in X$ and $f \Vdash x \in Y$. We now let $H = \mathrm{Stab}_G(X) \cap \mathrm{Stab}_G(Y)$ and let

$$B' := \mathrm{Cl}_H(B)$$

By lemma 6.3.3 we have that $B' \in V^\Gamma(\mathcal{A})$. Also, since $B \subseteq B'$, we can use the same proof as in 4.3.7 to construct a realizer for

$$X \cap Y \subseteq B'$$

It remains to check that we have a realizer for

$$B' \subseteq X \cap Y$$

So let $\langle \mathbf{p}\alpha(e)\alpha(f), \alpha(x) \rangle \in B'$, where $\langle \mathbf{p}ef, x \rangle \in B$ and $\alpha \in H$. Then $\langle e, x \rangle \in X$ and $f \Vdash x \in Y$. Hence $\langle \alpha(e), \alpha(x) \rangle \in X$ and $\alpha(f) \Vdash \alpha(x) \in Y$. We deduce that

$$(\lambda x).\mathbf{p}(\mathbf{p}(x)_0\mathbf{i}_r)(x)_1 \Vdash (\forall x \in B) x \in X \wedge x \in Y$$

as required.

Infinity Note that we can construct numerals from $\mathbf{s}$ and $\mathbf{k}$ as in chapter 2. Since we are working with strong automorphisms we know that $\mathbf{s}$ and $\mathbf{k}$ are fixed and hence that numerals constructed in this way are fixed by automorphisms. Hence we can assume that in fact $\overline{\omega}$ (and all its elements) are fixed by all automorphisms. Hence it is already an element of $V^{\Gamma}(\mathcal{A})$. The usual proof then shows that it can be used to show the soundness of infinity.

Union Recall from chapter 4

$$\mathrm{Un}(a) := \{\langle \mathbf{p}ef, c\rangle \mid \exists\langle e, b\rangle \in a, \langle f, c\rangle \in b\}$$

We show that if $a \in V^{\Gamma}(\mathcal{A})$, then $\mathrm{Un}(a) \in V^{\Gamma}(\mathcal{A})$. One can easily see that if this is the case then the same soundness proof as before will apply.

Let $\langle \mathbf{p}ef, c\rangle \in \mathrm{Un}(a)$. Then there is b such that $\langle e, b\rangle \in a$ and $\langle f, c\rangle \in b$.

Let $\alpha \in \mathrm{Stab}_G(a)$. Then since $\langle e, b\rangle \in a$ and $\alpha(a) = a$, we know that $\langle \alpha(e), \alpha(b)\rangle \in a$. Furthermore, by definition of the action of G, we know that $\langle alpha(f), \alpha(c)\rangle \in \alpha(b)$. Hence we get that $\langle \mathbf{p}\alpha(e)\alpha(f), \alpha(c)\rangle \in \mathrm{Un}(a)$. But we have now proved $\alpha(\mathrm{Un}(a)) \subseteq \mathrm{Un}(a)$. Similarly $\mathrm{Un}(a) \subseteq \alpha(\mathrm{Un}(a))$ and so $\alpha \in \mathrm{Stab}_G(\mathrm{Un}(a))$. Therefore $\mathrm{Stab}_G(a) \subseteq \mathrm{Stab}_G(\mathrm{Un}(a))$ and so $\mathrm{Stab}_G(a) \in \Gamma$ as required.

Pairing Recall from chapter 4

$$\mathrm{Pair}(a, b) := \{\langle \mathbf{0}, a\rangle, \langle \mathbf{1}, b\rangle\}$$

Suppose that $\alpha \in \mathrm{Stab}_G(a) \cap \mathrm{Stab}_G(b)$. Then we can easily see that

$$\alpha \in \mathrm{Stab}_G(\mathrm{Pair}(a, b))$$

Hence $\mathrm{Pair}(a, b) \in V^{\Gamma}(\mathcal{A})$, and so we can apply the same proof as before.

Strong Collection Suppose that

$$e \Vdash (\forall x \in A)(\exists y)\phi(x, y)$$

Then for each $\langle f, a\rangle \in A$, there is some $b \in V^{\Gamma}(\mathcal{A})$ such that

$$e.f \Vdash \phi(a, b)$$

Hence by strong collection in the background universe there is some C such that for every $\langle f, a\rangle \in A$, there is some $c \in C$ such that c is of the form $\langle \mathbf{p}f(ef), c'\rangle$ where $c' \in V^{\Gamma}(\mathcal{A})$ and

$$e.f \Vdash \phi(a, c')$$

and such that for every $c \in C$ there is some $\langle f, a\rangle \in A$ such that $c = \langle \mathbf{p}f(ef), c'\rangle$ and the above statement holds.

Note in particular that every element of C is of the form $\langle \mathbf{p}f(ef), c'\rangle$ where $c' \in V^{\Gamma}(\mathcal{A})$.

Now suppose that the parameters in ϕ are amongst $d_1, \ldots, d_n$ and let $H := \mathrm{Stab}_G(A) \cap \bigcap_{i=1}^{n} \mathrm{Stab}_G(d_i)$. Note that $H \in \Gamma$. Now let

$$C' := \mathrm{Cl}_H(C)$$

Then we know by lemma 6.3.3 and the above that $C' \in V^{\Gamma}(\mathcal{A})$. Note further that $C \subseteq C'$ and so we can easily show that

$$(\lambda x).\mathbf{p}(\mathbf{p}x(ex))(ex) \Vdash (\exists y \in C')\phi(x, y)$$

It remains only to construct a realizer for $(\forall y \in C)(\exists x \in A)\phi(x, y)$. We claim that this is realized by the identity, I.

Suppose that $c' \in C$. Then we know from the definitions that there are $\langle e, a\rangle \in A$ such that $ef \Vdash \phi(a, c)$, $\alpha \in H$ and

$$c' = \langle \alpha(\mathbf{p}e(ef)), \alpha(c)\rangle$$

Since $\alpha \in \mathrm{Stab}_G(A)$, we know that $\langle \alpha(e), \alpha(a)\rangle \in A$. Furthermore, since α fixes any parameters in ϕ, we know that

$$\alpha(ef) \Vdash \phi(\alpha(a), \alpha(c))$$

Hence $\mathbf{p}\alpha(e)\alpha(ef) \Vdash (\exists x \in A)\phi(x, \alpha(c))$ and so the identity is a realizer of $(\forall y \in C')(\exists x \in A)\phi(x, y)$ as required.

Subset Collection Fix $A, B \in V^\Gamma(\mathcal{A})$. Showing the soundness of subset collection amounts to finding $C \in V^\Gamma(\mathcal{A})$ and a realizer e for

$$\begin{aligned}&e \Vdash (\forall u)((\forall x \in A)(\exists y \in B)\phi(x, y, u) \to\\&\qquad (\exists z \in C)((\forall x \in A)(\exists y \in z)\phi(x, y, u) \wedge (\forall y \in z)(\exists x \in A)\phi(x, y, u)))\end{aligned}$$

This is quite similar to the case of subset collection in the proof of theorem 4.3.6 but with some alterations to ensure that $C \in V^\Gamma(\mathcal{A})$.

We will show this by applying subset collection in the background universe. To this end, note firstly that we can construct $\tilde{B}$ by strong collection such that

$$\tilde{B} = \{\langle \mathbf{p}gh, b\rangle \mid (\exists k)\langle k, b\rangle \in B, (\exists a)\langle g, a\rangle \in A, h \in \mathcal{A}\}$$

Now suppose that f, u are such that $f \in \mathcal{A}$, $u \in V^\Gamma(\mathcal{A})$, and

$$f \Vdash (\forall x \in A)(\exists y \in B)\phi(x, y, u)$$

Then in particular we know that for every $\langle g, a\rangle \in A$, there is some b such that $(fg)_1 \Vdash \phi(a, b, u)$ and $\langle \mathbf{p}g(fg)_1, b\rangle \in \tilde{B}$.

Hence we can apply subset collection in the background universe to find a C' such that whenever the situation above occurs, there is some $c \in C'$ such that for every $\langle g, a\rangle \in A$, there is b such that $\langle \mathbf{p}g(fg)_1, b\rangle \in c$ and such that *every* element of c is of this form.

Note that although $c \in V(\mathcal{A})$ as before, we don't necessarily have that $c \in V^\Gamma(\mathcal{A})$. However, if the parameters of ϕ are amongst $d_1, \ldots, d_n$ and $H = \mathrm{Stab}_G(A) \cap \mathrm{Stab}_G(B) \cap \bigcap_{i=1}^n \mathrm{Stab}_G(d_i) \cap \mathrm{Stab}_G(u)$ then we can take the closure under H. Let

$$c' = \mathrm{Cl}_H(c)$$

Since we know that $c \subseteq c'$ we can easily show that

$$(\lambda x).(\mathbf{p}(\mathbf{p}x(fx)_1)(fx)_1) \Vdash (\forall x \in A)(\exists y \in c')\phi(x, y, u)$$

Now note that every element of c' is of the form $\langle \alpha(\mathbf{p}gh), \alpha(b) \rangle$ where $\alpha \in H$ and there is a such that $\langle g, a \rangle \in A$ and $h \Vdash \phi(a, b, u)$.

Since $\alpha \in \mathrm{Stab}_G(A)$ we know that $\langle \alpha(g), \alpha(a) \rangle \in A$. Since $\alpha \in \mathrm{Stab}_G(u)$ and α fixes any parameters of ϕ, we know furthermore that

$$\alpha(h) \Vdash \phi(\alpha(a), \alpha(b), u)$$

Hence we have that the identity, I is a realizer for $(\forall y \in c')(\exists x \in A)\phi(x, y, u)$.

This only leaves the problem that we need to construct C before being given u and hence we don't have $\mathrm{Stab}_G(u)$. To overcome this we need to use the assumption that Γ is set generated. Let S be a generating set for Γ. We can now construct

$$C := \mathrm{Cl}_G(\{\langle \underline{0}, \mathrm{Cl}_H(c) \rangle \mid c \in C', H \in S, c \subseteq V^\Gamma(\mathcal{A})\})$$

Then, by the above reasoning, C is as required to show the soundness of subset collection.

$\in$-induction The proof for theorem 4.3.6 still holds here.

□

Theorem 6.3.4. *Suppose that full separation holds in the background universe. Then it also holds in $V^\Gamma(\mathcal{A})$.*

Proof. Construct given X and a formula ϕ, construct

$$B := \{\langle \mathbf{p}ef, x\rangle \mid \langle e, x\rangle \in X, f \Vdash \phi\}$$

Then let H be the intersection of X and any parameters appearing in ϕ. Note that if $\alpha \in H$, $\langle e, x\rangle \in X$, and $f \Vdash \phi$ then $\langle \alpha(e), \alpha(x)\rangle \in X$ and $\alpha(f) \Vdash \phi$. Hence $H \subseteq \mathrm{Stab}_G(B)$ and so $B \in V^\Gamma(\mathcal{A})$. One can easily construct a realizer to show that B witnesses this instance of full separation.

□

Theorem 6.3.5. *Suppose that powerset holds in the background universe. Then it also holds in $V^\Gamma(\mathcal{A})$.*

Proof. Note that by lemma 4.3.2 we know that $V^\Gamma(\mathcal{A}) \models a \in b$ implies that the rank of a is less than the rank of b. Hence the following is a set for any $A \in V^\Gamma(\mathcal{A})$:

$$P := \{\langle e, b\rangle \mid e \in \mathcal{A}, b \in V^\Gamma(\mathcal{A}), e \Vdash b \subseteq A\}$$

This is clearly an element of $V^\Gamma(\mathcal{A})$ and is a witness of powerset. □

6.4 Models where Countable Choice Fails

We can use symmetric models to give simple constructive models of set theory where countable choice fails.

This proof is based loosely on the existing proof that AC_ω is independent of **ZF**, which uses symmetric models and appears, for example in [17] and in [6].

Another result in this area is that a very weak version of **AC**, $\mathbf{AC}_{\omega,2}$ is independent of **IZF**. This states that every multivalued function from ω to 2 has a choice function. Note that this follows from excluded middle. Its independence from **IZF** can be shown using

Heyting-valued models (see [15]). Rathjen and Ming-Chen in [10] used Lifschitz realizability to show that $\mathbf{AC}_{\omega,2}$ is even independent of **IZF** if one adds a form of Church's thesis.

The proof in this section only shows the independence of $\mathbf{AC}_{\omega}$ but it has the advantage over some of the others that it requires only **CZF** as the background universe. It also illustrates some of the ideas that will appear in chapters 7 and 8.

Theorem 6.4.1. *Countable choice is independent of* **CZF**.

Let

$$X := \{\xi_i \mid i \in \omega\}$$

be a countable set of atoms, and let $\mathrm{CL}(X)$ be the set of terms over X. Let $\mathcal{T}$ be the term model obtained by quotienting out $\mathrm{CL}(X)$ by w-reduction as in chapter 2.

Let G be the group of automorphisms arising from permutations of X, and let Γ be the normal filter of finite support on X.

For each $n \in \omega$, define $\tilde{n} \in V^{\Gamma}(\mathcal{A})$ as follows:

$$\tilde{n} := \{\langle \xi_m, \overline{m} \mid m < n\}$$

We then get the following lemma

Lemma 6.4.2. *Suppose that $\alpha \in G$ and ξ_m are such that $\alpha(\xi_m) \neq \xi_m$. Then for $n > m$ and $n > 2$, $V^{\Gamma}(\mathcal{A}) \not\models \alpha(\tilde{n}) = \tilde{n}$.*

Proof. Suppose that $e \vdash \alpha(\tilde{n}) = \tilde{n}$. Then, by the definition of realizability of equality, we know that there is some $\langle ((e)_1 \xi_m)_0, b \rangle \in \alpha(\tilde{n})$ such that $((e)_1 \xi_m)_1 \Vdash \alpha(\overline{m}) = b$. By the definition of $\tilde{n}$ and the fact that α fixes $\overline{m}$, we can deduce that $b = \overline{m}$ and hence that $((e)_1 \xi_m)_0 = \alpha(\xi_m)$. Let m' be such that $m' \neq m$ and $m' < n$. Then we similarly get that $((e)_1 \xi_{m'})_0 = \alpha(\xi_{m'}) \neq \alpha(\xi_m)$. Therefore by lemma 2.5.22 we get a contradiction. □

Now let

$$R := \{\langle \underline{n}, (\overline{n}, \alpha(\tilde{n})) \rangle \mid n \in \omega, \alpha \in G\}$$

Then we can clearly find a realizers for

$$(\forall x \in R)(\exists n \in \omega)(\exists y)x = (n, y)$$

and

$$(\forall n \in \omega)(\exists x \in R)(\exists y)x = (n, y)$$

Suppose that there is some $R' \in V^\Gamma(\mathcal{A})$ such that there are realizers for

$$R' \subseteq R$$

and

$$(\forall n \in \omega)(\forall x, y)((n, x) \in R' \wedge (n, y) \in R' \rightarrow x = y)$$

Let N be large enough that $\mathrm{Stab}_G(\xi_1) \cap \ldots \cap \mathrm{Stab}_G(\xi_N) \subseteq \mathrm{Stab}_G(R')$. Then there is some $r \in R'$ and $\alpha \in G$ such that

$$V^\Gamma(\mathcal{A}) \models r = (\overline{N+2}, \alpha(\widetilde{N+2}))$$

Hence

$$V^\Gamma(\mathcal{A}) \models \alpha^{-1}(r) = (\overline{N+2}, \widetilde{N+2})$$

Note that

$$\alpha(\widetilde{N+2}) = \{\langle \alpha(\xi_n), \overline{n}\rangle \mid n < N+2\}$$

and hence that there must be $m, n < N+2$ such that $\alpha(\xi_m) = \xi_{m'}$, $\alpha(\xi_n) = \xi_{n'}$ and $m', n' \geq N$. Hence there is an automorphism $\beta \in \mathrm{Stab}_G(R')$ transposing $\xi_{n'}$ and $\xi_{m'}$. Furthermore $\beta(\alpha(\widetilde{N+2})) \neq \alpha(\widetilde{N+2})$, and so $\alpha^{-1} \circ \beta \circ \alpha(\widetilde{N+2}) \neq \widetilde{N+2}$. Applying 6.4.2, this gives that

$$V^\Gamma(\mathcal{A}) \not\models \alpha^{-1} \circ \beta \circ \alpha(\widetilde{N+2}) = \widetilde{N+2}$$

We use this to derive a contradiction.

