Rudimentary Constructive Set Theory

Set Theory, Model Theory, Generalized Quantifiers and Foundations of Mathematics:

Jouko's birthday conference!

Meeting in Honor of Jouko Väänänen's Sixtieth Birthday 16-18 September 2010 .

Peter Aczel

petera@cs.man.ac.uk

Manchester University,

Part I

Rudimentary CST

The Axiom Systems CZF, BCST and RCST

- CZF is formulated in the first order language $\mathcal{L}_\in$ for intuitionistic logic with equality, having $\in$ as only non-logical symbol. It has the axioms of Extensionality, Emptyset, Pairing, Union and Infinity and the axiom schemes of Δ_0-Separation, Strong Collection, Subset Collection and Set Induction. (CZF+ classical logic)$\equiv$ ZF.
- BCST (Basic CST) is a weak subsystem of CZF. It uses Replacement instead of Strong Collection and otherwise only uses the axioms of Extensionality, Emptyset, Pairing, Union and Binary Intersection ($x \cap y$ is a set for sets x, y).
- RCST (Rudimentary CST) is like BCST except that it uses the Global Replacement Rule (GRR) instead of the Replacement Scheme.

- Δ_0-Separation can be derived in RCST and so in BCST.

The Global Replacement Rule

- The Replacement Scheme: For each formula $\phi[\underline{x}, z, y]$, where $\underline{x}, z, y$ is a list $x_1, \ldots, x_n, z, y$ of distinct variables:

$$\forall \underline{x} \forall x \{(\forall z \in x) \exists ! y \phi[\underline{x}, z, y] \rightarrow \exists a \forall y (y \in a \ \leftrightarrow \ (\exists z \in x) \phi[\underline{x}, z, y])\}$$

- The Global Replacement Scheme:

$$[\forall \underline{x} \forall z \exists ! y \phi[\underline{x}, z, y] \rightarrow \forall \underline{x} \forall x \exists a \forall y (y \in a \ \leftrightarrow \ (\exists z \in x) \phi[\underline{x}, z, y])$$

- The Global Replacement Rule (GRR):

$$\frac{\forall \underline{x} \forall z \exists ! y \phi[\underline{x}, z, y]}{\forall \underline{x} \forall x \exists a \forall y (y \in a \ \leftrightarrow \ (\exists z \in x) \phi[\underline{x}, z, y])}$$

- Rudimentary CST (RCST): Extensionality, Emptyset, Pairing, Union, Binary Intersection and GRR

The Rudimentary Functions (à la Jensen)

Definition: *[Ronald Jensen (1972)] A function* $f : V^n \to V$ *is Rudimentary if it is generated using the following schemata:*

(a) $f(\underline{x}) = x_i$

(b) $f(\underline{x}) = x_i - x_j$

(c) $f(\underline{x}) = \{x_i, x_j\}$

(d) $f(\underline{x}) = h(\underline{g}(\underline{x}))$

(e) $f(\underline{x}) = \cup_{z \in y} g(z, \underline{x})$

where $h : V^m \to V$, $\underline{g} = g_1, \ldots, g_m : V^n \to V$ *and* $g : V^{n+1} \to V$ *are rudimentary and* $1 \leq i, j \leq n$.

Note that $f(\underline{x}) = \emptyset = x_i - x_i$ is rudimentary; and so is $f(\underline{x}) = x_i \cap x_j = x_i - (x_i - x_j)$ using classical logic.

