THE JOURNAL OF SYMBOLIC LOGIC
Volume 83, Number 3, September 2018

FROM MULTISETS TO SETS IN HOMOTOPY TYPE THEORY

HÅKON ROBBESTAD GYLTERUD

Abstract. We give a model of set theory based on multisets in homotopy type theory. The equality of the model is the identity type. The underlying type of iterative sets can be formulated in Martin-Löf type theory, without Higher Inductive Types (HITs), and is a sub-type of the underlying type of Aczel's 1978 model of set theory in type theory. The Voevodsky Univalence Axiom and mere set quotients (a mild kind of HITs) are used to prove the axioms of constructive set theory for the model. We give an equivalence to the model provided in Chapter 10 of "Homotopy Type Theory" by the Univalent Foundations Program.

§1. Introduction. The first model of set theory in type theory is due to Aczel and models the constructive set theory CZF [1]. The underlying type of sets in this model is $W_U T$, the type of all well-founded trees with branchings in a universe U with decoding family $T : U \to \text{Type}$. The interpretation of equality in this model allows deduplication and permutation of subtrees—incorporating the intuition that the order and multiplicity of elements of a set are irrelevant. If we instead insist to interpret equality as the identity type and assume the univalence axiom, the underlying type no longer models set theory, but rather multiset theory.

In a related work [3] we explore the notion of iterative multisets in type theory. Here we will specialise from the general multisets to the set-like ones, where each element occurs at most once. We will start by summarising the model of multisets and its relation to Aczel's model of CZF in type theory [1].

Once the notion of a multiset is defined, it is natural to study the hereditary subtype of multisets where each element occurs at most once. These are in a certain sense the most natural representations of iterative sets from a homotopy type theory point of view. These are namely the multisets for which the element hood relation is hereditarily, merely propositional (type level -1).

In this text we explore how this type models various axioms of constructive set theory. We also show that it is equivalent to the higher inductive type outlined in the book "Homotopy Type Theory" [5].

1.1. From multisets to sets—two ways. Assume for a moment that we would like to explain the notion of multiset to someone who knows the notion of a set. Here are two similar attempts at such an explanation.

Received March 30, 2017.
2010 *Mathematics Subject Classification.* 03B15.
Key words and phrases. constructive set theory, type theory, W-types, homotopy type theory, higher inductive types, multisets.

0022-4812/18/8303-0012
DOI:10.1017/jsl.2017.84

1.1.1. Variant A.

> A multiset is a generalisation of sets in which an element may occur any number of times, not just at most once.

1.1.2. Variant B.

> A multiset is a set with the extra information attached to each element about how many times it occurs in the multiset.

The two descriptions are almost identical, but critically different. Variant A describes the multisets as a more general concept than sets, in the sense that a set is a *special case* of a multiset, namely those multisets in which each element occurs at most once. Variant B, on the other hand, describes a multisets as sets with some extra structure. In both cases the impression given is that the multisets are, in an informal way, a *bigger concept* than that of a set. Variant A says that sets are just some of the multisets, while Variant B says that for each set there are numerous ways to make a multiset from it.

In mathematics these two notions of "bigger" correspond to the notion of

- sets being a subtype of multisets (Variant A)
- sets being a quotient of multisets (Variant B).

If we were to turn the direction of explanations, making them explanations of the concept of a set from the notion of a multiset, the above suggests two distinct routes of constructing a notion of sets from a notion of multisets. We either identify the subtype of *set-like* multisets, or identify the equivalence relation of multisets which *forgets the extra structure of multiplicites*.

EXAMPLE 1.1. The multiset $\{a, a, b\}$ would not be considered a set-like in the spirit of Variant A, since a occurs twice. On the other hand, Variant B would contest that $\{a, a, b\}$ and $\{a, b, b\}$ would *represent the same* set, since in both cases a and b are exactly the elements occurring at least once.

If we denote by M the multisets, and V_A and V_B denotes the two possible notions of sets arising from it, following Variant A and Variant B, respectively, we can draw the following diagram of the situation.

$$\begin{tikzcd} V_A \arrow[r, hook] & M \arrow[d, two heads] \\ & V_B \end{tikzcd}$$

1.2. Outline. In Sections 2 and 3 we set up a bit of framework to work within. Starting from Section 4 we will follow the path of Variant A.

Section 5 will take us through the basic lemmas about the type of iterative sets we define in Section 4. These lemmas are applied in Section 6 to give proofs that our model satisfies the axioms of Myhill's Constructive Set Theory.

In Section 7 we consider the problem of interpreting the two collection axioms of Aczel's CZF in our model.

In Section 8 we return to Variant B, which will make the relationship with the approach taken in Chapter 10 of the book "Homotopy Type Theory" [5] clear.

1.3. Notation. In what follows we will adhere to the following notation. Some of our notation is similar to that of the book "Homotopy Type Theory" [5], while some of it is inspired by the syntax of Agda.

- Function application will be denoted by juxtaposition, as in $f\ a$. Also, application of functions equipped with extra structure, such as equivalences and embeddings, will be denoted by juxtaposition.
- Quantifiers, such as $\forall$,$\exists$,$\prod$ and $\sum$ bind weakly. For instance, $\prod_{x:\mathcal{M}} x \in a \to \sum_{y:\mathcal{M}} y \in B \wedge P\,x\,y$ disambiguates to $\prod_{x:\mathcal{M}} \left(x \in a \to \sum_{y:\mathcal{M}} y \in B \wedge P\,x\,y\right)$.
- The equality sign, $=$, denotes the identity type. We sometimes equip it with a subscript emphasising which type the elements belong to, as in $a =_A a'$.
- Definitions are signified by $:=$.
- Judgemental equalities are denoted by $\equiv$.
- The notation A : Type denotes that A is a type.
- The notation A : Set denotes that A is a type which is a mere set.
- The notation A : Prop denotes that A is a type which is a mere proposition.
- The type U is a universe, with decoding family $T : U \to \text{Type}$. We assume that this universe
  - is univalent,
  - contains the empty type, 0,
  - is closed under Π-types,
  - is closed under Σ-types,
  - is closed under $+$-types,
  - is closed under (-1)-truncation, and
  - is closed under taking quotients of mere sets by equivalence relations.
- The notation e_A denotes the empty function $e : 0 \to A$. The subscript is dropped when inferable from the context.
- The notation $ap\,f$ refers to the usual function ap $f : a = a' \to f\ a = f\ a'$.