Since $\beta \in \mathrm{Stab}_G(R')$, we have that $\beta(r) \in R'$ and hence

$$V^\Gamma(\mathcal{A}) \models (\overline{N+2}, \beta(\alpha(\widetilde{N+2}))) \in R'$$

Using the realizer for $(\forall n \in \omega)(\exists x, y)((n, x) \in R' \wedge (n, y) \in R' \to x = y)$ we deduce that

$$V^{\Gamma}(\mathcal{A}) \models \alpha(\widetilde{N+2}) = \beta(\alpha(\widetilde{N+2}))$$

and hence

$$V^{\Gamma}(\mathcal{A}) \models \widetilde{N+2} = \alpha^{-1}(\beta(\alpha(\widetilde{N+2})))$$

giving a contradiction as required.

□

Chapter 7

Symmetric Models over Proper Classes

In this section we combine the techniques of chapters 6 and 4 and produce symmetric models where the copca we're working over may be a proper class. Proving the soundness theorem for **CZF**, in particular the soundness of subset collection presents several technical challenges. To overcome this we start by giving definitions necessary for handling collections of automorphisms acting on a proper class. Furthermore, we put an additional restriction on the normal filters that can be used and work over a background universe of **ZF**. Unfortunately we were not able to prove many of the lemmas that appear here over weaker set theories.

7.1 Permutation Families

In order to ensure that the theorems in this chapter can be formalised in **ZF** we make the following definitions. These allow us to handle proper classes of automorphisms acting on proper classes in a way that makes sense in set theory. The following definition is best thought of as a generalisation of symmetric group, where the group can act on a proper class M.

Definition 7.1.1. Given a class, M, a *permutation family* on M indexed by a class, I, is a formula $\phi(x, y, z)$ such that

1. $$(\forall x \in I)(\forall y \in M)(\exists! z \in M)(\phi(x,y,z))$$

2. $$(\forall x \in I)(\forall z \in M)(\exists! y \in M)(\phi(x,y,z))$$

3. $$(\forall x, x' \in I)(\exists x'' \in I)(\forall y, z \in M)(\phi(x'', y, z) \leftrightarrow (\exists z' \in M)(\phi(x, y, z') \wedge \phi(x', z', z)))$$

4. $$(\exists x \in I)(\forall y \in M)\phi(x,y,y)$$

5. $$(\forall x \in I)(\exists x' \in I)(\forall y \in M)(\exists z \in M)\phi(x,y,z) \wedge \phi(x',z,y)$$

To make this easier to visualise, we use the following notation.

We write $(\pi_x)_{x\in I}$ for a permutation family, and write $\pi_x(y) = z$ for $\phi(x,y,z)$. We will write $\pi_x = \pi_{x'}$ to mean that for all y in M, $\pi_x(y) = \pi_{x'}(y)$.

We write $\pi_{x''} = \pi_{x'} \circ \pi_x$ to mean that for every y in M, $\pi_{x''}(y) = \pi_{x'}(\pi_x(y))$. Note that from the definition, for any $x, x' \in I$ there is x'' such that $\pi_{x''} = \pi_{x'} \circ \pi_x$.

We write $\pi_{x'} = \pi_x^{-1}$ to mean that for every y in M, $\pi_{x'} \circ \pi_x(y) = y$ and $\pi_x \circ \pi_{x'}(y) = y$. Note that by the definition, for every $x \in I$, there is $x' \in I$ such that $\pi_{x'} = \pi_x^{-1}$.

Definition 7.1.2. Say that $(\pi')_{x\in I'}$ is a *sub permutation family* of $(\pi)_{x\in I}$ if I' is a subclass of I and $(\pi')_{x\in I'}$ is a permutation family on M indexed by I' and is defined by the same formula $\phi(x,y,z)$ as for $(\pi)_{x\in I}$.

Given two permutation families on M, $(\pi)_{x\in I}$ and $(\pi')_{x\in I'}$, we define the intersection as a the sub permutation family of $(\pi)_{x\in I}$ indexed by

$$\{x \in I \mid (\exists x' \in I')(\forall y \in M)\pi_x(y) = \pi_{x'}(y)\}$$

We now define automorphism families.

Definition 7.1.3. An *automorphism family* of a copca, $\mathcal{A}$ is a permutation family on $\mathcal{A}$ that preserves the order and application of the copca as well as s and $\mathbf{k}$. (So this corresponds to strong automorphisms.)

Permutation families should be regarded as proper class generalisation of symmetric groups. We therefore define notions of orbit and stabiliser.

The following definitions are defined over a permutation family, $G = (\pi_x)_{x \in I}$.

Definition 7.1.4. Given $y \in M$, define the *orbit* of y as the class

$$\mathrm{Orb}_{\mathrm{G}}(y) := \{z \in M \mid (\exists x \in I)\pi_x(y) = z\}$$

Definition 7.1.5. Given $y \in M$, define $\mathrm{Stab}_G(y)$ as the sub permutation family of G indexed by

$$I' := \{x \in I \mid \pi_x(y) = y\}$$

Definition 7.1.6. We say that G is *locally small* if for every $a \in M$, the orbit of a, $\mathrm{Orb}_{\mathrm{G}}(a)$, is a set.

Lemma 7.1.7. *Suppose that G is locally small. Then for every set $A \subseteq M$, there is some G' a subgroup of G (ie in particular G' is a set) and set $A' \supseteq A$ such that*

1. *for every $a \in A'$ and every $g \in G'$, $g(a) \in A'$*
2. *for every $x \in I$, there is $x' \in I$ and $g \in G'$ such that $\pi_{x'}$ fixes every element of A' and π_x factors $\pi_x = \pi_{x'} \circ g$*

Proof. Suppose that $A \subseteq M$. Then define A',

$$A' := \{\pi_x(a) \mid a \in A, x \in I\}$$

Note that this is equal to $\bigcup_{a \in A} \mathrm{Orb}_{\mathrm{G}}(a)$ and so in particular it is a set by local smallness of G.

Now define

$$S := \{f : A' \to M \mid (\exists x \in I)(\forall a \in A')f(a) = \pi_x(a)\}$$

Note that this is a subset of the set of functions from A' to $\bigcup_{a \in A'} \mathrm{Orb}_{\mathrm{G}}(a)$ and so in particular it is a set.

By collection on S, there is some *set* $I' \subseteq I$ such that for every f in S there is some x in I' such that for every $a \in A'$, $f(a) = \pi_x(a)$.

Now note that we can find some set $I'' \supseteq I'$ such that I'' is closed under composition and inverses. That is, for every x, x' in I'' there is some x'' in I'' such that $\pi_{x''} = \pi_x \circ \pi_{x'}$, and similarly for inverses. We can view I'' as a group, G' by quotienting out by the equivalence relation given by $x \sim x'$ if for every $y \in M$, $\pi_x(y) = \pi_{x'}(y)$. (Recall that under this condition we think of π_x and $\pi_{x'}$ as already being equal.)

We now show that A' and G' are as required.

Suppose that $x \in I$. Then there is some f in S such that for every a in A', $\pi_x(a) = f(a)$. Hence there is some $h \in G'$ such that for every a in A', $\pi_x(a) = h(a)$. Now viewing h as an element of the permutation family, there is x' such that

$$\pi_{x'} := \pi_x \circ h^{-1}$$

We can now clearly see that the conditions are satisfied. □

Given an automorphism family, $G = (\pi_x)_{x \in I}$, we can lift this to a permutation family G' of $V(\mathcal{A})$ in the same way as for automorphism groups.

Recall that in chapter 6 we made quite heavy use of the closure of an element of $V(\mathcal{A})$ (definition 6.3.2). We can similarly define closure here and show that it has similar properties to before.

Definition 7.1.8. Given a sub automorphism family, $H := (\pi')_{x \in I'}$ of G, and $a \in V(\mathcal{A})$, we define the closure as follows

$$\mathrm{Cl}_H(a) := \{\langle \pi'_x(e), \pi'_x(b)\rangle \mid x \in I', \langle e, b\rangle \in a\}$$

Note that as it stands, $\mathrm{Cl}_H(a)$ may be a proper class. We will show that under the assumption that G is locally small we can show that it is a set.

Proposition 7.1.9. *Suppose that G is locally small on $\mathcal{A}$. Then G is also locally small on $V(\mathcal{A})$.*

Proof. For every $a \in V(\mathcal{A})$, we define the support $\mathrm{Supp}(a)$ recursively as follows

$$\mathrm{Supp}(a) := \bigcup\{\{e\} \cup \mathrm{Supp}(b) \mid \langle e, b\rangle \in a\}$$

Let $A := \mathrm{Supp}(a)$. Then note that we can define $V_\alpha(A)$ recursively by

$$V_{\alpha+1}(A) := \mathcal{P}(V_\alpha(A))$$
$$V_\lambda := \bigcup_{\beta\in\lambda} V_\beta(A)$$

Then by induction we see that for every α, and for every $b \in V_\alpha(A)$ we have that $\mathrm{Orb}_{\mathrm{G}}(b) \subseteq V_\alpha(A)$.

But there must be some α such that $a \in V_\alpha(A)$ and so $\mathrm{Orb}_{\mathrm{G}}(a) \subseteq V_\alpha(A)$. However $V_\alpha(A)$ is a set (by induction and power set), and so $\mathrm{Orb}_{\mathrm{G}}(a)$ must also be a set.

Hence G is locally small. □

If G is locally small, then we can consider stabilisers and closures "locally" as follows.

Proposition 7.1.10. *Suppose that $A \subseteq M$ and H are sets such that H is a subgroup of G which acts on A, and that every element of G factors as an element of H and something fixing A pointwise (as in lemma 7.1.7). Then for $a \in A$,*

$$\mathrm{Stab}_G(a) = \{\pi_x \circ h \mid (\forall a' \in A)\pi_x(a') = a', h \in \mathrm{Stab}_H(a), x \in I\}$$

Proof. Suppose that $x \in I$ is such that for all a' in A, $\pi_x(a') = a'$. Then clearly $\pi_x(a) = a$, and so if $h \in \mathrm{Stab}_H(a)$, then $\pi_x \circ h \in \mathrm{Stab}_G(a)$.

Now suppose that $\pi_{x'} \in \mathrm{Stab}_G(a)$. Then there are π_x and h such that for all $a' \in A$, $\pi_x(a') = a'$, $h \in H$ and $\pi_{x'} = \pi_x \circ h$. Hence $h(a) = \pi_{x'}^{-1}(a) = a$. That is $h \in \mathrm{Stab}_H(a)$. □

Proposition 7.1.11. *Suppose that $A \subseteq \mathcal{A}$ and H are sets such that H is a subgroup of G which acts on A, and that every element of G factors as an element of H and something fixing A pointwise (as in lemma 7.1.7), and that $G' \subseteq G$ is a sub permutation family of G. Let $H' := H \cap G'$. Then H' is a subgroup of H and for any $a \in V(A)$, $\mathrm{Cl}_{G'}(a) = \mathrm{Cl}_{H'}(a)$.*

Proof. Suppose that $\langle \pi_x(e), \pi_x(b) \rangle \in \mathrm{Cl}_{G'}(a)$ where $\langle e, b \rangle \in a$. Then let $\pi_x = \pi_{x'} \circ h$ where $h \in H$ and $\pi_{x'}$ fixes A pointwise. Note in particular that $\pi_{x'}$ must also fix $V(A)$ pointwise (by induction). Hence $\langle \pi_x(e), \pi_x(b) \rangle = \langle h(e), h(b) \rangle$, and so $\langle \pi_x(e), \pi_x(b) \rangle \in \mathrm{Cl}_{H'}(a)$. But we can clearly see that $\mathrm{Cl}_{H'}(a) \subseteq \mathrm{Cl}_{G'}(a)$, and so we get the result. □

Note in particular that $\mathrm{Cl}_{H'}(a)$ is a set, so we can deduce that $\mathrm{Cl}_{G'}(a)$ is a set.

We now define an analogous notion to filter to that in chapter 6. In fact this definition is closer to that of generating set for the earlier definition of normal filter.

Because we require normal filters, we first show how to define conjugates of permutation families.

Definition 7.1.12. Suppose that H is a sub permutation family of $G = (\pi_x)_{x \in I}$ and that $g = \pi_x$ for some $x \in I$. Suppose that H is indexed by $I' \subseteq I$. Then we write gHg^{-1} to mean the sub permutation family of G indexed by

$$I'' := \{x'' \in I \mid (\exists x' \in I')\pi_{x''} = \pi_x \circ \pi_{x'} \circ \pi_x^{-1}\}$$

Definition 7.1.13. Let $G := (\pi_x)_{x \in I}$ be a permutation family. Then a *filter family*, Γ on G is a formula $\phi(x, y)$, and class J such that for any $x \in J$, the class $\{y \mid \phi(x, y)\}$ is a subclass of I. Given a sub permutation family, $H = (\pi'_x)_{x \in I'}$ of G, we write $H \in \Gamma$ to mean

$$(\exists x \in J)(\forall y \in I)\phi(x, y) \to (\exists y' \in I')(\forall z \in M)\pi_y(z) = \pi'_{y'}(z)$$

We require, furthermore, that

1. $G \in \Gamma$

2. for sub permutation families H, H' of G, if $H, H' \in \Gamma$ then $H \cap H' \in \Gamma$

3. if H is a sub permutation family of G and $g \in G$, then $H \in \Gamma$ implies that $gHg^{-1} \in \Gamma$

Definition 7.1.14. Let $G := (\pi_x)_{x \in I}$ be a permutation family on M. Then we define the *finite support* filter family as follows. Let J be the class of finite subsets of M. Then let $\phi(x, y)$ state that y consists of the n elements $y_1, \ldots, y_n$ and that for $i = 1, \ldots, n$, $\pi_x(y_i) = y_i$.

Proposition 7.1.15. *Suppose that H is a sub automorphism family of G and $a \subseteq \mathcal{A} \times V^\Gamma(\mathcal{A})$. Then $H \subseteq \mathrm{Stab}_H(\mathrm{Cl}_H(a))$, and hence if $H \in \Gamma$ then $\mathrm{Cl}_H(a) \in V^\Gamma(\mathcal{A})$.*

7.2 Soundness Theorem

We now define the realizability model and show that we have soundness for **CZF**. We work throughout in a background universe of **ZF**.

Definition 7.2.1. Given a uniform copca $\mathcal{A}$, an automorphism family $G = (\alpha_x)_{x \in I}$ on $\mathcal{A}$ and a filter family Γ on G such that for every $e \in \mathcal{A}$, $\mathrm{Stab}_G(e) \in \Gamma$, we define the class $V^\Gamma(\mathcal{A})$, recursively in the usual way. That is $a \in V^\Gamma(\mathcal{A})$ if $a \subseteq V^\Gamma(\mathcal{A})$ and $\mathrm{Stab}_G(a) \in \Gamma$.

