Core Extensional Mathematics and Local Constructive Set Theory

in honor of the 60th birthday of Giovanni Sambin

Advances in Constructive Topology

and

Logical Foundations,

Padua, October 2008 .

Peter Aczel

petera@cs.man.ac.uk

Manchester University

Two papers by Milly Maietti and Giovanni Sambin

- Toward a minimalist foundation for constructive mathematics
- A minimalist two level foundation for constructive mathematics

- My motivations are similar.

- But not the same.

Some settings for constructive mathematics

- Dependent Type Theory (DTT)
- Constructive Set Theory (CST)
- Local Constructive Set Theory (LCST)
- DTT is intensional and keeps the fundamental constructive notions explicit.
- CST is fully extensional and expressed in the single-sorted language of axiomatic set theory.
- LCST is also extensional, but many-sorted and is a predicative variation on higher order arithmetic.

My motivation: To have a setting for topics in constructive mathematics, such as point-free topology, that allows a rigorous presentation that can be simply translated into both the DTT and CST settings.

Core extensional mathematics (CeM)

- LCST is a setting for CeM. It is a generalised predicative version of John Bell's local set theory for the impredicative (topos mathematics)
- CeM has its origins in Bishop style constructive mathematics, as further developed by Bridges, Richman et al and influenced by Martin-Lof's DTT, by CST and by topos theory.
- Roughly, it is generalised predicative mathematics with intuitionistic logic. But it uses no form of choice, so as to be compatible with topos mathematics and allow sheaf models.
- A lot of elementary mathematics can be carried out in CeM; e.g. the categorical axiomatisations of the natural numbers and the constructive Dedekind reals.

Simple type structures over the set N.

- Impredicative: $N \quad \mathcal{P}N \quad \mathcal{P}\mathcal{P}N \quad \cdots$
  For each set A, $\mathcal{P}A$ is the set of all subsets of A.
- Predicative: $N \quad Pow(N) \quad Pow(Pow(N)) \quad \cdots$
  For each class A, $Pow(A)$ is the class of all subsets of A.
- N is a set, but the assertion that $Pow(N)$ is a set is taboo!.
- Given A, what is a set of elements of A?
- Some notions of set of:
  - logical
  - combinatorial
  - hybrid

Notions of set of

- Logical: Sets of elements of A are given as extensions $B = \{x : A \mid R(x)\}$ of propositional functions R on A. Then $a \in B \equiv R(a)$. But this is the notion of class on A.
- Combinatorial: Sets of elements of A are given as families $B = \{a_i\}_{i:I}$ of elements a_i of A, indexed by an index type I. Then $a \in B \equiv (\exists i : I)[a =_A a_i]$.
- Hybrid Sets of elements of A are given as $B = \{a_i \mid i : I \mid R(i)\}$, where $\{a_i\}_{i:I}$ is a family of elements a_i indexed by an index type I and R is a propositional function on I. Then $a \in B \equiv (\exists i : I)[R(i) \wedge a =_A a_i]$.
- The combinatorial notion works when the type theory uses propositions-as-types. The hybrid notion works more generally for type theories that use a suitable treatment of logic.

Interpreting CST in DTT

- The iterative notion of set, used to interprete CST in DTT, uses an inductive type V whose single introduction rule is

$$\frac{a \text{ is a set of elements of } V}{a : V}$$

- The combinatorial notion of set of is used, assuming propositions-as-types, or more generally the hybrid notion might be used. The index types of the families are the 'small' types; i.e. the types in some type universe.
- The interpretation of LCST in DTT does not need the inductively defined type V. The powertype of a type A is just the type of sets of elements of the type A.

Class notation

- $A \equiv \{x \mid \phi(x, \ldots)\}$
- $a \in A \ \leftrightarrow \ \phi(a, \ldots)$
- $A = B \ \leftrightarrow \ \forall x[x \in A \ \leftrightarrow \ x \in B]$

Treat classes as individual terms in a free logic that is conservative over the set theory.

In a free logic individual terms need not denote values in the range of the variables.