The Rudimentary Functions (à la CST)

Definition: *A function $f : V^n \to V$ is (CST)-Rudimentary if it is generated using the following schemata:*

(a) $f(\underline{x}) = x_i$

(b) $f(\underline{x}) = \emptyset$

(c) $f(\underline{x}) = f_1(\underline{x}) \cap f_2(\underline{x})$

(d) $f(\underline{x}) = \{f_1(\underline{x}), f_2(\underline{x})\}$

(e) $f(\underline{x}) = \cup_{z \in f_1(\underline{x})} f_2(z, \underline{x})$

Proposition: *The CST rudimentary functions are closed under composition ($f(\underline{x}) = h(\underline{g}(\underline{x}))$).*

Proposition: *Using classical logic, the CST rudimentary functions coincide with Jensen's rudimentary functions.*

The axiom system $RCST^*$, 1

- The language $\mathcal{L}^*_\in$ is obtained from $\mathcal{L}_\in$ by allowing individual terms t generated using the following syntax equation:

$$t ::= z \mid \emptyset \mid \{t_1, t_2\} \mid t_1 \cap t_2 \mid \cup_{z \in t_1} t_2[z]$$

Free occurences of z in $t_2[z]$ become bound in $\cup_{z \in t_1} t_2[z]$. $RCST^*$ has the Extensionality axiom and the following comprehension axioms for the forms of term of $\mathcal{L}^*_\in$:

$$\begin{array}{lllll} A1) & x \in \emptyset & \leftrightarrow & \bot \\ A2) & x \in t_1 \cap t_2 & \leftrightarrow & (x \in t_1 \wedge x \in t_2) \\ A3) & x \in \{t_1, t_2\} & \leftrightarrow & (x = t_1 \vee x = t_2) \\ A4) & x \in \cup_{z \in t_1} t_2[z] & \leftrightarrow & (\exists z \in t_1)\ (x \in t_2[z]) \end{array}$$

The axiom system $RCST^*$, 2

Some Definitions:

$$\{t\} \equiv \{t, t\}, \qquad \{t_2[z] \mid z \in t_1\} \equiv \cup_{z \in t_1}\{t_2[z]\}$$

$$\{t_2\}_{t_1} \equiv \{t_2 \mid z \in t_1\} \qquad \cup t \equiv \cup_{z \in t} z$$

$$[z \in t_1 \mid t_2[z]] \equiv \cup_{z \in t_1}\{z\}_{t_2[z]} \qquad t_1 \cup t_2 \equiv \cup\{t_1, t_2\}$$

$$< t_1 = t_2 > \equiv \{\emptyset\}_{\{t_1\} \cap \{t_2\}} \qquad < t_1 \subseteq t_2 > \equiv < t_1 \cap t_2 = t_1 >$$

Theorem: *There is an assignment of a term* $< \theta >$ *of* $\mathcal{L}^*_\in$ *to each* Δ_0*-formula* θ *of* $\mathcal{L}^*_\in$ *such that*

$$RCST^* \vdash [z \in < \theta >] \leftrightarrow [(z = \emptyset) \wedge \theta].$$

Corollary: *For each term* t *and each* Δ_0*-formula* $\theta[x]$ *of* $\mathcal{L}^*_\in$*, if* $\{x \in t \mid \theta[x]\} \equiv [x \in t \mid < \theta[x] >]$ *then*

$$RCST^* \vdash z \in \{x \in t \mid \theta[x]\} \leftrightarrow z \in t \wedge \theta[z].$$

The definition of $< \theta >$

The assignment of a term $< \theta >$ for each Δ_0-formula θ of $\mathcal{L}^*_\in$ is by structural recursion on θ using the following table.

$t_1 \in t_2$	$< \{t_1\} \subseteq t_2 >$
$\bot$	$\emptyset$
$\theta_1 \wedge \theta_2$	$< \theta_1 > \cap < \theta_2 >$
$\theta_1 \vee \theta_2$	$< \theta_1 > \cup < \theta_2 >$
$\theta_1 \rightarrow \theta_2$	$<< \theta_1 > \subseteq < \theta_2 >>$
$(\exists x \in t)\theta[x]$	$\cup_{x \in t} < \theta[x] >$
$(\forall x \in t)\theta[x]$	$< t \subseteq \{x \in t \mid \theta[x]\} >$

We have shown that each instance of Δ_0-Separation is a theorem of $RCST^*$.