Theorem 7.2.2. *$V^\Gamma(\mathcal{A})$ satisfies the axioms of* **CZF**.

The general idea to adapt the proof of theorem 6.3.1 by looking carefully at the proof.

For union, pairing, binary intersection, strong collection and infinity the proof of theorem 6.3.1 still holds here because when constructing the necessary sets, we never needed to assume that $\mathcal{A}$ was a set. Furthermore, the proof of soundness for extensionality and $\in$-induction for theorem 4.3.6 still applies here unchanged.

This only leaves subset collection, which we prove below.

Recall from the soundness theorem in chapter 4 that given a formula $\phi(x, u, y)$ and sets $A, B \in V(\mathcal{A})$ we constructed a set C satisfying the following property. Whenever there is $u \in V(\mathcal{A})$ and $e \in \mathcal{A}$ such that $e \Vdash (\forall x \in A)(\exists y \in B)\phi(x, u, y)$ there is $\langle \mathbf{0}, q\rangle \in C$ such that for every $\langle f, a\rangle \in A$ there is $\langle f, b\rangle \in q$ such that there exists $e', e'' \in \mathcal{A}$ with $ef \leq \mathbf{p}e'e''$, $\langle e', b\rangle \in B$ and $e'' \Vdash \phi(a, u, b)$, and such that every element of q is of this form.

Firstly note that we can perform the same construction as before but over $V^{\Gamma}(\mathcal{A})$ rather than $V(\mathcal{A})$. This only leaves the problem that we haven't guaranteed that the q with $\langle \mathbf{0}, q\rangle \in C$ are elements of $V^{\Gamma}(\mathcal{A})$. We fix this with basically the same idea as for (set sized) symmetric models as in 6. The main problem here is that since $\mathcal{A}$ may be a proper class, we are not able to construct q so that the elements of q are of the form $\langle \mathbf{p}fe'', b\rangle$ where $e'' \Vdash \phi(a, u, b)$. To overcome this we use the additional assumption that $\mathrm{Stab}_G(e) \in \Gamma$ for $e \in \mathcal{A}$. We will also make use of power set and full separation as well as the condition that G is locally small.

Let $S := \mathrm{Supp}(A) \cup \mathrm{Supp}(B) \cup \mathrm{Supp}(C)$. Then apply local smallness to S to get $S' \supseteq S$ and $G' \leq G$ such that G' and S' are sets such that G' acts on S' and every element of G factors as something fixing S' and an element of G'.

We can now use power set and full separation to construct the set Γ' where

$$\Gamma' := \{H' \leq G' \mid (\exists H \in \Gamma)(g \in H' \leftrightarrow (\exists x \in I)(((\forall y \in S')\pi_x(y) = y) \wedge \pi_x \circ g \in H))\}$$

Note that we have constructed this so that for any $H \in \Gamma$ there is some $H' \in \Gamma'$ such that for any q with $\langle \mathbf{0}, q\rangle \in C$ we have that $\mathrm{Cl}_{H'}(q) = \mathrm{Cl}_H(q)$.

Now construct C' as

$$C' := \mathrm{Cl}_G(\{\langle \mathbf{0}, \mathrm{Cl}_{H'}(q)\rangle \mid \langle \mathbf{0}, q\rangle \in D', H' \in \Gamma'\})$$

We can easily see from construction that this is an element of $V^{\Gamma}(\mathcal{A})$. It only remains to check that this can be used to show the soundness of subset collection.

Suppose that $u \in V^\Gamma(\mathcal{A})$ and $e \in \mathcal{A}$ with $e \Vdash (\forall x \in A)(\exists y \in B)\phi(x, u, y)$. Suppose that the parameters in $\phi(x, u, y)$ are amongst $c_1, \ldots, c_n$ and let

$$H := \mathrm{Stab}_G(A) \cap \mathrm{Stab}_G(B) \cap \bigcap_{i=1}^{n} \mathrm{Stab}_G(c_i) \cap \mathrm{Stab}_G(e) \cap \mathrm{Stab}_G(u)$$

Since we required that $\mathrm{Stab}_G(e) \in \Gamma$, we know that $H \in \Gamma$. Let q be such that $\langle \mathbf{0}, q\rangle \in C$ and such that for every $\langle f, a\rangle \in A$ there is $\langle f, b\rangle \in q$ and $e', e'' \in \mathcal{A}$ such that $ef \leq \mathbf{p}e'e''$, $\langle e', b\rangle \in B$ and $e'' \Vdash \phi(a, u, b)$. We will show that we can use $\mathrm{Cl}_H(q)$ to witness subset collection. Since $q \subseteq \mathrm{Cl}_H(q)$, we can use the same proof as in 4 to show that $(\forall x \in A)(\exists y \in q)\phi(x, u, y)$.

Now suppose that $\langle f, b\rangle \in q$. Then we know that there must be some $\langle f, a\rangle \in A$ and some $e', e'' \in \mathcal{A}$ such that $ef \leq \mathbf{p}e'e''$, $\langle e', b\rangle \in B$ and $e'' \Vdash \phi(a, u, b)$. Now if $\alpha \in H$, we know that $\langle \alpha(e'), \alpha(b)\rangle \in B$, and $\alpha(e'') \Vdash \phi(\alpha(a), u, \alpha(b))$. Furthermore, we know that

$$e\alpha(f) = \alpha(ef) \leq \mathbf{p}\alpha(e')\alpha(e'')$$

We deduce that we can find a realizer for $(\forall y \in \mathrm{Cl}_H(q))(\exists x \in A)\phi(x, u, y)$ as required.

7.3 The Weak Presentation Axiom

In [25], Moerdijk and Palmgren introduced a new choice principle that they called the axiom of multiple choice, $\mathbf{AMC}$. This principle was introduced for being sufficient to prove some useful results and yet stable under various category theoretic constructions such as internal sheaf constructions.

In the more recent [38], van den Berg and Moerdijk showed that in fact, in the presence of another axiom $\mathbf{WS}$, a weaker choice principle suffices to prove the set compactness theorem, a theorem related to inductive definitions and related results about formal topologies. In [38] the new, weaker axiom is referred to as the axiom of multiple choice. However, in this chapter we will follow [3] and refer to the new axiom as $\mathbf{wPAx}$ and use $\mathbf{AMC}$ to refer to the original axiom of multiple choice. In [38], it is also shown that

$\mathbf{wPAx}$ is stable under various category theoretic constructions including exact completion, realizability, and sheaves.

In [31], Rathjen notes that the axiom $\mathbf{AMC}$ follows from the axiom $\mathbf{SVC}$ studied by Blass in [9] and hence that $\mathbf{AMC}$ must hold in most commonly studied models of $\mathbf{ZF}$. He also shows that assuming the existence of certain large cardinals, it is possible to construct a model of $\mathbf{ZF}$ where $\mathbf{AMC}$ and $\mathbf{wPAx}$ fail.

In the next section we will construct a model of $\mathbf{CZF}$ where $\mathbf{AMC}$ fails. We will assume classical logic in the background universe, and hence the final result is only proved on the assumption that $\mathbf{ZF}$ is consistent.

In the below, let $\mathrm{mv}(X)$ be the class of multivalued functions on X. That is, the class of sets R of ordered pairs such that for every $(x, y) \in R$, $x \in X$, and for every $x \in X$ there is some y such that $(x, y) \in R$. Given $R \in \mathrm{mv}(X)$, we say that C is a *cover* for R if is satisfies

$$(\forall x \in X)(\exists y \in C)((x, y) \in R) \wedge (\forall y \in C)(\exists x \in X)((x, y) \in R)$$

Definition 7.3.1. A set Y is a *small cover base* for X if for every $R \in \mathrm{mv}(X)$, there is some cover C of R such that for some $y \in Y$ there is a surjection $f : y \twoheadrightarrow C$.

The *weak presentation axiom*, $\mathbf{wPAx}$, states that every set has a small cover base.

Definition 7.3.2. A set Y is a *small collection family* if for each $y \in Y$, Y is a small cover base for y.

The *axiom of multiple choice*, $\mathbf{AMC}$, states that every set is an element of a small collection family.

7.4 Independence of $\mathbf{wPAx}$

We show that $\mathbf{wPAx}$ is independent of $\mathbf{CZF}$. In order to do this we need to assume a background universe of $\mathbf{ZF}$ throughout this section. Hence, formally the theorem that we get is the following.

Theorem 7.4.1. *Suppose* $\mathbf{ZF}$ *is consistent. Then* $\mathbf{CZF} + \neg\mathbf{wPAx}$ *is consistent.*

We do this by constructing, in $\mathbf{ZF}$, a copca, $\mathcal{T}$, based on the term models and a set based class of automorphisms, G. We then know that this gives a realizability model satisfying the axioms of $\mathbf{CZF}$. We then show that ω does not have a small cover base in this model.

Define the class C of constants as the following disjoint union

$$\begin{aligned} C_0 &:= \{a \mid (\exists a_0, a_1)(a = \langle a_0, a_1\rangle \wedge a_0 \in a_1)\} \\ C &:= \{\mathbf{0}\} \amalg C_0 \end{aligned}$$

We then construct the closed term model using these constants as in example 4.2.2. However we now define the ordering by saying that $a \leq b$ when either $a = b$ or $b = \mathbf{0}$. We can identify this with a sub copca of the opca in example 4.2.2 by considering $\mathbf{0}$ as $\emptyset$ and $a \in C_0$ as the singleton $\{a\}$. This sub copca is upwards closed in the original copca and hence must be uniform by proposition 4.2.3.

Call this copca $\mathcal{T}$.

Let G be the class of automorphisms, α of $\mathcal{T}$ such that $\alpha(\mathbf{0}) = \mathbf{0}$ and for every $a \in C_0$, $\mathrm{Second}(\alpha(a)) = \mathrm{Second}(a)$, and such that the elements of C not fixed by α form a set. That is, we think of C_0 as the disjoint union of columns of size $|a_1|$ for any set a_1, and G is those automorphisms that preserve each column.

Formally, we define G as an automorphism family $(\pi_x)_{x \in I}$ as follows. Let I be the class of pairs $\langle A, (\tau_a)_{a\in A}\rangle$ such that for every a in A, τ_a is a permutation of a. If $x := \langle A, (\tau_a)_{a\in A}\rangle$, then we define its value on C_0 as follows

$$\pi_x(a) := \begin{cases} \langle \tau_{a_1}(a_0), a_1\rangle & \text{if } a_1 \in A \\ a & \text{otherwise} \end{cases}$$

We then extend this to $\mathcal{T}$ by setting $\pi_x(\mathbf{0}) = \mathbf{0}$, $\pi_x(\mathbf{s}) = \mathbf{s}$, $\pi_x(\mathbf{k}) = \mathbf{k}$ and requiring that it preserves application.

We now show that $\mathcal{T}$ is locally small. Note that for any constant $a = \langle a_0, a_1\rangle$, the orbit of a under G is the set $\{\langle a', a_1\rangle \mid a' \in a_1\}$. Since any element e of $\mathcal{T}$ contains only finitely many constants we can easily see that the orbit of e under G is also a set, so G is locally small.

Let Γ be the finite support filter.

So $V^{\Gamma}(\mathcal{T})$ is a realizability model for **CZF**.

We now prove that **wPAx** does not hold in $V^{\Gamma}(\mathcal{T})$. Suppose $V^{\Gamma}(\mathcal{T})$ realizes that a is a small cover base for ω. Let b be a set (in our background universe) of cardinality greater than any element of a. We construct R such that $V^{\Gamma}(\mathcal{T})$ realizes $R \in \mathrm{mv}(\omega)$, but such that for any $c \in V^{G}(\mathcal{T})$ such that $V^{G}(\mathcal{T})$ realizes an image of c covers R, the cardinality of c is at least that of b. Thus we derive a contradiction and show that ω does not have a small cover base in $V^{G}(\mathcal{T})$.

Let a and b be as above, noting that we can assume without loss of generality that b has a countably infinite subset $\{b_n\}_{n \in \omega}$. For each $n \in \omega$, let $c_n := \langle b_n, b \rangle$. We now construct R.

Following the proof of theorem 6.4.1, for each $n \in \omega$, define $\tilde{n}$ as follows

$$\tilde{n} = \{\langle \mathbf{c_m}, \overline{m} \rangle \mid m < n\}$$

Note that the proof of lemma 6.4.2 still applies here, and so we get the following.

Lemma 7.4.2. *Suppose that $\alpha \in G$ and $\mathbf{c_m}$ are such that $\alpha(\mathbf{c_m}) \neq \mathbf{c_m}$. Then for $n > m$ and $n > 2$, $V^{\Gamma}(\mathcal{A}) \not\models \alpha(\tilde{n}) = \tilde{n}$.*

Now define R

$$R = \{\langle \underline{n}, \alpha(\tilde{n}) \rangle \mid n \in \omega, \alpha \in G\}$$

(Note that this is a set since G is locally small).

Now suppose $c, f, d \in V^{G}(\mathcal{T})$ are such that we have realizers for $f : c \twoheadrightarrow d$ and d covers R.

Let $H \leq G$ be the intersection of the stabilisers of c, f, d and also any realizers that we have seen so far. Then since these are of finite support, we know that for n high enough, the orbit under H of $\mathbf{c_n}$ is the column $\{\langle y, b\rangle \mid y \in b\}$ minus some finite subset. One can check that since we ensured b has a countable subset, this implies that for n high enough $|\operatorname{Orb_H}(\alpha(\tilde{n}))| = |b|$, for any $\alpha \in G$.

Now working inside $V^G(\mathcal{T})$, we know that there is some $m \in d$ such that $V(\mathcal{T}) \models \langle \overline{n}, m\rangle \in R$. Hence there must be some $\langle e, l\rangle \in c$ and $\langle g, (l', m)\rangle \in f$ (in our background universe), such that we have a realizer for $m = \alpha(\tilde{n})$ for some $\alpha \in G$ and a realizer for $l' = l$. Now let $\beta \in H$, and suppose $\beta(l) = l$. Then using the realizer for f being well defined, we can extract a realizer for $\beta(m) = m$, and hence a realizer for $\beta(\alpha(\tilde{n})) = \alpha(\tilde{n})$. Since we know from the above that $|\operatorname{Orb_H}(\alpha(\tilde{n}))| = |b|$ and $V^G(\mathcal{T}) \models \alpha(\tilde{n}) = \beta(\alpha(\tilde{n})) \to \alpha(\tilde{n}) = \beta(\alpha(\tilde{n}))$, this implies that $|\operatorname{Orb_H}(l)| = |b|$. Since we know that H fixes c, this means that the cardinality of c is at least $|b|$. But this is exactly what we require to derive our contradiction, and so we have proved the result.

□

Chapter 8

Failure of the Existence Property for CZF

8.1 Existence Properties

Constructive theories are known for having metamathematical properties that are often not shared by stronger classical theories such as **ZFC**. The principles below are amongst the most well known of these properties.

Recall that constructive mathematicians read logical symbols according to the BHK interpretation. For the constructive mathematician, in order to know the disjunction $\phi \vee \psi$, one must either know ϕ or know ψ. They therefore often expect their formal theories to have the following property.

Definition 8.1.1. A theory, T has the *disjunction property* (DP) if whenever $T \vdash \phi \vee \psi$, either $T \vdash \phi$ or $T \vdash \psi$.