§2. Types and propositions. One of the main features of Martin-Löf's type theory is the interpretation of propositions as types [4]. The presence of the identity type gives the possibility of asking whether two proofs of a proposition are equal. A type in which all elements are equal is called, in homotopy type theory, a *mere proposition*.

The traditional interpretation of the existential quantifier in type theory is by the Σ-type $\sum_{a:A} P\,a$. A proof of an existential proposition is thus of the form a, p—a term $a : A$ of the quantified domain paired with a proof $p : P\,a$ that the term has the correct property. It is clear that since the existence is not necessarily unique, the type of such proof need not be a mere proposition.

In homotopy type theory, one introduces a truncated existential quantifier $\exists(x : A)P\,a$, which is constructed from $\sum_{a:A} P\,a$ by adding identifications of all elements in to make it a mere proposition. This gives the following introduction and elimination rule:[1]

$$\frac{a : A \qquad b : B\ a}{[a, b] : \exists(a : A)(B\ a)}\ \exists\text{-INTRO}$$

$$\frac{x : \exists(a : A)(B\ a) \qquad y : \exists(a : A)(B\ a)}{q : x = y}\ \exists\text{-QUOT}$$

$$\frac{P : \exists(a : A)(B\ a) \longrightarrow \text{Prop} \qquad p : (a : A) \longrightarrow (b : B\ a) \longrightarrow P[a, b]}{\exists - elimPp : (x : \exists(a : A)(B\ a)) \longrightarrow Px}\ \exists\text{-ELIM.}$$

Clearly $\sum_{a:A}(B\ a) \to \exists(a : A)(Ba)$ holds for all A and B. The opposite implication holds if $\sum_{a:A}(B\ a)$ is a mere proposition—which is to say that the existence is unique, with a unique proof.

The situation is similar for disjunctions. Traditionally, disjunction is interpreted as disjoint union in Martin-Löf's type theory, while homotopy type theory introduces a truncated variant. We will denote disjoint unions by the operator $+$ and the truncated disjunction by the operator $\vee$.

§3. Models where equality is identity.

In this section we define what an $\in$-structure is, and give some basic results on such structures in generality. We do this in order to adjust our expectation for the concrete model which will be main focus of this work.

3.1. $\in$-structures.

Definition 3.1. An $\in$-*structure* is a pair $(\mathcal{M}, \in)$ where $\mathcal{M}$: Set is a mere set, and $\in: \mathcal{M} \to \mathcal{M} \to \text{Prop}$.

Definition 3.2. For any $\in$-structure $(\mathcal{M}, \in)$ and element $a : \mathcal{M}$, we define $E\ a := \sum_{x:\mathcal{M}} x \in a$.

Definition 3.3. An $\in$-structure $(\mathcal{M}, \in)$ is called U-*like* if for each $a : \mathcal{M}$ the type $E\ a$ is essentially U-small. That is, if each $a : \mathcal{M}$ the type $E\ a$ has a code in U.

Remark. An $\in$-structure is basically a mere set with a merely propositional, binary predicate defined on it. The natural equality to consider for elements of such a structure is the identity type. This is in contrast to the setoid approach taken by Aczel.

"U-like" is meant to mimic the traditional terminology, "set-like", used in set theory.

3.2. Translations of first-order logic into type theory.

Definition 3.4. Given an $\in$-structure $(\mathcal{M}, \in)$ define two translations of formulas of first-order logic to type theory, $\sigma_{\mathcal{M},\in}$ and $\tau_{\mathcal{M},\in}$, by recursion on formulas. We let Context denote contexts (finite lists of variables, Variable Γ denoting the variables in Γ) and let Formula Γ denote formulas in a given context Γ : Context.

[1] In these rules, written in an Agda-like notation, `Prop` refers to the type of mere propositions.

Starting with $\sigma_{\mathcal{M},\in}$, leaving out the subscripts for ease of reading:

$$\begin{aligned}
&\sigma : \prod_{\Gamma:\text{Context}} \text{Formula } \Gamma \to (\text{Variable } \Gamma \to \mathcal{M}) \to \text{Type}\\
&\sigma\,\Gamma\,(\forall x\ \phi)\,\gamma := \prod_{a:\mathcal{M}} \sigma\,(\Gamma.x)\phi\,(\gamma.a)\\
&\sigma\,\Gamma\,(\exists x\ \phi)\,\gamma := \sum_{a:\mathcal{M}} \sigma\,(\Gamma.x)\phi\,(\gamma.a)\\
&\sigma\,\Gamma\,(\phi \wedge \psi)\,\gamma := \sigma\,\Gamma\,\phi\,\gamma \times \sigma\,\Gamma\,\psi\,\gamma\\
&\sigma\,\Gamma\,(\phi \vee \psi)\,\gamma := \sigma\,\Gamma\,\phi\,\gamma + \sigma\,\Gamma\,\psi\,\gamma\\
&\sigma\,\Gamma\,(\phi \to \psi)\,\gamma := \sigma\,\Gamma\,\phi\,\gamma \to \sigma\,\Gamma\,\psi\,\gamma\\
&\sigma\,\Gamma\,\bot\,\gamma := 0\\
&\sigma\,\Gamma\,\top\,\gamma := 1\\
&\sigma\,\Gamma\,(x \in y)\,\gamma := \gamma\,x \in \gamma\,y\\
&\sigma\,\Gamma\,(x = y)\,\gamma := \gamma\,x =_{\mathcal{M}} \gamma\,y,
\end{aligned}$$

where $\Gamma.x$ denotes the context Γ extended with the variable x, and $\gamma.a$ denotes the function Variable $(\Gamma.x) \to \mathcal{M}$ which maps x to a.