The free logic extension

- Define: $\downarrow A \equiv \exists x[x = A]$
- Modify quantifier axioms to:

$$[\forall x \phi(x) \wedge \ \downarrow A] \rightarrow \phi(A)$$

$$[\downarrow A \ \wedge \ \phi(A)] \rightarrow \exists x \phi(x)$$

- Add axioms:

$$\downarrow y, \quad \text{for each variable } y$$

$$A \in B \rightarrow \downarrow A, \quad \text{for class terms } A, B$$

- Keep the rule

$$\frac{\phi(x)}{\forall x \phi(x)} \ (*)$$

Local CST (LCST)

Formulated in a free logic version of many-sorted intuitionistic predicate logic with equality.

Sorts: $N \quad \alpha \times \beta \quad \mathcal{P}\alpha$

Basic formulae: $\bot \quad \top \quad [a = a'] \quad [a \in b]$ for $a, a' : \alpha, b : \mathcal{P}\alpha$

Compound formulae:

$$\phi \wedge \phi' \qquad \phi \vee \phi' \qquad \phi \rightarrow \phi'$$

$$(\forall x : \alpha)\phi(x) \qquad (\exists x : \alpha)\phi(x)$$

Individual terms:

$$\frac{}{0 : N} \qquad \frac{a : N}{s(a) : N} \qquad \frac{a : \alpha \quad b : \beta}{(a, b) : \alpha \times \beta}$$

$$\frac{}{\{x : \alpha \mid \phi(x)\} : \mathcal{P}\alpha}$$ for each formula $\phi(x)$

Axioms and rules

Free logic version of many-sorted intuitionistic predicate logic with equality.

$\downarrow$ axioms: $\downarrow x$ for variables x, $\downarrow 0$ and $\downarrow s(y)$ for each variable $y : N$.

$\downarrow(x, y)$ for variables $x : \alpha$, $y : \beta$

$[a \in b] \rightarrow \downarrow a$ for terms $a : \alpha$, $b : \mathcal{P}\alpha$

N and $\alpha \times \beta$ axioms:

$s(x) = 0 \rightarrow \perp$ and $s(x) = s(x') \rightarrow [x = x']$ for variables $x, x' : N$

$[(x, y) = (x', y')] \rightarrow [x = x'] \wedge [y = y']$ for variables $x, x' : \alpha$, $y, y' : \beta$

$(\exists x : \alpha)(\exists y : \beta)[z = (x, y)]$ for variable $z : \alpha \times \beta$

Structural $\mathcal{P}\alpha$ axioms:

$a \in \{x : \alpha \mid \phi(x)\} \leftrightarrow \phi(a)$ for terms $a : \alpha$

$(\forall x : \alpha)[x \in b \leftrightarrow x \in b'] \rightarrow [b = b']$ for terms $b, b' : \mathcal{P}\alpha$

When are class terms set terms?

Set existence axioms for $LCZF^-$

Emptysets: $\downarrow\emptyset_\alpha$, where $\emptyset_\alpha \equiv \{x : \alpha \mid \bot\}$.

Pairing: $\downarrow\{x, x'\}$ for variables $x, x' : \alpha$, where
$\{x, x'\} \equiv \{x'' : \alpha \mid x'' = x \vee x'' = x'\}$.

Equalitysets: $\downarrow\delta(x, x')$ for variables $x, x' : \alpha$, where
$\delta(x, x') \equiv \{x'' : \alpha \mid x'' = x \wedge x'' = x'\}$.

Indexed Union:
$$(\forall x : \alpha)[x \in z \rightarrow \downarrow\{y : \beta \mid (x, y) \in R\}]$$
$$\rightarrow \downarrow\{y : \beta \mid (\exists x : \alpha)[x \in z \wedge (x, y) \in R]\}$$
for variables $z : \mathcal{P}\alpha$ and terms $: \mathcal{P}(\alpha \times \beta)$.

Infinity: $\downarrow\mathbb{N}$ where $\mathbb{N} \equiv \{x \in N \mid (\forall z \in \mathcal{P}N)[Ind(z) \rightarrow x \in z]\}$

$$Ind(z) \equiv [0 \in z \wedge (\forall x : N)[x \in z \rightarrow s(x) \in z]]$$

Full Mathematical Induction:
$Ind(A) \rightarrow \mathbb{N} \subseteq A$ for terms $A : \mathcal{P}N$

Some abbreviations

In the following $\phi(x)$ is a formula, with $x : \alpha$ a variable.
$A, A' : \mathcal{P}\alpha$, $B : \mathcal{P}\beta$ and $R : \mathcal{P}(\alpha \times \beta)$ are terms.