In order to know $(\exists x)\phi(x)$, the constructive mathematician must be able to "construct" some witness a such that one knows $\phi(a)$. We certainly know what it means to construct an element of ω: we must be able to write down an actual natural number. We also know what it means to construct a function $\mathbb{N} \to \mathbb{N}$: we must be able to able to find (a number encoding) an algorithm whose graph is that function. Hence the constructive mathematician expects their formal theories to have the following properties. In the definitions below we assume that T has a constant ω such that T proves that ω is the natural numbers and for each n a constant $\overline{n}$ such that T proves $\overline{0}$ is empty and $\overline{n+1}$ is the successor of $\overline{n}$. For any theory that could "reasonably" be called a set theory, there will be at least a conservative extension with this property.

Definition 8.1.2. T has the *numerical existence property* (NEP) if whenever $T \vdash (\exists x \in \omega)\phi(x)$, there is some natural number n such that

$$T \vdash \phi(\overline{n})$$

Definition 8.1.3. T is closed under *Church's Rule* (CR) if whenever $T \vdash (\forall x \in \omega)(\exists y \in \omega)\phi(x, y)$, there is some natural number e such that

$$T \vdash (\forall x \in \omega)\phi(x, \{\overline{e}\}(x))$$

(where $\{e\}(x)$ denotes the result of applying the eth recursive function to x)

What it means to construct higher order objects, such as sets is not always as clear, at least for relational theories. However, a common interpretation of this is that they should at least be definable, in the sense below.

Definition 8.1.4. T has the *existence property* (EP) if whenever $T \vdash (\exists x)\phi(x)$, there is some formula $\chi(x)$ that only has free variable x such that

$$T \vdash (\exists! x)\phi(x) \wedge \chi(x)$$

The properties DP, NEP, and CR work extremely well as characterisations of constructive formal theories. None can hold for consistent recursively axiomatisable theories that have excluded middle, but on the other hand they hold for a rich variety of constructive theories.

In [26] Friedman and Myhill showed that $\mathbf{IZF}_R$ (that is, **IZF** with replacement instead of collection), has the existence property. In [27], Myhill showed the set theory $\mathbf{CST}^-$

also has EP and also that both $\mathbf{CST}^-$ and $\mathbf{CST}$ have DP and NEP, leaving open whether $\mathbf{CST}$ has EP. In [13] Friedman and Ščedrov showed that $\mathbf{IZF}_R + \mathbf{RDC}$ has EP, establishing that even set theories with choice principles can have EP.

Beeson then developed q-realizability, allowing him to show in [5] that NEP, DP, and CR hold for $\mathbf{IZF}$ and $\mathbf{IZF} + \mathbf{RDC}$. Rathjen developed realizability with truth based partly on Beeson's methods to show in [30] and [34] that DP, NEP, CR and other properties hold for a wide variety of intuitionistic set theories including $\mathbf{CZF}$, $\mathbf{CZF}+\mathbf{REA}$, $\mathbf{IZF}$, $\mathbf{IZF} + \mathbf{REA}$ with any combination of the axioms $\mathbf{MP}$, $\mathbf{AC}_\omega$, $\mathbf{DC}$, $\mathbf{RDC}$ and $\mathbf{PAx}$.

One can see that EP does not work so well as a characterisation of constructive theories as the other properties we have seen. As remarked in [30] EP can hold for classical theories, even extensions of $\mathbf{ZFC}$. On the other hand, Friedman and Ščedrov showed in [14] that $\mathbf{IZF}$ *does not* have EP.

Friedman and Ščedrov's proof that EP fails for $\mathbf{IZF}$ makes use of full separation and collection. Since $\mathbf{IZF}_R$ does have EP, it might seem reasonable to think that collection is responsible for the failure of EP and the use of full separation is only incidental. However due to recent work by Rathjen, this turns out not to be the case. Set theories with collection but only bounded separation can have EP.

In [35] Rathjen defined the following two variations on EP,

Definition 8.1.5. 1. T has the *weak existence property*, wEP, if whenever

$$T \vdash (\exists x)\phi(x)$$

there is some formula $\chi(x)$ having at most the free variable x such that

$$\begin{aligned} T &\vdash (\exists! x)\chi(x) \\ T &\vdash (\forall x)(\chi(x) \rightarrow (\exists u) u \in x) \\ T &\vdash (\forall x)(\chi(x) \rightarrow (\forall u \in x)\phi(u)) \end{aligned}$$

2. T has the *uniform weak existence property*, uwEP, if whenever

$$T \vdash (\forall u)(\exists x)\phi(u, x)$$

there is some formula $\chi(u, x)$ having at most the free variables u, x such that

$$\begin{aligned} T &\vdash (\forall u)(\exists ! x)\chi(u, x) \\ T &\vdash (\forall u)(\forall x)(\chi(u, x) \to (\exists z) z \in x) \\ T &\vdash (\forall u)(\forall x)(\chi(u, x) \to \forall z \in x \phi(u, z)) \end{aligned}$$

As remarked in [35], by analysing Friedman and Ščedrov's proof in [14] one can see that **IZF** doesn't even have wEP. On the other hand any extension of **ZF** has uwEP - consider V_α where α is the least ordinal such that V_α contains a witness.

In [35], Rathjen refers to the theories $\mathbf{CZF}^-$, $\mathbf{CZF}_E$ and $\mathbf{CZF}_{\mathcal{P}}$. $\mathbf{CZF}^-$ is **CZF** without subset collection. $\mathbf{CZF}_E$ is $\mathbf{CZF}^-$ with the exponentiation axiom. $\mathbf{CZF}_{\mathcal{P}}$ is **CZF** together with the power set axiom. All three of these theories have strong collection, and yet Rathjen shows in [35] that all three have uwEP (and hence wEP). In that paper he refers to a paper in preparation where he will show by using this result together with ordinal analysis that these three theories in fact have EP.

$\mathbf{CZF}_{\mathcal{P}}$, which has EP, is simply **IZF** with bounded separation in place of full separation, so the use of full separation in Friedman and Ščedrov's proof must be essential. Furthermore, **CZF** lies between $\mathbf{CZF}_E$ and $\mathbf{CZF}_{\mathcal{P}}$, two theories both satisfying EP and uwEP.

However, due to problems defining witnesses for the fullness axiom, these proofs do not apply to **CZF** itself. Rathjen goes so far as to conjecture in [35] that **CZF** does not even have wEP. In this chapter we prove that this conjecture is correct. **CZF** does not have wEP, and the fullness axiom is responsible.

8.2 Outline of Proof

The main idea is to prove this using a Kripke realizability model. The poset P has three elements laid out as follows:

$$\begin{tikzcd} & \bullet & \\ \bullet \arrow[ur, hook] & & \bullet \arrow[ul, hook'] \end{tikzcd}$$

At the top we have a minor variation on $V(\mathcal{A})$, that we call $V_1(\mathcal{A})$. One of the other two domains is $V_0^\Gamma(\mathcal{A})$, a variation on the symmetric models from chapter 6 that we call *partly symmetric*, and one is a new model of *injectively presented* sets, that we refer to as $V_0^{\mathrm{ip}}(\mathcal{A})$. To satisfy the definition of Kripke realizability models, we must have the following inclusions:

$$\begin{tikzcd}
& V_1(\mathcal{A}) & \\
V_0^{\mathrm{ip}}(\mathcal{A}) \arrow[ur, hook] & & V_0^\Gamma(\mathcal{A}) \arrow[ul, hook']
\end{tikzcd}$$

We will show that the axioms of **CZF** are satisfied at all three points.

The key point is proposition 3.2.3 from chapter 3. This says that realizability is "upwards closed" with respect to P, so that if $V_0^{\mathrm{ip}}(\mathcal{A}) \models \phi(a)$ for some a, then also $V_1(\mathcal{A}) \models \phi(a)$ and if $V_0^\Gamma(\mathcal{A}) \models \phi(b)$, then $V_1(\mathcal{A}) \models \phi(b)$. Hence if $\mathbf{CZF} \vdash (\exists! x)\phi(x)$, then $V_1(\mathcal{A}) \models a = b$. We will use this to get a contradiction.

8.3 Realizability at $V_1(\mathcal{A})$

We start by defining $V_1(\mathcal{A})$. In fact this model is defined so that realizability at $V_1(\mathcal{A})$ is completely equivalent to the realizability of $V(\mathcal{A})$. However, our adjustment will be necessary to get soundness at $V_0^\Gamma(\mathcal{A})$.

We define $V_1(\mathcal{A})$, as follows.

$$\begin{aligned}
V_1(\mathcal{A})_{\alpha+1} &= \mathcal{P}(2 \times |\mathcal{A}| \times V_1(\mathcal{A})_\alpha) \\
V_1(\mathcal{A})_\lambda &= \bigcup_{\beta<\lambda} V_1(\mathcal{A})_\beta \\
V_1(\mathcal{A}) &= \bigcup_{\alpha \in \mathbf{On}} V_1(\mathcal{A})_\alpha
\end{aligned}$$

One can think of $V_1(\mathcal{A})$ as things from $V(\mathcal{A})$ with an extra label from 2. Hence given any element of $V_1(\mathcal{A})$ we can think of it as an element of $V(\mathcal{A})$ by ignoring this extra label. Explicitly, we define this recursively as follows. Given $a \in V_1(\mathcal{A})$,

$$a^\circ := \{\langle e, b^\circ \rangle \mid \langle s, e, b \rangle \in a\}$$

We define realizability at $V_1(\mathcal{A})$ as follows

$$\begin{aligned}
e \Vdash_1 a \in b &\quad \text{iff} \quad e \Vdash a^\circ \in b^\circ \\
e \Vdash_1 a = b &\quad \text{iff} \quad e \Vdash a^\circ = b^\circ \\
e \Vdash_1 (\forall x \in a)\phi(x) &\quad \text{iff} \quad e \Vdash (\forall x \in a^\circ)\phi(x) \\
e \Vdash_1 (\exists x \in a)\phi(x) &\quad \text{iff} \quad e \Vdash (\exists x \in a^\circ)\phi(x)
\end{aligned}$$

We then easily get the following proposition.

Proposition 8.3.1. *For any ϕ, $e \Vdash_1 \phi$ if and only if $e \Vdash \phi^\circ$, writing ϕ° to mean the formula obtained by replacing any parameter a in ϕ by a°.*

8.4 Realizability at $V_0^\Gamma(\mathcal{A})$

This model is essentially the same as we saw in chapter 6. The difference is that sets can have “asymmetric” elements that can’t be seen until “moving up to $V_1(\mathcal{A})$.”

Formally we define $V_0^\Gamma(\mathcal{A})$ as follows:

Definition 8.4.1. Given a group G of strong automorphisms of $\mathcal{A}$ and set generated normal filter, Γ, we define the class $V_0^\Gamma(\mathcal{A}) \subseteq V_1(\mathcal{A})$, of *partly symmetric* sets inductively as follows.

Given $a \in V_1(\mathcal{A})$, we say $a \in V_0^\Gamma(\mathcal{A})$ if $\mathrm{Stab}_G(a) \in \Gamma$ and for every $\langle 0, e, b \rangle \in a$ we have $b \in V_0^\Gamma(\mathcal{A})$.

In other words, a, has a “large” stabiliser and every element that has been labelled with 0 is also partly symmetric. Note that this property is preserved by automorphisms, and one can easily show the following.

Proposition 8.4.2. *If* $a \in V_1(\mathcal{A})$ *and* $\alpha \in G$ *is such that* $\alpha(a) = a$*, then* $\alpha(a^\circ) = a^\circ$*.*

In particular if we take an element of $V_0^\Gamma(\mathcal{A})$, then it still has $\mathrm{Stab}_G(a) \in \Gamma$ when we consider it as an element of $V(\mathcal{A})$.

We can now define realizability at $V_0^\Gamma(\mathcal{A})$ as follows

$$\begin{aligned}
e \Vdash_\Gamma a \in b &\quad \text{iff} \quad \exists\langle 0, (e)_0, c\rangle \in b \; (e)_1 \Vdash_\Gamma a = c \\
e \Vdash_\Gamma a = b &\quad \text{iff} \quad \forall\langle 0, f, c\rangle \in a \; (e)_0 f \Vdash_\Gamma c \in b \,\wedge \\
&\qquad\quad\ \forall\langle 0, f, c\rangle \in b \; (e)_1 f \Vdash_\Gamma c \in a \wedge e \Vdash_1 a = b \\
e \Vdash_\Gamma (\exists x \in a)\phi(x) &\quad \text{iff} \quad \exists\langle 0, (e)_0, b\rangle \in a \; (e)_1 \Vdash_\Gamma \phi(b) \\
e \Vdash_\Gamma (\forall x \in a)\phi(x) &\quad \text{iff} \quad \forall\langle 0, f, b\rangle \in a \; e.f \Vdash_\Gamma \phi(b) \text{ and } e \Vdash_1 (\forall x \in a)\phi(x)
\end{aligned}$$

Axioms of Equality

Proposition 8.4.3. *One can construct realizers* $\mathbf{i}_r, \mathbf{i}_s, \mathbf{i}_t, \mathbf{i}_0, \mathbf{i}_1$ *such that*

1. $\mathbf{i}_r \Vdash_\Gamma (\forall x) x = x$
2. $\mathbf{i}_s \Vdash_\Gamma (\forall x, y) x = y \to y = x$
3. $\mathbf{i}_t \Vdash_\Gamma (\forall x, y, z)(x = y \to (y = z \to x = z))$
4. $\mathbf{i}_0 \Vdash_\Gamma (\forall x, y, z)(x = y \to (y \in z \to x \in z))$
5. $\mathbf{i}_1 \Vdash_\Gamma (\forall x, y, z)(x = y \to (z \in x \to z \in y))$

Furthermore, for each formula (without parameters), $\phi(x, z_1, \ldots, z_n)$*, there is* $\mathbf{i}_\phi$ *such that*

$$\mathbf{i}_\phi \Vdash_\Gamma x = y \to (\phi(x, z_1, \ldots, z_n) \to \phi(y, z_1, \ldots, z_n))$$

Proof. We take these realizers from chapter 4 and check that they still work here.

Recall that $\mathbf{i}_r$ is defined such that

$$\begin{aligned} ((\mathbf{i}_r)_0 f)_0 &= f \\ ((\mathbf{i}_r)_0 f)_1 &= \mathbf{i}_r \\ ((\mathbf{i}_r)_1 f)_0 &= f \\ ((\mathbf{i}_r)_1 f)_1 &= \mathbf{i}_r \end{aligned}$$

In order to show $\mathbf{i}_r \Vdash_\Gamma (\forall x) x = x$, by proposition 3.2.4, what we need to show is

1. for every $a \in V_0^\Gamma(\mathcal{A})$, $\mathbf{i}_r \Vdash_\Gamma a = a$
2. for every $a \in V_1(\mathcal{A})$, $\mathbf{i}_r \Vdash_1 a = a$

However note that the second of these conditions is basically the same as the statement $\mathbf{i}_r \Vdash a = a$ in $V(\mathcal{A})$. Hence we only have to check the first condition.

Furthermore, since we already know that for every $a \in V_0^\Gamma(\mathcal{A})$, $\mathbf{i}_r \Vdash_1 a = a$, all we have to check is the following:

$$\forall \langle 0, f, b\rangle \in a\ (\mathbf{i}_r)_0 \Vdash_\Gamma b \in a$$

and

$$\forall \langle 0, f, b\rangle \in a\ (\mathbf{i}_r)_1 \Vdash_\Gamma b \in a$$

We show by induction that these conditions hold for every $a \in V_0^\Gamma(\mathcal{A})$.