We define $\tau_{\mathcal{M},\in}$ analogously, only difference being in the clauses for $\vee$ and $\exists$:

$$\begin{aligned}
&\tau : \prod_{\Gamma:\text{Context}} \text{Formula } \Gamma \to (\text{Variable } \Gamma \to \mathcal{M}) \to \text{Type}\\
&\tau\,\Gamma\,(\forall x\ \phi)\,\gamma := \prod_{a:\mathcal{M}} \tau\,(\Gamma.x)\phi\,(\gamma.a)\\
&\tau\,\Gamma\,(\exists x\ \phi)\,\gamma := \exists(a : \mathcal{M})\ \tau\,(\Gamma.x)\phi\,(\gamma.a)\\
&\tau\,\Gamma\,(\phi \wedge \psi)\,\gamma := \tau\,\Gamma\,\phi\,\gamma \times \tau\,\Gamma\,\psi\,\gamma\\
&\tau\,\Gamma\,(\phi \vee \psi)\,\gamma := \tau\,\Gamma\,\phi\,\gamma \vee \tau\,\Gamma\,\psi\,\gamma\\
&\tau\,\Gamma\,(\phi \to \psi)\,\gamma := \tau\,\Gamma\,\phi\,\gamma \to \tau\,\Gamma\,\psi\,\gamma\\
&\tau\,\Gamma\,\bot\,\gamma := 0\\
&\tau\,\Gamma\,\top\,\gamma := 1\\
&\tau\,\Gamma\,(x \in y)\,\gamma := \gamma\,x \in \gamma\,y\\
&\tau\,\Gamma\,(x = y)\,\gamma := \gamma\,x =_{\mathcal{M}} \gamma\,y.
\end{aligned}$$

EXAMPLE 3.5. The axiom of union is translated differently by the two translations:

$$\begin{aligned}
\text{UNION} &:= \forall x\, \exists u\, \forall z\ z \in u \leftrightarrow \exists y \in x\ z \in y\\
\sigma\,()\,(\text{UNION}) &= \prod_{x:M} \sum_{u:\mathcal{M}} \prod_{z:\mathcal{M}} z \in u \leftrightarrow \sum_{y:\mathcal{M}} y \in x \wedge z \in y\\
\tau\,()\,(\text{UNION}) &= \prod_{x:M} \exists(u : \mathcal{M}) \prod_{z:\mathcal{M}} z \in u \leftrightarrow \exists(y : \mathcal{M})\ y \in x \wedge z \in y.
\end{aligned}$$

If the structure $(\mathcal{M}, \in)$ satisfies the extensionality axiom, then the property $\prod_{z:\mathcal{M}} z \in u \leftrightarrow \exists(y : \mathcal{M})\ y \in x \wedge z \in y$ completely characterises u, making

$\tau\,()\,(\text{UNION}) \simeq \sum_{u:\mathcal{M}} \prod_{z:\mathcal{M}} z \in u \leftrightarrow \exists(y : \mathcal{M})\ y \in x \wedge z \in y$. However, $\sum_{y:\mathcal{M}} y \in x \wedge z \in y$ is not always implied by $\exists(y : \mathcal{M})\ y \in x \wedge z \in y$ so the two axioms remain distinct.

3.3. Axioms of set theory. The axioms of set theory contain a number of axiom schemas, such as collection or replacement, or (restricted) separation. In set theory this adds one axiom for each first-order formula. In type theory it is more convenient to use the higher-order features of type theory and regard these as quantified over all predicates. The result is much stronger than the original axiom scheme. In the following we will exploit this extra strength.

DEFINITION 3.6. Given a structure, $(\mathcal{M}, \in)$, and a predicate $P : \mathcal{M} \to \mathcal{M} \to \text{Type}$ and an element $m : \mathcal{M}$, we define *σ-replacement for P and m in $(\mathcal{M}, \in)$* to be the type $\sigma_P\,(a)\,((\forall x \in a\,\exists! y\ P\,x\,y) \to \exists b\,\forall y(y \in b \leftrightarrow \exists x \in a\ P\,x\,y))\,m$, where σ_P is σ extended with the clause $\sigma\,\Gamma\,(P\,x\,y)\,\gamma := P\,(\gamma\,x)\,(\gamma\,y)$, in order to interpret the P as a predicate symbol.

Define τ-replacement in the same way, substituting τ for σ.

PROPOSITION 3.7. *If an $\in$-structure $(\mathcal{M}, \in)$ satisfies extensionality, σ-replacement and has an ordered pairing operation $\langle -, - \rangle : \mathcal{M} \to \mathcal{M} \to \mathcal{M}$, then the following choice principle, stemming from the so-called* type theoretic choice principle,[2] *holds*:

For any $P : \mathcal{M} \to \mathcal{M} \to$ Type *and $a, b : \mathcal{M}$ if*

$$\prod_{x:\mathcal{M}} x \in a \to \sum_{y:\mathcal{M}} y \in B \wedge P\,x\,y,$$

then there is a function $f : \mathcal{M}$ with domain a and codomain b such that $\prod_{x:\mathcal{M}} P\,x\,(f\,x)$.