The axiom system $RCST^*$, 3

Each term t whose free variables are taken from $\underline{x} = x_1, \ldots, x_n$ defines in an obvious way a function $F_t : V^n \to V$.

Proposition: *A function $f : V^n \to V$ is rudimentary iff $f = F_t$ for some term t of $\mathcal{L}^*_\in$.*

Proposition: *We can associate with each term t of $\mathcal{L}^*_\in$ a formula $\psi_t[y]$ of $\mathcal{L}_\in$ such that $RCST^* \vdash (y = t \;\leftrightarrow\; \psi_t[y])$ and $RCST \vdash \exists! y \psi_t[y]$.*

Definition: $RCST_0$ *is the axiom system in the language $\mathcal{L}_\in$ with the Extensionality axiom and the axioms $\exists y \psi_t[y]$ for terms t of $\mathcal{L}^*_\in$.*

Proposition: *Every theorem of $RCST_0$ is a theorem of $RCST$ and $RCST^*$ is a conservative extension of $RCST_0$.*

The definition of the $\psi_t[y]$

We simultaneously define formulae of $\mathcal{L}_\in$

- $\phi_t[x]$ such that $RCST^* \vdash (x \in t \leftrightarrow \phi_t[x])$ and
- $\psi_t[y]$ such that $RCST^* \vdash (y = t \leftrightarrow \psi_t[y])$

by structural recursion on terms t of $\mathcal{L}^*_\in$:

$$\psi_t[y] \equiv \forall x(x \in y \leftrightarrow \phi_t[x])$$

t	$\phi_t[x]$
z	$x \in z$
$\emptyset$	$\bot$
$\{t_1, t_2\}$	$\psi_{t_1}[x] \vee \psi_{t_2}[x]$
$t_1 \cap t_2$	$\phi_{t_1}[x] \wedge \phi_{t_2}[x]$
$\cup_{z \in t_1} t_2[z]$	$\exists z(\phi_{t_1}[z] \wedge \phi_{t_2[z]}[x])$

The axiom system $RCST^*$, 4

If ϕ is a formula of $\mathcal{L}^*_\in$ let $\phi^\sharp$ be the formula of $\mathcal{L}_\in$ obtained from ϕ by replacing each atomic formula $t_1 = t_2$ by $\exists y(\psi_{t_1}[y] \wedge \psi_{t_2}[y])$ and each atomic formula $t_1 \in t_2$ by $\exists y(\psi_{t_1}[y] \wedge \phi_{t_2}[y])$.

Proposition: *For each formula ϕ of $\mathcal{L}^*_\in$*

1. $RCST^* \vdash (\phi \quad \leftrightarrow \quad \phi^\sharp)$,
2. $\vdash (\phi \quad \leftrightarrow \quad \phi^\sharp)$ *if ϕ is a formula of $\mathcal{L}_\in$,*
3. $RCST^* \vdash \phi$ *implies* $RCST_0 \vdash \phi^\sharp$.

Theorem: *[The Term Existence Property] If $RCST_0 \vdash \exists y \phi[y, \underline{x}]$ then $RCST^* \vdash \phi[t[\underline{x}], \underline{x}]$ for some term $t[\underline{x}]$ of $\mathcal{L}^*_\in$.*

Proof Idea: Use Friedman Realizability, as in Myhill (1973).

Corollary: *The Replacement Rule is admissible for $RCST^*$ and hence $RCST \vdash \phi$ implies $RCST^* \vdash \phi$.*

The axiom system $RCST^*$, 5

Corollary: *$RCST$ has the same theorems as $RCST_0$.*
Corollary: *$RCST^*$ is a conservative extension of $RCST$.*
Proposition: *$RCST_0$ is finitely axiomatizable.*

The proof uses a constructive version of the result of Jensen that the rudimentary functions can be finitely generated using function composition.

The Rudimentary Relations

Define $0 = \emptyset, 1 = \{0\}, 2 = \{0, 1\}$, etc. and let Ω be the class of all subsets of 1.