Suppose that $\langle 0, f, b\rangle \in a$. Then since this has been labelled with 0, we know that b *is also partly symmetric*. Also b is of strictly lower rank, so we can apply induction here and the above arguments to get

$$\mathbf{i}_r \Vdash_\Gamma b = b$$

However, recall that we defined $\mathbf{i}_r$ using the fixed point theorem so that for all f,

$$\begin{aligned} ((\mathbf{i}_r)_0 f)_0 &= f \\ ((\mathbf{i}_r)_0 f)_1 &= \mathbf{i}_r \end{aligned}$$

(and the same equations for $(\mathbf{i}_r)_1$).

Hence $\mathbf{i}_r \Vdash_\Gamma a = a$ as required.

The proof that $\mathbf{i}_s$ works as required from the proof of proposition 4.3.3 still holds here.

$\mathbf{i}_t$, $\mathbf{i}_0$ and $\mathbf{i}_1$ are also the same as in chapter 4 and the proofs that they are as required can be similarly adapted to this context.

The $\mathbf{i}_\phi$ are constructed by induction on the construction of ϕ. We will explicitly show how to do this for unbounded universal quantifiers and implication since these contain the main ideas for the rest of the induction.

We first show how to construct $\mathbf{i}_{\phi\to\psi}$.

Suppose that $a, b, c \in V_0^\Gamma(\mathcal{A})$, $e \Vdash_\Gamma a = b$ and $f \Vdash_\Gamma \phi(a, c) \to \psi(a, c)$. Suppose further that

$$g \Vdash_\Gamma \phi(b, c)$$

Then

$$\mathbf{i}_\phi(\mathbf{i}_s e)g \Vdash_\Gamma \phi(a, c)$$

and so

$$f(\mathbf{i}_\phi(\mathbf{i}_s e)g) \Vdash_\Gamma \psi(a, c)$$

and finally

$$\mathbf{i}_\psi e(f(\mathbf{i}_\phi(\mathbf{i}_s e)g)) \Vdash_\Gamma \psi(b, c)$$

Hence we can apply similar reasoning for $\Vdash_1$ and for $a, b, c \in V_1(\mathcal{A})$ and use proposition 3.2.4 to show that we can take $\mathbf{i}_{\phi\to\psi}$ to be

$$\mathbf{i}_{\phi\to\psi} := (\lambda x, y, z).\mathbf{i}_\psi x(y(\mathbf{i}_\phi(\mathbf{i}_s x)z))$$

For unbounded universal quantifiers, we show that we can take $\mathbf{i}_{(\forall z)\phi(x,z)} := \mathbf{i}_{\phi(x,z)}$. Suppose that

$$\mathbf{i}_{\phi(x,z)} \Vdash_\Gamma (\forall z)(x = y \to (\phi(x,z) \to \phi(y,z)))$$

and suppose that for $a, b \in V_0^\Gamma(\mathcal{A})$, $e \Vdash_\Gamma a = b$ and

$$f \Vdash_\Gamma (\forall z)\phi(a,z)$$

Then for all $c \in V_0^\Gamma(\mathcal{A})$,

$$f \Vdash_\Gamma \phi(a,c)$$

and so

$$\mathbf{i}_{\phi(x,z)}ef \Vdash_\Gamma \phi(b,c)$$

One can check the corresponding case for $c \in V_1(\mathcal{A})$ to get

$$\mathbf{i}_{\phi(x,z)}ef \Vdash_\Gamma (\forall z)\phi(b,z)$$

as required. □

Proposition 8.4.4. *Bounded and unbounded quantifiers agree. That is, we can find realizers for the following statements.*

1. $(\forall x \in a)\phi(x) \to (\forall x)(x \in a \to \phi(x))$
2. $(\forall x)(x \in a \to \phi(x)) \to (\forall x \in a)\phi(x)$
3. $(\exists x \in a)\phi \to (\exists x)(x \in a \wedge \phi(x))$
4. $(\exists x)(x \in a \wedge \phi(x)) \to (\exists x \in a)\phi(x)$

Proof. The proof of proposition 4.3.4 can be adapted using proposition 3.2.4. □

The following helps illustrate the relation between realizability in $V_0^\Gamma(\mathcal{A})$ and $V(\mathcal{A})$.

Definition 8.4.5. We say that $a \in V_0^\Gamma(\mathcal{A})$ is *(completely) symmetric* if every element of a is of the form

$$\langle 0, e, b \rangle$$

where b is completely symmetric. (This is an inductive definition).

Proposition 8.4.6. *Suppose that ϕ is a bounded formula, all of whose parameters are completely symmetric. Then*

$$e \Vdash_\Gamma \phi \textit{ iff } e \Vdash_1 \phi$$

Proof. When all parameters are completely symmetric the two definitions of realizability agree for everything except unbounded quantifiers. □

We now move on to the proof of soundness for the axioms of set theory.

Theorem 8.4.7. *$V_0^\Gamma(\mathcal{A})$ satisfies the axioms of* **CZF**.

We first deal with what are sometimes referred to as "set existence axioms." That is, axioms of the form

$$(\forall z_1, \ldots, z_n)(\forall x)(\exists y)\phi(x, y, z_1, \ldots, z_n)$$

where the free variables of ϕ are amongst $x, y, z_1, \ldots, z_n$. For these axioms we can apply proposition 3.2.4 to show that it is sufficient to find e such that for every $a, c_1, \ldots, c_n \in V_1(\mathcal{A})$, there is $b \in V_1(\mathcal{A})$ such that

$$e \Vdash_1 \phi(a, b, c_1, \ldots, c_n)$$

and for every $a, c_1, \ldots, c_n \in V_0^\Gamma(\mathcal{A})$ there is $b \in V_0^\Gamma(\mathcal{A})$ such that

$$e \Vdash_\Gamma \phi(a, b, c_1, \ldots, c_n)$$

However, the first of these statements follows from the soundness theorem for $V(\mathcal{A})$. Hence we only have to check the second of these conditions.

For infinity, union, strong collection, pairing, and bounded separation we simply follow the soundness proof in chapter 6 and note that any sets we construct for witnesses of the set existence axioms are still witnesses in $V_1(\mathcal{A})$. For example, consider the case of binary intersection.

Binary Intersection Given sets A and B in $V_0^\Gamma(\mathcal{A})$, form the set C as

$$C := \{\langle 0, \mathbf{p}ef, a\rangle \mid \langle 0, e, a\rangle \in A, f \Vdash_\Gamma a \in B\} \cup \\ \{\langle 1, \mathbf{p}ef, a\rangle \mid \langle n, e, a\rangle \in A, f \Vdash_1 a \in B\}$$

Note that if $\alpha \in \mathrm{Stab}_G(A) \cap \mathrm{Stab}_G(B)$, $\langle 0, e, a\rangle \in A$ and $f \Vdash_\Gamma a \in B$, then we also have that $\langle 0, \alpha(e), \alpha(a)\rangle \in A$ and $\alpha(f) \Vdash_\Gamma \alpha(a) \in B$. Hence if $c = \langle 0, \mathbf{p}ef, a\rangle \in C$ then $\alpha(c) \in C$.

We can also show the analogous result for when $c = \langle 1, \mathbf{p}ef, a\rangle \in C$.

Hence we already have that $\mathrm{Stab}_G(C) \in \Gamma$, and so $C \in V_0^\Gamma(\mathcal{A})$. Hence we can use the usual realizer for binary intersection.

Union We assume that we are given a set $A \in V_0^\Gamma(\mathcal{A})$ and construct a set to show the union axiom.

Let

$$\mathrm{Un}(a) := \{\langle 0, \mathbf{p}ef, b\rangle \mid \langle 0, e, c\rangle \in A, \langle 0, f, b\rangle \in c\} \cup \\ \{\langle 1, \mathbf{p}ef, b\rangle \mid \langle s, e, c\rangle \in A, \langle s', f, b\rangle \in c\}$$

As in chapter 6, this is already a symmetric set so $\mathrm{Un}(a) \in V_0^\Gamma(\mathcal{A})$. Hence we can use the same realizer as in the proof of theorem 4.3.6 to show the soundness of union.

Pair Given $a, b \in V_0^\Gamma(\mathcal{A})$, consider the set

$$\mathrm{Pair}(a, b) := \{\langle 0, \underline{0}, a\rangle, \langle 0, \underline{1}, b\rangle\}$$

We can easily see that this is an element of $V_0^\Gamma(\mathcal{A})$ and that the usual realizer still works.

Infinity We check that the proof in chapter 4 still holds here. We use the same $\bar{\omega}$ as in section 4.4. We write $\bot_v$ for the formula $(\forall x \in v)\bot$, and write $SC(x, y)$ for $y = x \cup \{x\}$ (expressed as a bounded formula).

Note first that we can apply proposition 8.4.6 and theorem 4.3.6 to reduce the problem to finding a realizer for

$$(\forall v)((\bot_v \vee (\exists u \in \bar{\omega})SC(u,v)) \rightarrow v \in \bar{\omega})$$

Since we can clearly find a realizer to show that the empty set is in $\bar{\omega}$, this is reduced to finding a realizer for

$$(\forall v)(\exists u \in \bar{\omega})SC(u,v) \rightarrow v \in \bar{\omega})$$

Hence we assume that there is $a \in V_0^\Gamma(\mathcal{A})$ with $e \Vdash_\Gamma (\exists u \in \bar{\omega})SC(u,a)$. So there must be some n such that $(e)_0 = \underline{n}$ and $(e)_1 \Vdash_\Gamma SC(\overline{n}, a)$.

One can clearly find a realizer for $SC(\overline{n}, \overline{n+1})$ and hence a realizer, using the soundness of extensionality (once we have checked this) for $SC(u,v) \wedge SC(u,v') \rightarrow v = v'$. We can use these to construct a realizer for $a \in \overline{\omega}$, as required.

Strong Collection Assume

$$e \Vdash_\Gamma (\forall x \in A)(\exists y)\phi(x,y)$$

where ϕ is a formula with all parameters partly symmetric.

By strong collection in the background universe, we can find a C_0 such that whenever $\langle 0, f, a \rangle \in A$, there is $\langle 0, f, c \rangle \in C_0$ such that c is partly symmetric and $e.f \Vdash_\Gamma \phi(a,c)$, and such that every element of C_0 is of this form

Similarly, there is a C_1, such that whenever $\langle s, f, a \rangle \in A$, there is $\langle 1, \mathbf{0}, c \rangle \in C_1$ such that $e.f \Vdash_1 \phi(a,c)$ and such that every element of C_1 is of this form.

Let $C = C_0 \cup C_1$, and let

$$H := \mathrm{Stab}_G(A) \cap \bigcap_{i=1}^{n} \mathrm{Stab}_G(d_i)$$

where the parameters in ϕ are amongst $d_1, \ldots, d_n$.

Then as in the proof of theorem 6.3.1 we can use this to prove the soundness of strong collection.

Subset Collection We basically follow the proof in chapter 6.

Suppose that $A, B \in V_0^\Gamma(\mathcal{A})$, and ϕ is a formula with parameters in $V_0^\Gamma(\mathcal{A})$. Then we can form B_0, B_1 and $\tilde{B}$ as follows

$$B_0 = \{\langle 0, \mathbf{p}gh, b\rangle \mid (\exists k)\langle 0, k, b\rangle \in B, (\exists a)\langle 0, g, a\rangle \in A, h \in \mathcal{A}\}$$

$$B_1 = \{\langle 1, \mathbf{p}gh, b\rangle \mid (\exists k)\langle m, k, b\rangle \in B, (\exists a)\langle m, g, a\rangle \in A, h \in \mathcal{A}\}$$

$$\tilde{B} = B_0 \cup B_1$$

Then, analogously to chapter 6, we form C_0 and C_1 such that whenever $f \in \mathcal{A}$ and $u \in V_0^\Gamma(\mathcal{A})$ and

$$f \Vdash_\Gamma (\forall x \in A)(\exists y \in B)\phi(x, y, u)$$

we have that there is some $c \in C_0$ such that for every $\langle 0, g, a\rangle \in A$ there is b such that $\langle 0, \mathbf{p}g(fg)_1, b\rangle \in c$, and whenever $\langle 1, g, a\rangle \in A$, there is b such that $\langle 1, \mathbf{p}g(fg)_1, b\rangle \in c$ and such that every element of c is of one of these forms.

C_1 is defined such that whenever $f \in \mathcal{A}$ and $u \in V_1(\mathcal{A})$ are such that

$$f \Vdash_1 (\forall x \in A)(\exists y \in B)\phi(x, y, u)$$

we have that there is some $c \in C_1$ such that for every $\langle n, g, a\rangle \in A$ there is b, m such that $\langle m, \mathbf{p}g(fg)_1, b\rangle \in c$, and such that every element of c is of this form.

Then define,

$$C_0' := \{\mathrm{Cl}_H(c) \mid c \in C', H \in S, c \subseteq V_0^\Gamma(\mathcal{A})\}$$

(where S is a generating set for Γ, as in chapter 6)

Finally let

$$C := \mathrm{Cl}_G(\{\langle 0, \underline{0}, c\rangle \mid c \in C_0'\} \cup \{\langle 1, \underline{0}, c\rangle \mid c \in C_1\})$$

The same reasoning as before can now be used to show that this is a witness for subset collection.

After checking the set existence axioms, it only remains to check extensionality and $\in$-induction.

Extensionality One can check that the realizers for the formula

$$((\forall x \in a)x \in b) \wedge ((\forall x \in b)x \in a)$$

in fact are already realizers for $a = b$, so we can use the identity to show extensionality (in this form).

$\in$-Induction Suppose that

$$e \Vdash_\Gamma (\forall y)((\forall x \in y)\phi(x) \rightarrow \phi(y))$$

Let $e' = (\lambda x, y).e.x$ and let f be given by the fixed point theorem so that for all g

$$f.g \simeq e'.f.g$$

Note that we know

$$e \Vdash_1 (\forall y)((\forall x \in y)\phi(x) \rightarrow \phi(y))$$

and so by the usual proof we have that for all $a \in V_1(\mathcal{A})$, and all $g \in \mathcal{A}$, $f.g \Vdash_1 \phi(a)$. We claim that for all $a \in V_0^\Gamma(\mathcal{A})$, and all $g \in \mathcal{A}$, $f.g \downarrow$ and $f.g \Vdash_\Gamma \phi(a)$.

So suppose that $a \in V_0^\Gamma(\mathcal{A})$. Then for every $\langle 0, g, b\rangle \in a$, we know by induction in the background universe (since b must be partly symmetric and of strictly lower rank than a) that $f.g \downarrow$ and $f.g \Vdash_\Gamma \phi(b)$. We also know from the above that $f \Vdash_1 (\forall x \in a)\phi(x)$. Hence $f \Vdash_\Gamma (\forall x \in a)\phi(x)$. Thus we have for any $g \in \mathcal{A}$, $e'fg \simeq ef$ (is defined and) realizes $\phi(a)$. But $e'fg \simeq fg$ and so $f.g \Vdash_\Gamma \phi(a)$ as required.

□

Remark 8.4.8. *Note that when we proved the axiom of infinity we used the same standard representation $\overline{\omega}$ as for $V(\mathcal{A})$. Note further that if $f \in \mathcal{A}$ is such that for all $n \in \omega$ there is $m \in \omega$ with $f\underline{n} = \underline{m}$, then the $\overline{f}$ from section 4.4 is completely symmetric and hence we have the same standard representations of the natural numbers and Baire space as we did before.*

8.5 Realizability at $V_0^{\mathrm{ip}}(\mathcal{A})$

For this section we will assume that $\mathcal{A}$ is a non-trivial pca rather than something more general.

We say that $a \in V(\mathcal{A})$ is *injectively presented* if for any $\langle e, b\rangle, \langle e', b'\rangle \in a$, if $e = e'$ then $b = b'$.