$(\forall x \in A)\ \phi(x)$	$(\forall x : \alpha)\ (x \in A\ \rightarrow\ \phi(x))$
$(\exists x \in A)\ \phi(x)$	$(\exists x : \alpha)\ (x \in A\ \wedge\ \phi(x))$
$\{x \in A \mid \phi(x)\}$	$\{x : \alpha \mid x \in A\ \wedge\ \phi(x)\}$
$A \subseteq A'$	$(\forall x \in A)\ x \in A'$
$Pow(A)$	$\{y : \mathcal{P}\alpha \mid y \subseteq A\}$
$A \cup A'$	$\{x : \alpha \mid x \in A\ \vee\ x \in A'\}$
$A \cap A'$	$\{x : \alpha \mid x \in A\ \wedge\ x \in A'\}$
$R : A \succ\!\!- B$	$(\forall x \in A)(\exists y \in B)\ (x, y) \in R$
$R : A \succ\!\!-\!\!\prec B$	$R : A \succ\!\!- B\ \ \wedge\ \ (\forall y \in B)(\exists x \in A)\ (x, y) \in R$
$A \times B$	$\{z \in \alpha \times \beta \mid (\exists x \in A)(\exists y \in B)[z = (x, y)\}$
$mv(A, B)$	$\{z \in Pow(A \times B) \mid z : A \succ\!\!- B]\}$

Collection Schemes

Strong Collection $(\forall u \in Pow(A))$

$$[R : u \succ B] \;\rightarrow\; (\exists v \in Pow(B))[R : u \succ\!\prec v]$$

Fullness (equivalent to Subset Collection)

$$(\forall u \in Pow(A))(\forall v \in Pow(B))(\exists z \in Pow(mv(u, v)))$$
$$(\forall r \in mv(x, y))(\exists r' \in z)[r' \subseteq r]$$

Inductive definitions in Local CST,1

- Let $\mathcal{I}\alpha \equiv \mathcal{P}(\alpha \times \mathcal{P}\alpha)$ and extend the language by allowing basic formulae $t \vdash a$ for $t : \mathcal{I}\alpha$ and $a : \alpha$.
- We think of t as an inductive definition or abstract axiom system with inductive generation rules or inference steps

$$\frac{X}{a} \quad \text{for } (a, X) \in t$$

- $t \vdash a$ is intended to express that a is inductively generated by t or is a theorem of t.
- Define $CL(t, c) \equiv (\forall x : \alpha)(\forall y : \mathcal{P}\alpha)[(x, y) \in t \wedge y \subseteq c] \rightarrow x \in c$ and $I(t) \equiv \{x : \alpha \mid t \vdash x\}$

Inductive definitions in Local CST,2

- $LCZF$ is obtained from $LCZF^-$ by adding

  $\mathcal{I}0$ $t \subseteq t' \rightarrow I(t) \subseteq I(t')$.

  $\mathcal{I}1$ $(\forall z : \mathcal{I}\alpha)\, CL(z, I(z))$.

  $\mathcal{I}2$ $(\forall z : \mathcal{I}\alpha)\, CL(z, c) \rightarrow I(z) \subseteq c)$ for terms $c : \mathcal{P}\alpha$.

- Theorem: Define $\overline{I}(t) \equiv \{x : \alpha \mid (\exists z \in Pow(t))\, x \in I(z)\}$. Then

  1. $CL(t, \overline{I}(t))$,
  2. $CL(t, c) \rightarrow \overline{I}(t) \subseteq c$ for $c : \mathcal{P}\alpha$.

Inductive definitions in Local CST,3

- To extend to an axiom system $LCZF^+$ primitive $\vdash$ is not needed as we can define

$$t \vdash' a \equiv (\forall y : \mathcal{P}\alpha)[CL(t, y) \to a \in y]$$

  and

$$I'(t) \equiv \{x : \alpha \mid t \vdash' x\}.$$

  and add the axiom $(\forall z : \mathcal{I}\alpha)\ \downarrow I'(z)$.

- Then $\mathcal{I}'0$ and $\mathcal{I}'1$ are derivable. We should add the further axiom

$$\mathcal{I}'2 : (\forall z : \mathcal{I}\alpha)[CL(z, c) \to I'(z) \subseteq c]$$

  for $z : \mathcal{P}\alpha$.

- But further axioms are needed to get the desired local applications of REA etc.