PROOF. Given a,b and a proof $p : \prod_{x:\mathcal{M}} x \in a \to \sum_{y:\mathcal{M}} y \in B \wedge P\,x\,y$, apply σ-replacement to a and the predicate $P' : \mathcal{M} \to \mathcal{M} \to \text{Prop}$ defined by

$$P'\,x\,z := \sum_{q:x\in a} z =_{\mathcal{M}} \langle x, \pi_0\,(p\,x\,q)\rangle.$$

The resulting element of $\mathcal{M}$ is a function with the desired properties. ⊣

REMARK. Proposition 3.7 shows us that we cannot hope to have a model satisfying all axioms of constructive set theory by interpreting the existential quantifier as Σ-types while at the same time interpreting equality as the identity type of a mere set. This is because the above proposition shows that AC will hold, in this interpretation, and thus if all other CZF axioms hold (in fact U-restricted separation and pairing should suffice), Diaconescu's theorem demonstrates that the law of excluded middle holds (for all U-small propositions).

§4. The model of iterative sets.

We recall the definition, from [3], of the type of iterated multisets and the membership relation.

[2] The type theoretic choice principle is the fact that for all A, B and P, the type $(\prod_{a:A} \sum_{b:B\,a} P\,a\,b) \to \sum_{f:\prod_{a:A} B\,a} \prod_{a:A} P\,a\,(f\,a)$ is inhabited.

DEFINITION 4.1.

$$M := W_U T$$

$$\in_M : M \to M \to \text{Set}$$
$$x \in_M (\text{sup } a\ f) := \sum_{i:T\ a} f\ i = x.$$

The elements of M are the iterative multiset in which another element of M may occur any U-small number of times. This is expressed by the relation $\in_M$, as follows: Given $x, y : M$ the type $x \in_M y$ is the type of occurrences of x in y. For instance, if $(x \in_M y) \simeq 2$ then x occurs twice in y.

What we would like to consider are the elements of M in which every element occurs at most once. Such a multiset would be called *set-like*. Being set-like could be expressed in different ways. The most direct would be to say that $y : M$ is set-like whenever $x \in_M y$ is a mere proposition for all other $x : M$. Another way to state this is to say that the function mapping each instance of an element in y to the element it represents is an embedding.

The *iterative sets* are those multisets which are hereditarily set-like. On M we define the predicate itset, recursively, as follows.

DEFINITION 4.2.

$$\text{itset} : M \to \text{Type}$$
$$\text{itset}\,(\text{sup } a\ f) := \text{embedding } f \wedge \prod_{i:T\ a} \text{itset}\,(f\ a).$$

For each $x : M$, whenever we have itset x, we say that x is an *iterative set*.

A Σ-type then collects the type of iterative sets as a subtype of M—with elementhood defined by the restriction of elementhood for multisets.

DEFINITION 4.3. The type of iterative sets, V, is defined as the subtype of M of iterative sets. That is $V := \sum_{x:M} \text{itset } x$.

We denote by $\in_V$ the specialisation of $\in_M$ to V. That is, $x \in_V y := \pi_0\, x \in_M \pi_0\, y$.

NOTATION. *We will permit ourselves a slight abuse of notation when denoting elements of V. We will for the remainder of this article use the notation* sup $a\ f$ *to denote an element of V constructed by $a : U$ and an embedding $f : T\ a \hookrightarrow V$.*

REMARK. Checking that a multiset is an iterative set can be a tedious task, since it has to be carried out on each level of the tree, but the next section will give lemmas to make it easier to construct new iterative sets.

§**5. Basic results.** In this section we clarify the basic properties of iterative multisets and $(V, \in_V)$. The most important of these is the extensionality of V with respect to $\in_V$.

We start with reminding ourselves of the extensionality theorem for multisets.

THEOREM 5.1. $x =_M y \simeq \prod_{z:M} ((z \in_M y) \simeq (z \in_M y))$

PROOF. See Theorem 3.14 in Section 3.5 of [3]. ⊣

LEMMA 5.2. *The type* itset x *is a mere proposition for every* $x : M$.

PROOF. Immediate by induction on M and that embedding f is a mere proposition. ⊣

LEMMA 5.3. *The function* ap $\pi_0 : (x =_V y) \to (\pi_0\, x =_M \pi_0\, y)$ *is an equivalence.*

PROOF. Since itset is a mere proposition, the first projection, $\pi_0 : V \to M$, is an embedding. Hence, ap π_0 is an equivalence on the identity of V. ⊣

LEMMA 5.4. *For any* $x : M$ *and* $y : V$ *we have that the type* $x \in_M \pi_0 y$ *is a mere proposition*.

PROOF. Assume $y \equiv (\sup a\ f, (p, q))$. Observe that $x \in_M \pi_0 y$ is the fibre of f over y. Since p proves f to be an embedding, and embeddings have propositional fibres, then $x \in_M \pi_0 y$ is a proposition. ⊣

LEMMA 5.5.

$$\left(\prod_{z:V} (z \in_V x \leftrightarrow z \in_V y)\right) \simeq \left(\prod_{z:M} (z \in_M \pi_0 x \leftrightarrow z \in_M \pi_0 y)\right).$$

PROOF. Both sides of the equivalence are mere propositions, so it is enough to show biimplication. Passing from right to left is trivial, so we show only the implication from left to right.

Assume $z : M$. If $z \in \pi_0 x$ then z must be an iterative set. Thus, $z \in y$ which is to say $z \in \pi_0 y$. This demonstrates $z \in \pi_0 x \to z \in \pi_0 y$. That $z \in \pi_0 y \to z \in \pi_0 x$ is shown symmetrically. Hence, $z \in \pi_0 x \leftrightarrow z \in \pi_0 y$, which completes the proof. ⊣

LEMMA 5.6. *Given a small type* $a : U$ *and a function* $f : T\,a \to V$, *there is a set* image $a\ f$ *such that*

- *for each* $i : T\,a$ *we have that* $f\ i \in (\text{image}\ a\ f)$
- *for any merely propositional predicate* $P : V \to \text{Set}$, *given* $\prod_{i:T\,a} P\,(f\ i)$ *we can prove that* $\prod_{z:V}(z \in (\text{image}\ a\ f) \to P\,z)$.