Define $V_0^{\mathrm{ip}}(\mathcal{A})$ inductively as follows

$$\begin{aligned} V_0^{\mathrm{ip}}(\mathcal{A})_{\alpha+1} &= \{X \subseteq 2 \times |\mathcal{A}| \times V_0^{\mathrm{ip}}(\mathcal{A})_\alpha \mid X^\circ \text{ is injectively presented}\} \\ V_0^{\mathrm{ip}}(\mathcal{A})_\lambda &= \bigcup_{\beta<\lambda} V_0^{\mathrm{ip}}(\mathcal{A})_\beta \\ V_0^{\mathrm{ip}}(\mathcal{A}) &= \bigcup_{\alpha\in\mathbf{On}} V_0^{\mathrm{ip}}(\mathcal{A})_\alpha \end{aligned}$$

We define realizability at $V_0^{\mathrm{ip}}(\mathcal{A})$ as follows. We write $\Vdash_1$ for realizability at $V(\mathcal{A})$.

$$\begin{aligned} e \Vdash_{\mathrm{ip}} a \in b &\quad\text{iff}\quad (\exists\langle n, (e)_0, c\rangle \in b)(e)_1 \Vdash_{\mathrm{ip}} a = c \\ e \Vdash_{\mathrm{ip}} a = b &\quad\text{iff}\quad (\forall\langle n, f, c\rangle \in a)(e)_0.f \Vdash_{\mathrm{ip}} c \in b \wedge \\ &\qquad\qquad (\forall\langle n, f, c\rangle \in b)(e)_1 f \Vdash_{\mathrm{ip}} c \in a \\ e \Vdash_{\mathrm{ip}} (\exists x \in a)\phi(x) &\quad\text{iff}\quad (\exists\langle n, (e)_0, b\rangle \in a)(e)_1 \Vdash_{\mathrm{ip}} \phi(b) \\ e \Vdash_{\mathrm{ip}} (\forall x \in a)\phi(x) &\quad\text{iff}\quad (\forall\langle n, f, b\rangle \in a)e.f \Vdash_{\mathrm{ip}} \phi(b) \end{aligned}$$

We write $V_0^{\mathrm{ip}}(\mathcal{A}) \models \phi$ to mean that there is some $e \in \mathcal{A}$ such that $e \Vdash_{\mathrm{ip}} \phi$.

Remark 8.5.1. *Note that as at $V_1(\mathcal{A})$ and unlike at $V_0^{\Gamma}(\mathcal{A})$, we completely ignore the extra label from 2. Hence, realizability for bounded formulas is identical in $V_0^{\mathrm{ip}}(\mathcal{A})$ and $V(\mathcal{A})$. We also know that we can work with a° for $a \in V_1(\mathcal{A})$ instead of a itself. For convenience we will often do this.*

Proposition 8.5.2. $V_0^{\mathrm{ip}}(\mathcal{A})$ *satisfies the axioms of equality.*

Proof. This follows by exactly the same proof as for $V_0^{\Gamma}(\mathcal{A})$. □

It remains to check that when we show the soundness of the axioms of **CZF**, we can assume the sets we construct are injectively presented. Since we will require choice in the background universe for this proof, we work over a background universe of **ZFC**.

Theorem 8.5.3. $V_0^{\mathrm{ip}}(\mathcal{A})$ *is sound with respect to the axioms of* **CZF**.

Extensionality This is the same as for $V(\mathcal{A})$.

Bounded Separation Given $A \in V_0^{\mathrm{ip}}(\mathcal{A})$ and a bounded formula, ϕ, consider the set

$$S = \{\langle \mathbf{p}ef, a\rangle \mid \langle e, a\rangle \in A, f \Vdash_{\mathrm{ip}} \phi(a)\}$$

Note that this is injectively presented, since A is, and since realizability for bounded formulas is identical in $V_0^{\mathrm{ip}}(\mathcal{A})$ and $V(\mathcal{A})$, we can see that this can be used to show the soundness of bounded separation.

Pair Given $a, b \in V(\mathcal{A})$, consider

$$P = \{\langle \mathbf{0}, a\rangle, \langle \mathbf{1}, b\rangle\}$$

This is clearly injectively presented, and we can easily use this to show the soundness of pair.

Union Suppose we have been given $a \in V_0^{\mathrm{ip}}(\mathcal{A})$. We want to find an injectively presented set that we can use to show the union axiom. Recall from chapter 4

$$\mathrm{Un}(a) = \{\langle \mathbf{p}ef, c\rangle \mid \langle f, b\rangle \in a, \langle e, c\rangle \in b\}$$

Then this is already injectively presented, so we can use the same proof as for theorem 4.3.6 to show the soundness of union.

Infinity We note that the $\overline{\omega}$ given in section 4.4 is injectively presented, and since no other sets need to be constructed in the proof of infinity, this means we can use the same proof as usual here.

Strong Collection Suppose that

$$e \Vdash_{\text{ip}} (\forall x \in A)(\exists y)\phi(x, y)$$

For each $\langle f, a\rangle \in A$, we can assume by choice in the background universe that we have chosen a $c_f \in V_0^{\text{ip}}(\mathcal{A})$ such that $e.f \Vdash_{\text{ip}} \phi(a, c_f)$ (and hence also $e.f \Vdash_1 \phi(a, c_f)$).

Let

$$C = \{\langle f, c_f\rangle \mid \langle f, a\rangle \in A\}$$

This is clearly injectively presented (since A is).

Note that

$$(\lambda x).\mathbf{p}x(e.x) \Vdash_{\text{ip}} (\forall x \in A)(\exists y \in C)\phi(x, y)$$

and in fact we can use exactly the same realizer again in

$$(\lambda x).\mathbf{p}x(e.x) \Vdash_{\text{ip}} (\forall y \in C)(\exists x \in A)\phi(x, y)$$

(since every element of C is of the form $\langle f, c_f\rangle$ where $\langle f, x\rangle \in A$ and $e.f \Vdash_{\text{ip}} \phi(x, c_f)$). So we get soundness for strong collection.

Subset Collection Suppose we are given sets $A, B \in V_0^{\text{ip}}(\mathcal{A})$. Suppose further that $e \in \mathcal{A}$ is such that for all $\langle f, a\rangle \in A$, $e.f \downarrow$ and there is $\langle e.f, b\rangle \in B$ for some b. In this case we can define

$$\overline{e} := \{\langle f, b\rangle \mid \exists a\langle f, a\rangle \in A, \langle e.f, b\rangle \in B\}$$

(Clearly $\overline{e} \in V_0^{\text{ip}}(\mathcal{A})$).

Now let

$$D := \{\langle e, \overline{e}\rangle \mid e \in \mathcal{A}, \overline{e} \text{ is defined}\}$$

Clearly $D \in V_0^{\mathrm{ip}}(\mathcal{A})$. We shall show that we can use D to show the soundness of subset collection.

Suppose that $u \in V(\mathcal{A})$ is such that

$$e \Vdash_1 (\forall x \in A)(\exists y \in B)\phi(x, y, u)$$

Let

$$e' := (\lambda x).(ex)_0$$

Note that for every $\langle f, a\rangle \in A$, we have $e'.f\downarrow$ and there is (a unique) b with $\langle e'.f, b\rangle \in B$, and so $\langle e', \overline{e'}\rangle \in D$. Furthermore $(e.f)_1 \Vdash_1 \phi(a, b, u)$, and so we can find a realizer for

$$(\forall x \in A)(\exists y \in \overline{e'})\phi(x, y, u) \wedge (\forall y \in \overline{e'})(\exists x \in A)\phi(x, y, u)$$

We can do exactly same if

$$e \Vdash_{\mathrm{ip}} (\forall x \in A)(\exists y \in B)\phi(x, y, u)$$

Hence this does give a proof of the soundness of subset collection.

$\in$-Induction The same proof as for $V_0^{\Gamma}(\mathcal{A})$ still holds here. □

8.6 The pca $\mathcal{T}$

8.6.1 Definition

We will define a term model based on the term model of inside first reduction given in definition 2.5.17.

Recall that this is defined using $\mathrm{CL}(X)$. We set X to be the disjoint union of two sets of constants, ξ_i for $i \in \omega$, and ζ_F for bijections $F : \omega_{>0} \to \omega_{>0}$.

Recall that $\mathrm{CL}(X)$ comes equipped with the following reduction relations.

$$\begin{aligned} \mathbf{s}xyz &\rightarrow xz(yz) \\ \mathbf{k}xy &\rightarrow x \end{aligned}$$

In addition to these, we add a new reduction rule. Below, let $\underline{n}$ be n encoded using s and $\mathbf{k}$ in the usual way. We define ζ-reduction as follows:

$$\zeta_F t \rightarrow \underline{n}$$

where t is a closed term and n is either maximal such that $n = F(m)$ where ξ_m occurs in t or $n = 0$ and no ξ_m occurs in t.

Note that this term rewriting system is ambiguous. That is, there are terms that can be reduced in two incompatible ways. For example, the term $\zeta_{(\lambda x).x}(\mathbf{kk}\xi_1)$ can reduce either to $\underline{1}$ or to $\underline{0}$ depending on whether the subterm $\mathbf{kk}\xi_1$ is reduced before or after ζ-reduction. However, we still have a notion of normal form (when no reduction rule can be applied to a term) and leftmost innermost reduction, as defined below.

Definition 8.6.1. We define a sequence of partial operators, RED_n for each n as follows:

For $n = 0$, define RED_0 as follows:

1. if t is a normal form, $\mathrm{RED}_0(t) = t$
2. for $t = \mathbf{k}rs$ where r and s are normal forms, $\mathrm{RED}_0(\mathbf{k}rs) = r$
3. for $t = \zeta_F r$ where r is a normal form, $\mathrm{RED}_0(\zeta_F r) = \underline{n}$ where n is maximal such that $\xi_{F^{-1}(n)}$ occurs in r or 0 if no ξ_i occurs in r

If RED_n has been already been defined, then we define RED_{n+1} as follows:

1. if $\mathrm{RED}_n(t) \downarrow$, then $\mathrm{RED}_{n+1}(t) = \mathrm{RED}_n(t)$

2. for $t = \mathrm{s}rsu$, where r, s, and u are normal forms,

$$\mathrm{RED}_{n+1}(\mathbf{s}rsu) \simeq \mathrm{RED}_n(\mathrm{RED}_n(ru)\,\mathrm{RED}_n(su))$$

3. if $t = rs$ and neither of previous cases apply, then

$$\mathrm{RED}_{n+1}(rs) \simeq \mathrm{RED}_n(\mathrm{RED}_n(r)\,\mathrm{RED}_n(s))$$

We then define RED as

$$\mathrm{RED} = \bigcup_{n \in \omega} \mathrm{RED}_n$$

Note that if $\mathrm{RED}(t)$ is defined, then it is a normal form.

We now define our pca, $\mathcal{T}$ in the same way as in chapter 2, that is

Definition 8.6.2. Let $\mathcal{T}$ be the set of normal forms of $\mathcal{C}$ together with the following application:

$$s.t := \mathrm{RED}(s.t)$$

(undefined if $\mathrm{RED}(s.t)$ is undefined)

As in chapter 2 we get the following propositions.

Proposition 8.6.3. *Suppose that t is a closed term over $\mathcal{T}$ (in the sense of definition 2.1.5) and write t^* for the corresponding term (in the sense of definition 2.5.9). Then* $\mathrm{RED}(t^*)$ *is defined if and only if t denotes, and in this case we have*

$$\mathrm{RED}(t^*) = t$$

Proof. The proof of proposition 2.5.18 still holds here. □

Proposition 8.6.4. *$\mathcal{T}$ is a pca.*

Proof. The proof of proposition 2.5.19 still holds here. □

8.6.2 Preservation of Atoms

The non trivial structure of $V_0^\Gamma(\mathcal{T})$ will rely on the ξ_i, and the rich supply of automorphisms arising from permutations of them. We will want to ensure therefore that under suitable conditions the atoms aren't eliminated by the realizability structure. In this section, we will aim towards a lemma that will enable us to show this.

Definition 8.6.5. For any pca, $\mathcal{A}$, one may consider the following classes of elements

1. recall from definition 4.4.1 that $f \in \mathcal{A}$ is *type 1* if for every $n \in \omega$, $f.\underline{n} \downarrow$, and there is some $m \in \omega$ such that $f.\underline{n} = \underline{m}$
2. $e \in \mathcal{A}$ is *type 2* if for every type 1 f, $e.f \downarrow$ and $e.f$ is type 1
3. $e \in \mathcal{A}$ is a *type 2 identity* if it is type 2 and for all f type 1 and for all $n \in \omega$, $ef\underline{n} = f\underline{n}$

We will now show that being able to decide whether a term is defined or not is equivalent to the halting problem.

Proposition 8.6.6. *Suppose that* $t(x) = t_1(x)t_2(x)$*,* $l \in \omega$*, and* r *is a normal form. If* $\mathrm{RED}_l((\lambda x).t(x)r) \downarrow$*, then* $l > 0$ *and* $\mathrm{RED}_{l-1}(t(r)) \downarrow$*.*

Proof. Note that from the definition of lambda terms over a pca (in the proof of proposition 2.2.3) we know that

$$(\lambda x).t(x) := \mathbf{s}((\lambda x).t_1(x))((\lambda x).t_2(x))$$

Note firstly that

$$(\lambda x).t(x)r = \mathbf{s}(\lambda x).t_1(x)(\lambda x).t_2(x)r$$

and hence we can only have $\mathrm{RED}_l((\lambda x).t(x)r) \downarrow$ for $l > 0$. Furthermore,

$$\mathrm{RED}_l(\mathbf{s}(\lambda x).t_1(x)(\lambda x).t_2(x)r) \simeq \\ \mathrm{RED}_{l-1}(\mathrm{RED}_{l-1}((\lambda x).t_1(x)r)\,\mathrm{RED}_{l-1}((\lambda x).t_2(x)r))$$

Since we are assuming that $\mathrm{RED}_l((\lambda x).t(x)r)\downarrow$, we know that $\mathrm{RED}_{l-1}((\lambda x).t_1(x)r)\downarrow$ and $\mathrm{RED}_{l-1}((\lambda x).t_2(x)r)\downarrow$, and hence

$$\begin{aligned}\mathrm{RED}_{l-1}(\mathrm{RED}_{l-1}((\lambda x).t_1(x)r)\,\mathrm{RED}_{l-1}((\lambda x).t_2(x)r)) &= \mathrm{RED}_{l-1}(t_1(r)t_2(r))\\ &= \mathrm{RED}_{l-1}(t(r))\end{aligned}$$

and in particular $\mathrm{RED}_{l-1}(t(r))\downarrow$.

□

Proposition 8.6.7. *For any $m, n \in \omega$, there is a closed normal form t_m and a normal form $t'_m(x)$ with free variable x such that for all $r \in \mathcal{T}$*

1. $\mathrm{RED}(t_m r)\downarrow$ *if and only if the mth Turing machine halts on input m, and if this occurs* $\mathrm{RED}(t_m r) = I$ *($I := \mathbf{skk}$)*
2. $\mathrm{RED}(t'_m(\zeta_F)r)\downarrow$ *if and only if the mth Turing machine halts on input m, and if this occurs* $\mathrm{RED}(t_m(\zeta_F)r) = \underline{F(n)}$
3. *t'_m contains ξ_n*
4. *t_m contains no ξ_i and t'_m contains only ξ_i for $i = n$*

Proof. By representability of computable functions in pcas (see eg [39] or [5]), one can construct u_m such that for every $k \in \omega$, and every $v \in \mathcal{T}$

$$u_m\underline{k} = \begin{cases}\mathbf{k}I & \text{if the } m^{\text{th}} \text{ Turing machine halts by stage k}\\ (\lambda z).(z\underline{k+1}) & \text{if the } m^{\text{th}} \text{ Turing machine does not halt by stage k}\end{cases}$$

Then, following the construction in the fixed point theorem,

$$\begin{aligned} w &:= (\lambda x).((\lambda y).u_m y(xx))\\ v &:= ww\\ &= (\lambda y).u_m y(ww)\end{aligned}$$

Then if the mth Turing machine halts at stage k,

$$\begin{aligned} v\underline{0} &\simeq u_m\underline{0}(ww) \\ &\simeq u_m\underline{0}v \\ &\simeq v\underline{1} \\ &\vdots \\ &\simeq v\underline{k} \\ &\simeq u_m\underline{k}(ww) \\ &\simeq (\mathbf{k}I)(ww) \\ &\simeq I \end{aligned}$$

In particular $v\underline{0}\downarrow$.