Definition: *A relation $R \subseteq V^n$ is a rudimentary relation if its characteristic function $c_R : V^n \to \Omega$, where*

$$c_R(\underline{x}) = \{z \in 1 \mid R(\underline{x})\},$$

is a rudimentary function.

Proposition: *A relation is rudimentary iff it can be defined, in RCST, by a Δ_0 formula.*

Proposition: *If $R \subseteq V^{n+1}$ and $g : V^n \to V$ are rudimentary then so are $f : V^n \to V$ and $S \subseteq V^n$, where*

$$f(\underline{x}) = \{z \in g(\underline{x}) \mid R(z, \underline{x})\}$$

and

$$S(\underline{x}) \ \leftrightarrow \ R(g(\underline{x}), \underline{x}).$$

Some References

Jensen, Ronald *The Fine Structure of the Constructible Hierarchy*, Annals of Math. Logic 4, pp. 229-308 (1972)
Jensen's definition of the rudimentary functions.

Myhill, John *Some Properties of Intuitionistic Zermelo-Fraenkel set theory*, in Matthias, A. and Rogers, H., (eds.) Cambridge Summer School in Mathematical Logic, pp. 206-231, LNCS 337 (1973)
The Myhill-Friedman proof of the Set Existence Property for IZF using Friedman realizability.

Part II

Arithmetical CST

The class of natural numbers

We use class notation, as is usual in set theory. So if $A = \{x \mid \phi[x]\}$ then $x \in A \ \leftrightarrow \ \phi[x]$.
A class X is inductive, written $Ind(X)$, if

$$0 \in X \wedge (\forall z \in X)\ z^+ \in X,$$

where $0 = \emptyset$ and $t^+ = t \cup \{t\}$.
Definition:

$$Nat \equiv \{x \mid \forall y \in x^+ (Trans(y) \wedge (y = 0 \vee Succ(y)))\}$$

where

$$Trans(y) \equiv \forall z \in y\ z \subseteq y \text{ and } Succ(y) \equiv (\exists z \in y)(y = z^+).$$

Note that Nat is inductive.

The Mathematical Induction Scheme

The Scheme: $Ind(X) \rightarrow Nat \subseteq X$ for each class X; i.e. Nat is the smallest inductive class.

Proposition: *Each instance of Mathematical Induction can be derived assuming* $RCST^*$*+Set Induction.*

- We focus on the axiom system, Arithmetical CST $(ACST)$, where $ACST \equiv RCST^*$+Mathematical Induction.

- This axiom system has the same proof theoretic strength as Peano Arithmetic and is probably conservative over HA.

- A set X is finite/finitely enumerable if there is a bijection/surjection $n \rightarrow X$ for some $n \in Nat$.
- *Note:* A set is finite iff it is finitely enumerable and discrete (equality on the set is decidable).

Two Theorems of $ACST$

Theorem: *[The Finite AC Theorem] For classes B, R, if A is a finite set such that $(\forall x \in A)(\exists y \in B)[(x, y) \in R]$ then there is a set function $f : A \to B$, such that $(\forall x \in A)[(x, f(x)) \in R]$.*

Proof: Use mathematical induction on the size of A.

Theorem: *[The Finitary Strong Collection Theorem] For classes B, R, if A is a finitely enumerable set such that $(\forall x \in A)(\exists y \in B)[(x, y) \in R]$ then there is a finitely enumerable set $B_0 \subseteq B$ such that*

$$(\forall x \in A)(\exists y \in B_0)[(x, y) \in R] \ \& \ (\forall y \in B_0)(\exists x \in A)[(x, y) \in R]$$

Proof: Let $g : n \to A$ be a surjection, where $n \in Nat$, so that $(\forall k \in n)(\exists y \in B)[(g(k), y) \in R]$. By the finite AC theorem there is a function $f : n \to B$ such that, for all $m \in n$, $(g(m), f(m)) \in R$. The desired finitely enumerable set B_0 is $\{f(m) \mid m \in n\}$.