PROOF. Given $a : U$ and $f : T\,a \to V$. Take the image factorisation of f, which can be expressed as a simple higher inductive type. Since V is locally U-small, the image has a code $b : U$. Denote the injection of the image into V by $g : Tb \to V$, and define image $a\ f := \sup b\ v$. ⊣

§6. V models Myhill's constructive set theory.

In this section we prove that $(V, \in_V)$ models the axioms of Myhill's Constructive Set Theory (CST), when the existential quantifiers are interpreted as truncated. In fact, we shall see that except for a few critical places, positive occurrences of the existential quantifier can be strengthened to $\sum$, mostly because the constructions we make are explicit.

6.1. Extensionality.

The lemmas we have proved line up to give the following equivalence:

THEOREM 6.1. $x =_V y \leftrightarrow \prod_{z:V} (z \in x \leftrightarrow z \in y)$.

PROOF.

$$
\begin{aligned}
x =_V y \simeq \pi_0 x = \pi_0 y & \qquad (1)\\
\simeq \prod_{z:M} (z \in_M \pi_0 x \simeq z \in_M \pi_0 y) & \qquad (2)\\
\simeq \prod_{z:M} (z \in_M \pi_0 x \leftrightarrow z \in_M \pi_0 y) & \qquad (3)\\
\simeq \prod_{z:V} (z \in_V \pi_0 x \leftrightarrow z \in_M \pi_0 y)\,. & \qquad (4)
\end{aligned}
$$

⊣

6.2. The empty set, natural numbers. The empty set is given by $\emptyset := \sup 0\, e$. Furthermore, the multiset of natural numbers we constructed in Section 4.10 of [3] is indeed an iterative set.

6.3. Separation. Restricted separation can be done in V without quotienting, as long as the separating predicate is merely propositional. Thus, whenever we separate a formula with existential quantifier in a positive position, the existence must be unique or truncated. If there are more than one witness of the statement, the result would be a multiset where the element occurs once per witness of the statement. The same is true for disjunction. Notice that if $A + B$ is a proposition then A and B are mutually exclusive (since $l\ a$ and $r\ b$ are always distinct).

PROPOSITION 6.2 (Separation). *For any U-small predicate $P : Vi \to \mathrm{Prop}$, and $x : V$ there is $u : V$ such that for any $z : V$ we have $z \in u \leftrightarrow (P\ z) \times (z \in x)$.*

PROOF. Assume that $x \equiv \sup A\ f$ and let $u := \sup(\sum_{a:A} P\,(f\ a))(f \circ \pi_0)$. Since $P \circ f$ is a mere proposition $\pi_0 : (\sum_{a:A} P\,(f\ a)) \to A$ is injective, thus $f \circ \pi_0$ is injective.

If $z \in u$ then $z = f\ a$ for some $a : A$ such that $P\,(f\ a)$, and hence $P\ z$ and $z \in x$. If $p : P\ z$ and $q : z \in x$ then let $a := \pi_0 q$, $((a, p), \pi_1\ q)$ will prove that $z \in u$. ⊣

6.4. $\in$-induction. Induction on V can be performed, even when the predicate is a general type, not necessarily merely propositional.

PROPOSITION 6.3 ($\in$-induction). *For every predicate $P : V \to \mathrm{Type}$, if for each $x : V$ we have that $\prod_{y:V} y \in x \to P\ y$ implies $P\ x$, then we have $P\ x$ for every $x : V$.*

PROOF. By induction on V. Assume $x \equiv \sup A\ f$ then by induction hypothesis $P\,(f\ i)$ for every $i : A$. We must show that if $y \in x$ then $P\ y$. However, $y \in x$ means that there is i such that $y = f\ i$ so we can transport the induction hypothesis to obtain $P\ y$. Thus, we have shown $\prod_{y:V} y \in x \to P\ y$, which implies $P\ x$ by assumption. ⊣

6.5. Pairing and union. In order to show pairing and union we will have to apply the image construction, previously introduced (Lemma 5.6). If we applied the constructions of union and pairing for multisets which we defined in [3], then the resulting multisets would not be set-like. Therefore, we need a different construction, and the most natural is to take quotients to make the multisets back into sets. The fact that quotienting was not needed for multisets, may be an indication that iterative multisets is a more natural notion than iterative sets to consider in type theory.

DEFINITION 6.4. Given $x, y : V$, we define $\{x, y\} :=$ image $(1+1)$ (const x + const y).

PROPOSITION 6.5 (Pairing). *For any $x, y : V$ and for each $z : V$ we have that $z \in \{x, y\} \leftrightarrow ((x = z) \vee (y = z))$.*

PROOF. Simple consequence of Lemma 5.6. ⊣

DEFINITION 6.6. Given $x : V$, where $x \equiv \sup A\, f$ define
$\cup x :=$ image $(\sum_{a:A} \overline{(f\, a)})\, (\lambda\langle i, j\rangle.\widetilde{(f\, i)}\, j)$.

PROPOSITION 6.7 (Union). *For any $x : V$ and for any $z : V$, we have that $z \in \cup x \leftrightarrow \exists y\, (y \in x \wedge z \in y)$.*

PROOF. Simple consequence of Lemma 5.6. ⊣

REMARK. The truncated existential quantifier in the above proposition cannot be strengthened to a Σ-type, since it would mean constructing sections for almost arbitrary quotients.