Now suppose that the mth Turing machine never halts. We show by induction on l that for all $l \in \omega$ and for all $k \in \omega$,

$$\mathrm{RED}_l(v\underline{k})\uparrow$$

Assume that for all $k \in \omega$ and for all $l' < l$ the statement above holds and assume for a contradiction that $\mathrm{RED}_l(v\underline{k})\downarrow$. Note that

$$\mathrm{RED}_l(v\underline{k}) = \mathrm{RED}_l(((\lambda y).u_m y(ww))\underline{k})$$

and so by proposition 8.6.6, we know in particular that $\mathrm{RED}_{l-1}(u_m\underline{k}(ww))\downarrow$. But in this case

$$\begin{aligned} \mathrm{RED}_{l-1}(u_m\underline{k}(ww)) &= \mathrm{RED}_{l-2}(\mathrm{RED}_{l-2}(u_m\underline{k})\,\mathrm{RED}_{l-2}(ww)) \\ &= \mathrm{RED}_{l-2}((\lambda z).(z\underline{k+1})v) \\ &= \mathrm{RED}_{l-3}(v\underline{k+1}) \end{aligned}$$

and so in particular $\mathrm{RED}_{l-3}(v\underline{k+1})\downarrow$ giving a contradiction as required.

Finally, let $t_m = \mathrm{s}(\mathbf{k}v)(\mathbf{k}\underline{0})$. Then, for all r, $t_m r \simeq v\underline{0}$, by the basic properties of s and $\mathbf{k}$

For parts 2 and 3, let t_m be as above and let $t'_m(x) = \mathbf{s}(\mathbf{s}t_m(\mathbf{k}x))(\mathbf{k}\xi_n)$ and note that the result follows from the basic properties of s and $\mathbf{k}$ □

Lemma 8.6.8 (Preservation of Atoms)**.** *Let e be a type 2 identity in $\mathcal{T}$. Then for any n, there is some type 1 f in $\mathcal{T}$ such that* $\mathrm{RED}(e.f)$ *contains the atom ξ_n as a subterm and furthermore, only contains ξ_i such that $i = n$.*

Proof. We assume that this is not the case and derive a contradiction.

We will define a (computable) family $f_m(x)$ of normal forms with one free variable such that for each F, $f_m(\zeta_F)$ is type 1 in $\mathcal{T}$.

Let $g_m \in \mathcal{T}$ be such that for all $l \in \omega$, $g_m\underline{l} = \mathbf{k}(\mathbf{k0})$ if the mth Turing machine with input m has not halted by stage l and $g_m\underline{l} = I$ if the mth Turing machine has halted by stage l. We can do this using the representability of primitive recursive functions in pcas..

Then let t'_m be as in proposition 8.6.7. Define

$$f_m(x) := \mathbf{s}(\mathbf{s}g_m(\mathbf{k}t'_m(x)))I$$

Note that this is in normal form, and that if the mth Turing machine has not halted by stage l then for any ζ_F

$$\begin{aligned}
\mathrm{RED}(f_m(\zeta_F)\underline{l}) &\simeq \mathrm{RED}(\mathrm{RED}((\mathbf{s}g_m(\mathbf{k}t'_m(\zeta_F)))\underline{l})\underline{l}) \\
&\simeq \mathrm{RED}(\mathrm{RED}(\mathrm{RED}(g_m\underline{l})t'_m(\zeta_F))\underline{l}) \\
&\simeq \mathrm{RED}(\mathrm{RED}(\mathbf{k}(\mathbf{k0})t'_m(\zeta_F))\underline{l}) \\
&\simeq \mathrm{RED}(\mathbf{k0}\underline{l}) \\
&\simeq \mathbf{0}
\end{aligned}$$

In particular, see that $f_m(\zeta_F)\underline{l}\downarrow$ even if the mth Turing machine never halts on input m.

If the mth Turing machine on input m has halted by stage l, then

$$\begin{aligned}
\mathrm{RED}(f_m(\zeta_F)\underline{l}) &\simeq \mathrm{RED}(\mathrm{RED}((\mathbf{s}g_m(\mathbf{k}t'_m(\zeta_F)))\underline{l})\underline{l}) \\
&\simeq \mathrm{RED}(\mathrm{RED}(\mathrm{RED}(g_m\underline{l})t'_m(\zeta_F))\underline{l}) \\
&\simeq \mathrm{RED}(\mathrm{RED}(It'_m(\zeta_F))\underline{l}) \\
&\simeq \mathrm{RED}(t'_m(\zeta_F)\underline{l}) \\
&\simeq \underline{F(n)}
\end{aligned}$$

Hence for any $m \in \omega$ and any ζ_F, $f_m(\zeta_F)$ is type 1 in the sense we defined earlier.

We therefore know that $e.f_m(\zeta_F) \simeq \mathrm{RED}(e.f_m(\zeta_F)) \downarrow$ and by hypothesis $\mathrm{RED}(e.f)$ cannot contain ξ_n. For convenience, in the below we will assume that F is chosen such that ζ_F does not occur anywhere in e.

Note that we can carry out an algorithm to find $\mathrm{RED}(e.f_m(\zeta_F))$ from m. (Only finitely many ξ_i's and ζ_G's occur in e and $f_m(\zeta_F)$, so we can give these terms Gödel numbers and the ζ-rule does not cause a problem here because we only need to know $G(k)$ where ζ_G occurs in e or $G = F$ and ξ_k occurs in e or $k = n$ and this is only finitely much information).

Furthermore, note that when we carry out this algorithm we can check whether or not we ever need to evaluate $\mathrm{RED}(t'_m(\zeta_F)r)$ for some r. If we did need to evaluate this, then in particular $\mathrm{RED}(t'_m(\zeta_F)r) \downarrow$ and so the mth Turing machine must halt on input m. On the other hand, if we did not need to evaluate $\mathrm{RED}(t'_m(\zeta_F)r)$, then ζ_F was never used in the ζ-rule because it only ever occurs as a subterm of the normal form $t'_m(\zeta_F)$. Furthermore, by hypothesis $t'_m(\zeta_F)$ cannot occur as a subterm of $\mathrm{RED}(e.f_m(\zeta_F))$, because otherwise $e.f_m(\zeta_F)$ would contain ξ_n.

Hence if we choose F' such that $F'(n) \neq F(n)$ then

$$\mathrm{RED}(e.f_m(\zeta_F)) = \mathrm{RED}(e.f_m(\zeta_{F'}))$$

But note that this means $f_m(\zeta_F)$ and $f_m(\zeta_{F'})$ must have the same value on every l. This can only happen if they are both identically zero and hence the mth Turing machine does not halt on input m.

Therefore we could use such an algorithm to solve the halting problem and we derive our contradiction. □

8.6.3 Automorphisms of $\mathcal{T}$

Suppose that $\pi : \omega_{>0} \to \omega_{>0}$ is a permutation. Then π induces an automorphism $\alpha : \mathcal{T} \to \mathcal{T}$ as follows.

1. $\alpha(\xi_n) = \xi_{\pi(n)}$
2. $\alpha(\zeta_F) = \zeta_{F \circ \pi^{-1}}$
3. $\alpha(\mathbf{s}) = \mathbf{s}$
4. $\alpha(\mathbf{k}) = \mathbf{k}$
5. $\alpha(s.t) = \alpha(s)\alpha(t)$

Note that we have chosen the action of α on the ζ_F so that it is compatible with the ζ-rule and the action of α on the ξ_n. α is clearly therefore an automorphism of $\mathcal{T}$.

8.7 A Useful Lemma

Before we move onto the proof itself, we prove a lemma that is true in general for any pca $\mathcal{A}$. Informally, what this says is the property of being injectively presented can be inherited "up to realizability" across sets that are realizably equal.

Lemma 8.7.1. *There is some $e \in \mathcal{A}$ such that for any $a, b \in V(\mathcal{A})$, if $f \in \mathcal{A}$ is such that $f \Vdash a = b$ and a is injectively presented, and if $\langle g, c\rangle, \langle g, c'\rangle \in b$, then*

$$efg \Vdash c = c'$$

Proof. Since $f \Vdash a = b$, there must be $\langle((f)_1 g)_0, d\rangle, \langle((f)_1 g)_0, d'\rangle \in a$ such that

$$\begin{aligned} ((f)_1 g)_1 &\Vdash c = d \\ ((f)_1 g)_1 &\Vdash c' = d' \end{aligned}$$

Since a is injectively presented, we know in fact that $d = d'$ and so

$$\mathbf{i}_t((f)_1 g)_1(\mathbf{i}_s((f)_1 g)_1) \Vdash c = c'$$

Hence we can take

$$e := (\lambda x, y).\mathbf{i}_t((x)_1 y)_1(\mathbf{i}_s((x)_1 y)_1)$$

□

8.8 Failure of the Existence Property

We will show that the existence property fails for **CZF** in the following instance.

Theorem 8.8.1. *There is no formula with one free variable $\chi(x)$ such that*

$$\mathbf{CZF} \vdash (\exists ! x)\chi(x)$$

and

$$\mathbf{CZF} \vdash \chi(x) \rightarrow x \subseteq \mathrm{mv}(\mathbb{N}^{\mathbb{N}}, \mathbb{N}) \wedge (\forall R \in \mathrm{mv}(\mathbb{N}^{\mathbb{N}}, \mathbb{N}))(\exists S \in x) S \subseteq R$$

This will immediately give the following corollary.

Corollary 8.8.2. **CZF** *does not have wEP.*

Proof. We know that

$$\mathbf{CZF} \vdash (\exists x)(x \subseteq \mathrm{mv}(\mathbb{N}^{\mathbb{N}}, \mathbb{N}) \wedge (\forall R \in \mathrm{mv}(\mathbb{N}^{\mathbb{N}}, \mathbb{N}))(\exists S \in x) S \subseteq R)$$

Suppose that there is some $\psi(x)$ such that

$$\begin{aligned} \mathbf{CZF} &\vdash (\exists! x)\psi(x) \\ \mathbf{CZF} &\vdash (\forall x)\psi(x) \to (\exists z) z \in x \\ \mathbf{CZF} &\vdash (\forall x)\psi(x) \to (\forall z \in x) \\ &\qquad (z \subseteq \mathrm{mv}(\mathbb{N}^{\mathbb{N}}, \mathbb{N}) \wedge (\forall R \in \mathrm{mv}(\mathbb{N}^{\mathbb{N}}, \mathbb{N}))(\exists S \in z) S \subseteq R) \end{aligned}$$

Then by taking $\chi(w)$ to be $\forall x \psi(x) \to w = \bigcup x$, we would get

$$\mathbf{CZF} \vdash (\exists! w)\chi(w)$$

and

$$\mathbf{CZF} \vdash \chi(w) \to w \subseteq \mathrm{mv}(\mathbb{N}^{\mathbb{N}}, \mathbb{N}) \wedge (\forall R \in \mathrm{mv}(\mathbb{N}^{\mathbb{N}}, \mathbb{N}))(\exists S \in w) S \subseteq R$$

contradicting the theorem. □

Proof of theorem 8.8.1 Assume that there is such a $\chi(x)$.

Let $\mathcal{T}$ be the pca from section 8.6 and let G be the group of all automorphisms obtained from permutations of ω, as in section 8.6.3. Let Γ be the normal filter generated by $\{\mathrm{Stab}_G(\xi_n) \mid n \in \omega\}$. Hence if G acts on some class X, then for $x \in X$, $\mathrm{Stab}_G(x) \in \Gamma$ means that x "has finite support relative to the ξ_n."

By the soundness theorems, there must be $C^{\mathrm{ip}} \in V_0^{\mathrm{ip}}(\mathcal{T})$ and $C^{\Gamma} \in V_0^{\Gamma}(\mathcal{T})$ such that

$$\begin{aligned} V_0^{\mathrm{ip}}(\mathcal{T}) &\models \chi(C^{\mathrm{ip}}) \\ V_0^{\Gamma}(\mathcal{T}) &\models \chi(C^{\Gamma}) \end{aligned}$$

Hence we must have that

$$V_1(\mathcal{T}) \models \chi(C^{\mathrm{ip}}) \wedge \chi(C^{\Gamma})$$

and so

$$V_1(\mathcal{T}) \models C^{\mathrm{ip}} = C^{\Gamma}$$

This allows us to apply lemma 8.7.1 and deduce that there is some e_0 such that for any $\langle f, c\rangle, \langle f, c'\rangle \in C^\Gamma$,

$$e_0.f \Vdash_1 c = c'$$

In fact this is the only point where we need C^{ip} and we can now derive a contradiction by examining C^Γ carefully.

Recall that we can assume that the elements of $\mathbb{N}^\mathbb{N}$ are of the form $\langle f, \overline{f}\rangle$ as described in section 4.4.

Write ζ_1 for $\zeta_{(\lambda x).x}$ and for each N, construct $R_N \in V_0^\Gamma(\mathcal{T})$,

$$R_N := \{\langle 0, f, \overline{\langle \overline{f}, \overline{n}\rangle}\rangle \mid f \text{ is type } 1, n \leq N, \underline{n} = \zeta_1 f\} \cup \\ \{\langle 0, f, \overline{\langle \overline{f}, \overline{n}\rangle}\rangle \mid f \text{ is type } 1, n > N, \zeta_1 f > N\}$$

Lemma 8.8.3. *We have constructed these R_N so that the following hold:*

1. *$R_N \in V_0^\Gamma(\mathcal{T})$. In fact $\bigcap_{i=1}^N \mathrm{Stab}_G(\xi_i) \subseteq \mathrm{Stab}_G(R_N)$.*
2. *There is some $e_1 \in \mathcal{T}$ such that for all N, $e_1 \Vdash_\Gamma R_N \in \mathrm{mv}(\mathbb{N}^\mathbb{N}, \mathbb{N})$.*
3. *Suppose that $\langle f, a\rangle \in R_N$ and ξ_i occurs in f only if $i \leq N$. Then $a = \overline{\langle \overline{f}, \overline{n}\rangle}$ where $n = \zeta_1 f$ (and $n \leq N$).*

Proof. For 1, note that each set in the binary union in the definition of R_N is preserved by elements of $\bigcap_{i=1}^N \mathrm{Stab}_G(\xi_i)$.

For 2, note that each R_N can be "represented" by ζ_1. This can clearly be used to produce a realizer that these are multi valued functions.

Part 3 is clear from the definition. □

We will aim for our contradiction by first showing a lemma stating that any automorphism satisfying certain properties has to be the identity. This will use the key lemma from section 8.6.2 as well as the basic properties of R_N. We will then construct a non trivial automorphism satisfying these conditions. In this lemma we work over $V(\mathcal{T})$ and R_N in fact refers to R_N°.