6.6. Replacement.

PROPOSITION 6.8 (Replacement). *For any $a : V$ and $P : V \to V \to$ Prop, such that for all $x \in a$ there exists a unique y for which $P\, x\, y$, then there is $b : V$ such that for each $y : V$ we have that $y \in b$ if and only if there exists $x \in a$ such that $P\, x\, y$.*

PROOF. Given $a = \sup \bar{a}\, \tilde{a}$, the assumptions let us construct a map $T\, \bar{a} \to V$. Using Lemma 5.6, we can construct its image in V, which will have the desired properties. ⊣

PROPOSITION 6.9. *For any $a : V$ and $F : V \to V$, there is $y : V$ such that for any $z : V$ we have $z \in b \leftrightarrow \exists (w : V)\, z = F\, w$.*

PROOF. Assume $x \equiv \sup a\, f$ and let $b =$ image $(F \circ f)$, and apply Lemma 5.6. ⊣

6.7. Exponentiation. The construction of exponentials in this model is particularly easy, since a set-theoretical function between two elements, $(\sup A\, f)$ and $(\sup B\, g)$, of V boils down to a function in the type theory $A \to B$. Instead of giving a direct proof, we can lean on [3], Section 4.9 in order to prove the correctness of this construction.

Exponentiation of sets is a special case of exponentiation of multisets. For multisets, we defined[3] the type $\text{operation}_{a,b}\, f$ for every $a, b, f : M$, and showed that there is a multiset Exp $a\, b$, such that $f \in \text{Exp}\, a\, b \simeq \text{operation}_{a,b}\, f$. We will here show that whenever $a, b, f : V$, we have $\text{operation}_{\pi_0\, a, \pi_0\, b}\, (\pi_0\, f)$ if an only if Fun $a\, b\, f$, and that in fact itset $(\text{Exp}\, (\pi_0\, a)\, (\pi_0\, b))$, in order to conclude that there is exponentiation in V.

LEMMA 6.10. *Whenever $a, b, f : V$, we have that $\text{operation}_{\pi_0\, a, \pi_0\, b}\, (\pi_0\, f) \leftrightarrow \text{Fun}\, a\, b\, f$.*

[3]Definition 4.12 in Section 4.7 of [3] .

Proof. Recall that[4] for every $a, b, f : M$,

$$\begin{aligned}\text{operation}_{a\,b}\ f :=& \left(\prod_z z \in f \to \sum_x \sum_y z = \langle x, y\rangle\right)\\ &\wedge \left(\prod_x x \in a \simeq \sum_y \langle x, y\rangle \in f\right)\\ &\wedge \left(\prod_y y \in b \leftarrow \sum_x \langle x, y\rangle \in f\right).\end{aligned}$$

If here it said $\leftrightarrow$ instead of $\simeq$, this would state that f is a total relation between a and b. We thus have to show that this strengthening is exactly the same as ensuring functionality of a total relation.

In the middle conjunction, $x \in a$ is a mere proposition since a is an iterative set by assumption. Thus, $\sum_y \langle x, y\rangle \in f$ must also be a mere proposition, and thus equivalent to $\exists!(y : M)\langle x, y\rangle \in f$. This is exactly the requirement for a total relation to be functional. ⊣

Remark. Since $\text{operation}_{\pi_0\,a, \pi_0\,b}\,(\pi_0\,f)$ and $\text{Fun}\ a\ b\ f$ are both mere propositions, the biimplication is also an equivalence of types.

Lemma 6.11. *For every $a, b : V$ the multiset* $\text{Exp}\,(\pi_0\,a)\,(\pi_0\,b)$ *is an iterative set.*

Proof. The definition of $\text{Exp}\ a\ (\pi_0 b)$ is

$$\begin{aligned}\text{Exp}\,(\pi_0 a)\,(\pi_0 b) := \sup\,&(\overline{(\pi_0\,a)} \to \overline{(\pi_0\,b)})\\ &(\lambda f.\sup \overline{(\pi_0\,a)}\\ &(\lambda i.\langle \widetilde{(\pi_0\,a)} i, \widetilde{(\pi_0\,b)}\,(f\ i)\rangle)).\end{aligned}$$

Thus, we need to show that the function $\lambda f.\sup \overline{(\pi_0\,a)}\,(\lambda i.\langle \widetilde{(\pi_0 a)} i, \widetilde{(\pi_0 b)}(f\ i)\rangle)$, which takes a function to its graph, is injective, but this comes down to that a function is determined by its graph, which follows from function extensionality.

Next, we need to argue that each graph of each function is itself an iterative set. Assume that $f : \overline{(\pi_0\,a)} \to \overline{(\pi_0\,b)}$, then the function which maps an element $i : \overline{(\pi_0 a)}$ to $\langle \widetilde{(\pi_0 a)}\,i, \widetilde{(\pi_0 b)}\,(f\,i)\rangle$ is injective since $\pi_0\ a$ is an iterative set. Furthermore, $\langle \widetilde{(\pi_0\,a)}\,i, \widetilde{(\pi_0\,b)}\,(f\ i)\rangle$ is an iterative set since both a and b are iterative sets. Thus, the graph of f is an iterative set. ⊣

Proposition 6.12 (Exponentiation). *For every $a, b : V$ there is a $u : V$ such that for any $c : V$ there is an biimplication $c \in u \leftrightarrow$* $\text{Fun}\ a\ b\ c$.

Proof. Direct from Lemma 6.10, Lemma 6.11, and exponentiation in M[5], letting $u := \text{Exp}\,(\pi_0 a)\,(\pi_0 b) \leftrightarrow \text{Fun}\ a\ b\ f$. ⊣

§7. Collection axioms. In this section we discuss the status of collection axioms of constructive set theory in our model.

[4] ibid.

[5] `(M-EXP)` in Section 4.9 of [3] .

Neither strong collection, nor subset collection seem to hold in either extreme interpretation of the existential quantifier (i.e., applying τ or σ). Interpreting the existential quantifier as Σ-types forces us to make arbitrary choices in an apparently unconstructive way. Interpreting the existential quantifier as the truncated $\exists$, the assumptions become too weak to work with.

We discuss two approaches to solving this problem. On the one hand, we identify which existential quantifiers need to be weakened—and which have to remain strict—in order to get something like the collection axioms to become provable for our model. On the other hand, we identify axioms about the type theoretical universe, from which V was constructed, from which we can derive collection and subset collection in the truncated form.

7.1. Strong collection. Together with subset collection, strong collection is the most subtle of the axioms of constructive set theory. First of all because it is underspecified: the strong collection axiom states the existence of a set, but does not define it up to equality.

On an intuitive level, strong collection states that if we have shown that for all elements of a set x there exists some element with a certain property, then the proof is in some way an operation which should have an image in V.

The problem is that the proof in first-order logic may not be uniform, in the sense that the operation may not respect equality of elements. However, this would not prevent us from taking its image.

In Aczel's original model one can see this, as his V is a setoid and we can talk about extensional operations on the underlying type. However, our V has the identity type as its equality type. This means that if we interpret the existential quantifier as the Σ-type, then any proof operation will give rise to an actual function which respects equality. The image of such an operation is naturally a multiset, and we have seen how to quotient such a multiset to a set. The only wrinkle of this approach is that the "strong part" of strong collection has to be weakened by using a truncated existential quantifier.

7.1.1. Strong quantifiers. The following proposition is the rendering of strong collection in which we, as far as our abilities go, interpreted the existential quantifier as Σ-types.

PROPOSITION 7.1. *For any predicate $P : V \to V \to \mathrm{Type}$ and every $a : V$ if $\prod_{x:V}(x \in a) \to \sum_{y:V} P\,x\,y$ then there is $b : V$ such that*

1. $\prod_{x:V}(x \in a) \to \sum_{y:V} y \in b \wedge (P\,x\,y)$
2. $\prod_{y:V}(y \in b) \to \exists(x : V)\, x \in a \wedge (P\,x\,y)$.

PROOF. Given $a \equiv \sup\,\bar{a}\,\tilde{a}$, the assumptions let us construct a map $T\,\bar{a} \to V$. Using Lemma 5.6, we can construct its image in V, which will have the desired properties. ⊣

REMARK. It is well known that, in constructive set theory, collection implies replacement, and that the converse implication does not hold. But the strong version of replacement proven for our model in Proposition 6.8, formulated for a given $\in$-structure, does in fact entail the collection principle of Proposition 7.1, for the same $\in$-structure.

7.1.2. Weak quantifies. Aczel and Gambino [2] discuss a general approach to interpreting first-order logic into type theory. For any given interpretation in their framework, they identify type theoretic principles corresponding to strong collection and subset collection. Here we will, in a similar fashion, give a sufficient principle for our model to satisfy strong collection in the sense of weak quantifiers.

DEFINITION 7.2. **Collection principle for a universe, U:**
For every locally U-small B : Set, given $a : U$ and $P : T\,a \to B \to \mathrm{Type}$, such that $\prod_{x:T\,A} \exists(y : B) P\,x\,y$ then $\exists(r : U)\exists(\beta : T\,r \hookrightarrow B)(\prod_{x:T\,a} \exists(y : T\,r) P\,x\,(\beta\,y)) \wedge (\prod_{y:T\,r} \exists(x : T\,a) P\,x\,y)$.

PROPOSITION 7.3. *The collection principle for U implies strong collection in the following sense*:
For any predicate $P : V \to V \to \mathrm{Type}$ and every $a : V$ if $\prod_{x:V}(x \in a) \to \exists(y : V) P\,x\,y$ then there merely exists $b : V$ such that

1. $\prod_{x:V}(x \in a) \to \exists(y : V)\; y \in b \wedge (P\,x\,y)$
2. $\prod_{y:V}(y \in b) \to \exists(x : V)\; x \in a \wedge (P\,x\,y)$.

PROOF. Apply the collection principle for U to $P \circ \bar{a}$, to obtain the mere existence r and β, which together form $b := \sup r\,\beta$. 1. and 2. follow from the property of the collection principle for U. ⊣

7.2. Subset collection. Subset collection is the principle that for any pair of sets there is a third set, such that each total relation between the two has an image in the third. The precise formulation of the axiom in first-order logic is slightly complicated by the fact that one cannot quantify over all (or even all definable) total relations in the middle of a formula. Therefore, the axiom is an axiom schema quantified over ternary formulas, where the first parameter is allowed to vary. Our formulation will be close to the first-order formulation:

$$\begin{aligned}\forall a, b\, \exists c\, \forall u\, (\forall x \in a \to \exists y \in b \wedge P\,u\,x\,y)\\ \to (\exists d \in c \wedge (\forall x \in a \to \exists y \in d \wedge P\,u\,x\,y)\\ \wedge (\forall y \in d \to \exists x\; x \in a \wedge P\,u\,x\,y).\end{aligned}$$

In the above formula there are three existential quantifiers to interpret, either as a Σ-type or as a truncated existential. At one extreme it is possible to give all but the last existential quantifier the Σ-type interpretation, truncating the last one.

PROPOSITION 7.4. *For every predicate $P : V \to V \to V \to \mathrm{Type}$ and every $a, b : V$ there is $c : V$ such that for all $u : V$ if $\prod_{x:V}(x \in a) \to \sum_{y:V} P\,u\,x\,y$ then there is $d \in c$ such that*

1. $\prod_{x:V}(x \in a) \to \sum_{y:V} y \in d \wedge (P\,u\,x\,y)$
2. $\prod_{y:V}(y \in d) \to \exists(x : V)\; x \in a \wedge (P\,u\,x\,y)$.

PROOF. Given $a \equiv \sup \bar{a}\,\tilde{a}$ and $b \equiv \sup \bar{b}\,\tilde{b}$, consider the function $\gamma : (\bar{a} \to \bar{b}) \to V$ which maps each $f : \bar{a} \to \bar{b}$ to $\mathrm{image}(\tilde{b} \circ f)$ in V. Let $c := \mathrm{image}\,\gamma$, which will have the desired properties. ⊣

7.2.1. Weak quantifiers. In the same way we did for strong collection, we identify a principle of subset collection for our universe which is sufficient to prove the truncated variation of subset collection for our model.