Lemma 8.8.4. *Suppose that $a \in V(\mathcal{T})$, $N < N' \in \mathbb{N}$, and $e, f \in \mathcal{T}$ are such that*

1. *For any ξ_i occurring in e or f, $i \leq N$*
2. $\bigcap_{i=1}^{N} \mathrm{Stab}_G(\xi_i) \subseteq \mathrm{Stab}_G(a)$
3. $e \Vdash_1 (\forall x \in a) x \in R_{N'}$
4. $f \Vdash_1 (\forall x \in \mathbb{N}^{\mathbb{N}})(\exists y \in a)(\exists z \in \mathbb{N}) y = \langle x, z \rangle$

Then, whenever $\alpha \in G$ fixes ξ_i for $i \leq N$ and $i > N'$, α must also fix ξ_i for $N < i \leq N'$ and hence α must be the identity.

Proof. We first check that $(\lambda x).(e(fx)_0)_0$ is a type 2 identity.

Let g be type 1. Then $\langle g, \overline{g} \rangle \in \mathbb{N}^{\mathbb{N}}$. Therefore there is b such that $\langle (fg)_0, b \rangle \in a$ and $(fg)_1 \Vdash_1 (\exists z \in \mathbb{N}) b = \langle \overline{g}, z \rangle$.

Let $h := (e(fg)_0)_0$. Then we know that there is some c such that $\langle h, c \rangle \in R_{N'}$ and $(e(fg)_0)_1 \Vdash b = c$. By the basic properties of $R_{N'}$ we know that c must be of the form $\overline{\langle \overline{h}, \overline{m} \rangle}$ for some $m \in \mathbb{N}$. From above we know that $V(\mathcal{T}) \models (\exists z \in \omega) b = \langle \overline{g}, z \rangle$ and $V(\mathcal{T}) \models b = \overline{\langle \overline{h}, \overline{m} \rangle}$, so we deduce that $V(\mathcal{T}) \models \overline{g} = \overline{h}$. Hence g and h must have the same graphs as type 1 elements, and so $(\lambda x).(e(fx)_0)_0$ is a type 2 identity as required.

Now let $\alpha \in G$ fix ξ_i for $i \leq N$ and $i > N'$. Suppose for a contradiction that there is some n with $N < n < N'$ such that $\alpha(\xi_n) \neq \xi_n$.

By applying lemma 8.6.8 we can find a first order g such that g only contains ξ_i for $i = n$ and such that ξ_n does occur in $(e(fg)_0)_0$. Let b, h, and c be as above, but for this particular g.

Since e and f only contain ξ_i for $i \leq N$, we know that h can only contain ξ_i for $i \leq N$ or $i = n$. Since we have guaranteed that h does contain ξ_n, we know that $\zeta_1 h = \underline{n}$. In particular $n \leq N'$, so we know from the definition of $R_{N'}$ that c must be of the form $\overline{\langle \overline{h}, \overline{n} \rangle}$.

Since α fixes ξ_i for $i \leq N$ we know from our assumptions that α also fixes a. Therefore, since $\langle (fg)_0, b \rangle \in a$ we must also have $\langle \alpha((fg)_0, \alpha(b) \rangle \in a$. Hence if $h' := (e\alpha((fg)_0))_0$ we know that there is some c' with $\langle h', c' \rangle \in R_{N'}$ and $V(\mathcal{T}) \models \alpha(b) = c'$.

Since α fixes ξ_i for $i \leq N$ we know that ξ_i can only occur in e and $\alpha(f)$ for $i \leq N$. Since α fixes ξ_i for $i > N'$, we know that $\alpha(\xi_n)$ must be amongst ξ_i for $i \leq N'$. Hence h' only contains ξ_i for $i \leq N'$. Furthermore neither $\alpha(f)$ nor $\alpha(g)$ contains ξ_n and from the assumption that $\alpha(\xi_n) \neq \xi_n$ we also know that ξ_n does not occur in $\alpha(g)$. Hence $\zeta_1 h' = \underline{m}$ for some $m \leq N'$ with $m \neq n$. Again from the definition of $R_{N'}$, we know therefore that c' is of the form $\overline{\langle \overline{h'}, \overline{m} \rangle}$.

But then since $V(\mathcal{T}) \models b = \overline{\langle \overline{h}, \overline{n} \rangle}$, we have that $V(\mathcal{T}) \models \alpha(b) = \overline{\langle \alpha(\overline{h}), \alpha(\overline{n}) \rangle}$. Together with $V(\mathcal{T}) \models \alpha(b) = \overline{\langle \overline{h'}, \overline{m} \rangle}$ this gives $V(\mathcal{T}) \models \alpha(\overline{n}) = \overline{m}$. In fact $\alpha(\overline{n}) = \overline{n}$, so $V(\mathcal{T}) \models \overline{n} = \overline{m}$. But this is a contradiction since $m \neq n$.

□

Since we know $V_0^\Gamma(\mathcal{T}) \models (\forall x \in \mathrm{mv}(\mathbb{N}^\mathbb{N}, \mathbb{N}))(\exists y \in C)(y \subseteq x \wedge y \in \mathrm{mv}(\mathbb{N}^\mathbb{N}, \mathbb{N}))$, there must be $f, e_2, e_3 \in \mathcal{T}$ and c_n such that for all n,

$$\begin{array}{rcl} \langle 0, f, c_n \rangle & \in & C \\ e_2 & \Vdash_\Gamma & (\forall x \in c_n)(x \in R_n) \\ e_3 & \Vdash_\Gamma & (\forall x \in \mathbb{N}^\mathbb{N})(\exists y \in c_n)(\exists z \in \mathbb{N}) y = \langle x, z \rangle \end{array}$$

In particular we know that for all n, $\mathrm{Stab}_G(c_n) \in \Gamma$ and hence by proposition 8.4.2 $\mathrm{Stab}_G(c_n^\circ) \in \Gamma$. From now on we will work entirely over $V(\mathcal{T})$. When we write R_n and c_n we will in fact mean R_n° and c_n° respectively.

Recall that we chose e_0 so that for all m and n,

$$e_0 f \Vdash_1 c_m = c_n$$

and so by substitution we can use $e_0 f$ and e_2 to construct e_4 such that for all m and n

$$e_4 \Vdash_1 (\forall x \in c_m) x \in R_n$$

Now let N be large enough such that the list $\xi_1, \ldots, \xi_N$ includes any ξ_n in a support of c_0, or appearing in $e_0, e_1 e_2, e_3$ or e_4.

Let $N' = N + 2$.

Note that we have

$$e_4 \Vdash_1 (\forall x \in c_0) x \in R_{N'}$$

Let α be the automorphism that swaps round ξ_{N+1} and ξ_{N+2}, fixing everything else. Then we know that α fixes ξ_i for $i \leq N$ (and hence also fixes c_0 and any ξ_i occurring in e_3 and e_4) and fixes ξ_i for $i > N'$. However, clearly α does not fix ξ_{N+1}. Hence we can finally get a contradiction by applying lemma 8.8.4.

□

Chapter 9

Conclusion

The aim of this thesis was to use develop our understanding of constructive set theories by developing and using realizability.

Towards this aim we developed symmetric realizability models and have shown that they can be used to show the independence of various choice principles from constructive set theory.

The main result in this thesis was the result in chapter 8 that $\mathbf{CZF}$ does not have EP, or indeed even wEP. Since EP was described in the introduction as a property to be expected from constructive formal theories based on the BHK interpretation, one might ask if its failure indicates some weakness in $\mathbf{CZF}$ as a constructive theory. The short answer is no: $\mathbf{CZF}$ is still a sound foundation for constructive mathematics.

What we showed essentially was that $\mathbf{CZF}$ asserts the existence of mathematical objects that it does not know how to construct. However, $\mathbf{CZF}$ does have natural interpretations in which these objects can be constructed. One example is Aczel's original interpretation of $\mathbf{CZF}$ into type theory in [1]. Here, the sets asserted in the fullness axiom are sets of those multivalued relations that arise from elements of a particular exponential type. Another (related) interpretation is Rathjen's "formulas as classes" in [32], in which $\mathbf{CZF}$ is interpreted into $\mathbf{CZF}_E$. In this example the full sets appear as exponentials in the background universe. In [36] Rathjen and Tupailo showed using these techniques that

$\mathbf{CZF}$ with a choice principle $\mathbf{\Pi\Sigma} - \mathbf{AC}$ has a form of the existence property.

We may conclude therefore that there are examples of reasonable constructive theories where the existence property does not hold.

Bibliography

[1] P. Aczel. The type theoretic interpretation of constructive set theory. In A. MacIntyre, L. Pacholski, and J. Paris, editors, *Logic Colloquium '77*, pages 55–66. North–Holland, Amsterdam-New York, 1978.

[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-New York, 1982.

[3] P. Aczel and M. Rathjen. Notes on constructive set theory. Technical Report 40, Institut Mittag-Leffler, 2001.

[4] H. P. Barendregt. *The Lambda Calculus: Its Syntax and Semantics*, volume 103 of *Studies in Logic and the Foundations of Mathematics*. North-Holland, 1981.

[5] M. Beeson. *Foundations of Constructive Mathematics: Metamathematical Studies*. Springer, 1985.

[6] J. L. Bell. *Boolean-Valued Models and Independence Proofs in Set Theory*, volume 12 of *Oxford Logic Guides*. Oxford University Press, 1985.

[7] I. Bethke and J. W. Klop. Collapsing partial combinatory algebras. In *Higher-order algebra, logic, and term rewriting (Paderborn, 1995)*, volume 1074 of *Lecture Notes in Comput. Sci.*, pages 57–73. Springer, Berlin, 1996.

[8] I. Bethke, J. W. Klop, and R. de Vrijer. Extending partial combinatory algebras. *Mathematical Structures in Computer Science*, 9:483–505, 1999.

[9] A. Blass. Injectivity, projectivity, and the axiom of choice. *Trans. Amer. Math. Soc.*, 255:31–59, 1979.

[10] R.-M. Chen and M. Rathjen. Lifschitz realizability for intuitionistic Zermelo-Fraenkel set theory. *Archive for Mathematical Logic*, pages 1–30. 10.1007/s00153-012-0299-2.

[11] P. J. Cohen. Independence results in set theory. In J. Addison, L. Henkin, and A. Tarksi, editors, *The Theory of Models*, pages 39–54. North-Holland, 1963.

[12] H. Friedman. The consistency of classical set theory relative to a set theory with intuitionistic logic. *Journal of Symbolic Logic*, 38:315–319, 1973.

[13] H. Friedman and A. Ščedrov. Set existence property for intuitionistic theories with dependent choice. *Annals of Pure and Applied Logic*, 25:129–140, 1983.

[14] H. Friedman and A. Ščedrov. The lack of definable witnesses and provably recursive functions in intuitionistic set theory. *Advances in Mathematics*, 57:1–13, 1985.

[15] R. J. Grayson. Heyting-valued models for intuitionistic set theory. In M. P. Fourman, C. J. Mulvey, and D. S. Scott, editors, *Applications of Sheaves*, volume 753 of *Lecture Notes in Mathematics*, pages 402–414. Springer, Berlin, 1979.

[16] J. M. E. Hyland, P. T. Johnstone, and A. M. Pitts. Tripos theory. *Math. Proc. Cambridge Philos. Soc.*, 88(2):205–231, 1980.

[17] T. J. Jech. *The Axiom of Choice*. North-Holland, 1973.

[18] S. C. Kleene. Countable functionals. In A. Heyting, editor, *Constructivity in Mathematics (Proceedings of the colloquium held at Amsterdam, 1957)*, pages 81–100. North-Holland, 1959.

[19] J. Lipton. Constructive Kripke semantics and realizability. In *Logic from computer science (Berkeley, CA, 1989)*, volume 21 of *Math. Sci. Res. Inst. Publ.*, pages 319–357. Springer, New York, 1992.

[20] J. Longley. *Realizability Toposes and Language Semantics*. PhD thesis, University of Edinburgh, 1995.

[21] R. Lubarsky and M. Rathjen. On the constructive Dedekind reals. *Logic and Analysis*, 1(2):131–152, 2008.

[22] R. S. Lubarsky. Independence results around constructive ZF. *Annals of Pure and Applied Logic*, 132(2-3):209 – 225, 2005.

[23] R. S. Lubarsky. CZF and second order arithmetic. *Annals of Pure and Applied Logic*, 141(1-2):29 – 34, 2006.

[24] D. C. McCarty. *Realizability and Recursive Mathematics*. PhD thesis, Oxford University, 1984.

[25] I. Moerdijk and E. Palmgren. Type theories, toposes and constructive set theory: predicative aspects of ast. *Annals of Pure and Applied Logic*, 114:155 – 201, 2002.

[26] J. Myhill. Some properties of intuitionistic Zermelo–Fraenkel set theory. In A. R. D. Mathias and H. Rogers, editors, *Cambridge Summer School in Mathematical Logic*, volume 337 of *Lecture Notes in Mathematics*, pages 206–231. Springer, Berlin, 1973.

[27] J. Myhill. Constructive set theory. *Journal of Symbolic Logic*, 40:347–382, 1975.

[28] D. Normann. Set recursion. In *Generalized Recursion Theory II*, pages 303–320. North Holland, Amsterdam, 1978.

[29] P. Odifreddi. *Classical Recursion Theory*. North-Holland, 1989.

[30] M. Rathjen. The disjunction and other properties for Constructive Zermelo-Frankel set theory. *Journal of Symbolic Logic*, 70:1233–1254, 2005.

[31] M. Rathjen. Choice principles in constructive and classical set theories. In *Logic Colloquium '02*, volume 27 of *Lect. Notes Log.*, pages 299–326. Association for Symbolic Logic, La Jolla, CA, 2006.

[32] M. Rathjen. The formulae-as-classes interpretation of constructive set theory. In H. Schwichtenberg and K. Spies, editors, *Proof Technology and Computation*, volume 200 of *Series III: Computer and Systems Sciences*, pages 279 – 322. IOS Press, 2006.

[33] M. Rathjen. Realizability for constructive Zermelo-Fraenkel set theory. In V. Stoltenberg-Hansen and J. Väänänen, editors, *Logic Colloquium '03*. Association for Symbolic Logic, 2006.

[34] M. Rathjen. Metamathematical properties of intuitionistic set theories with choice principles. In C. S. Barry, B. Löwe, and S. Andrea, editors, *New Computational Paradigms*, pages 84–98. Springer, 2008.

[35] M. Rathjen. From the weak to the strong existence property. *Annals of Pure and Applied Logic*, 163(10):1400 – 1418, 2012.

[36] M. Rathjen and S. Tupailo. Characterizing the interpretation of set theory in Martin-Löf type theory. *Annals of Pure and Applied Logic*, 141:253–258, 2006.

[37] D. van Dalen and A. S. Troelstra. *Constructivism in Mathematics: An Introduction*, volume 121,123 of *Studies in Logic and the Foundation of Mathematics*. North-Holland, 1988.

[38] B. van den Berg and I. Moerdijk. The axiom of multiple choice and models for constructive set theory. Preprint available - arXiv:1204.4045v1, 2012.

[39] J. van Oosten. *Realizability: An Introduction to its Categorical Side*, volume 152 of *Studies in Logic and the Foundations of Mathematics*. Elsevier, 2008.

[40] J. van Oosten and P. Hofstra. Ordered partial combinatory algebras. *Mathematical Proceedings of the Cambridge Philosophical Society*, 134:445–463, 2003.

[41] A. Ziegler. Generalizing realizability and heyting models for constructive set theory. *Annals of Pure and Applied Logic*, 163(2):175 – 184, 2012.