DEFINITION 7.5. **Subset collection principle for U:**
For each $a, b : U$ there merely exists $c : U$ such that for every $P : T\,a \to T\,b \to \mathrm{Type}$ such that $\prod_{x:T\,a} \exists(y : T\,b) P\,x\,y$, there $\exists(r : T\,c)(\prod_{x:T\,a} \exists(y : T\,r) P\,x\,(\alpha\,y)) \wedge (\prod_{y:T\,r} \exists(x : T\,a) P\,x\,y)$.

PROPOSITION 7.6. *For every predicate $P : V \to V \to V \to \mathrm{Type}$ and every $a, b : V$, there merely exists a $c : V$ such that for every $u : V$, if $\prod_{x:V}(x \in a) \to \sum_{y:V} P\,u\,x\,y$ then there merely exists $d \in c$ such that*

1. $\prod_{x:V}(x \in a) \to \exists(y : V)\; y \in d \wedge (P\,u\,x\,y)$
2. $\prod_{y:V}(y \in d) \to \exists(x : V)\; x \in a \wedge (P\,u\,x\,y)$.

PROOF. Apply the subset collection principle for U to a,b to obtain the mere existence of c, and then use the property of c on the predicate $P\,u$. ⊣

§8. Equivalence with the HIT-formulation.

Section 5.1 of Chapter 10 of the book "Homotopy Type Theory" [5], is dedicated to set theory in the context of homotopy type theory. The iterative hierarchy is presented there, in the form of a higher inductive type (HIT). Our V is a HIT-free alternative to this, and in this section we show that the two types are equivalent.

The HIT formulation bears more than a slight similarity to Aczel's original construction of the iterative hierarchy in type theory. Both are quotients of the type we call M. The difference is that while Aczel uses the untruncated version of the quantifiers and leaves the quotient a setoid, HTT uses the truncated quantifiers and postulates the existence of a type with the identity type to match.

In this section we define the bisimulation relation on M of which the iterative hierarchy in HTT Chapter 10 can be seen a quotient. We show that this quotient is equivalent to our V. The proof of this equivalence relies on a function, iterative-image : $M \to V$, which turns any multiset into an iterative set by identifying all occurrences of each elements, having first applied the process inductively on all elements.

DEFINITION 8.1. We define by induction on M the binary relation:

$$\approx\, : M \to M \to \mathrm{Type}$$

$$(\sup\ a\ f) \approx (\sup\ b\ g) := \left(\prod_{x:T\,a} \exists(y : T\,b)(f\ x \approx g\ y)\right) \times \left(\prod_{y:T\,b} \exists(x : T\,a)(f\ x \approx g\ y)\right).$$

DEFINITION 8.2. We define by induction on M the function:

$$\text{iterative-image} : M \to V$$
$$\text{iterative-image}\,(\sup\ a\ f) := \text{image}\ a\ (\text{iterative-image} \circ f).$$

LEMMA 8.3. *For each* $x : M$ *we have that* $x \approx \text{iterative-image } x$.

PROOF. For each element of x there is a corresponding element in iterative-image x, since the type of elements of iterative-image x is a quotient of the type of elements in x. In the other direction there just *merely* exists an element of x for each element of iterative-image x, since it was a quotient. However, this is sufficient to show that $x \approx \text{iterative-image } x$. ⊣

LEMMA 8.4. *For iterative sets,* $\approx$ *is equivalent to the identity type. That is, for every* $x, y : M$ *given* itset x *and* itset y, *we have that* $x \approx y \to x =_M y$.

PROOF. By W-induction. Let $x \equiv \sup a\, f$ and $y \equiv \sup b\, g$, and assume $x \approx y$. By extensionality, it suffices to show that for any $z : M$ we have that $z \in_M x$ if and only if $z \in_M y$.

In one direction, if $z \in_M x$ we know that there is $i : T\, a$ such that $z =_M f\, i$. Since $z \in_M y$ is a mere proposition, we can assume from $x \approx y$ that there is a $j : T\, b$ such that $f\, i \approx g\, j$. By inductive hypothesis, $f\, i \approx g\, j \to f\, i =_M g\, j$, and thus $z =_M g\, j$ which is to say $z \in_M y$.

The other direction is symmetric in x and y. ⊣

PROPOSITION 8.5. $V \simeq M/{\approx}$.

PROOF. Direct consequence of the previous two lemmas. ⊣

REMARK. That $M/{\approx}$ is equivalent to the HIT formulation in the book can be seen from Lemma 10.5.5 of “Homotopy Type Theory” [5]. Thus, proposition 8.5 shows that our V is indeed equivalent to the HIT formulation of the iterative hierarchy.

REFERENCES

[1] P. ACZEL, *The type theoretic interpretation of constructive set theory*, ***Logic Colloquium ’77*** (A. MacIntyre, L. Pacholski, and J. Paris, editors), North–Holland, Amsterdam, 1978, pp. 55–66.

[2] P. ACZEL and N. GAMBINO, *The generalised type-theoretic interpretation of constructive set theory*, this JOURNAL, vol. 71 (2006), no. 1, pp. 67–103.

[3] H. R. GYLTERUD, *Multisets in Type Theory*, preprint, 2016, arXiv:1610.08027.

[4] P. MARTIN-LÖF, ***Intuitionistic Type Theory***, Studies in Proof Theory, vol. 1, Bibliopolis, Naples, 1984.

[5] THE UNIVALENT FOUNDATIONS PROGRAM, ***Homotopy Type Theory: Univalent Foundations of Mathematics***, homotopytypetheory.org, Institute for Advanced Study, 2013.

DEPARTMENT OF INFORMATICS
UNIVERSITY OF BERGEN
POSTBOKS 7803
N-5020 BERGEN, NORWAY
E-mail: hakon.gylterud@uib.no