Inductive Definitions

- Any class Φ can be viewed as an inductive definition, having as its (inference) steps all the ordered pairs $(X, a) \in \Phi$.
- A step will usually be written X/a, with the elements of X the premisses of the step and a the conclusion of the step.
- A class Y is Φ-closed if, for each step X/a of Φ,

$$X \subseteq Y \;\Rightarrow\; a \in Y.$$

- Φ is generating if there is a smallest Φ-closed class; i.e. a class Y such that (i) Y is a Φ-closed class, and (ii) $Y \subseteq Y'$ for each Φ-closed class Y'.
- Any smallest Φ-closed class is unique and is written $I(\Phi)$ and called the class inductively defined by Φ

Finitary Inductive Definitions

- An inductive definition Φ is finitary if X is finitely enumerable for every step X/a of Φ.

Theorem: *[$ACST$] Each finitary inductive definition is generating.*

Example: The finitary inductive definition, having the steps X/X for all finitely enumerable sets X, generates the class HF of hereditarily finitely enumerable sets.

The Primitive Recursion Theorem

- Theorem: Let $G_0 : B \to A$ and $F : Nat \times B \times A \to A$ be class functions, where A, B are classes. Then there is a unique class function $G : Nat \times B \to A$ such that, for all $b \in B$ and $n \in Nat$,

$$(*) \quad \begin{cases} G(0, b) & = G_0(b), \\ G(n^+, b) & = F(n, b, G(n, b)), \end{cases}$$

- Proof: : Let $G = I(\Phi)$, where Φ is the inductive definition with steps $\emptyset/((0, b), G_0(b))$, for $b \in B$, and $\{((n, b), x)\}/(n^+, F(n, b, x))$ for $(n, b, x) \in Nat \times B \times A$.
- It is routine to show that G is the unique required class function.
  ■

$HA \leq (ACST)$

- Theorem: There are unique binary class functions $Add, Mult : Nat \times Nat \to Nat$ such that, for $n, m \in Nat$,
  1. $Plus(n, 0) = n$,
  2. $Plus(n, m^+) = Plus(n, m)^+$,
  3. $Mult(n, 0) = 0$,
  4. $Mult(n, m^+) = Plus(Mult(n, m), n)$.
- Proof: Apply the Primitive Recursion theorem with $A = B = Nat$, first with $F(n, m, k) = k^+$ to obtain $Plus$ and then with $F(n, m, k) = Plus(k, n)$ to obtain $Mult$.
  ■
- Using this result it is clear that there is an obvious standard interpretation of Heyting Arithmetic in $BCST_- + MathInd$.

The Finite AC Theorem, 1

Theorem[$ACST$]: For each class B and each class R, if A is a finite set such that

$$(\forall x \in A)(\exists y \in B)[(x, y) \in R]$$

then there is a set, that is a function $f : A \to B$, such that

$$(\forall x \in A)[(x, f(x)) \in R].$$

We present results and proofs informally using standard set and class notation and terminology.

Proof: Let $g : n \sim A$ be a bijection, where $n \in Nat$, so that

$$(\forall k \in n)(\exists y \in B)[(g(k), y) \in R].$$

The Finite AC Theorem, 2

Proof: Let $g : n \sim A$ be a bijection, where $n \in Nat$, so that

$$(\forall k \in n)(\exists y \in B)[(g(k), y) \in R].$$

- If $m \in n^+$ call $h : m \to B$ m-good if

$$(\forall k \in m)[(g(k), h(k)) \in R].$$

- Let X be the class of $m \in Nat$ such that if $m \in n^+$ then there is an m-good $h : m \to B$.
- Claim: X is inductive and hence $Nat \subseteq X$.
- By the claim, as $n \in n^+$ there is an n-good function h.
- Then $\{(g(k), h(k)) \mid k \in n\}$ is a function $f : A \to B$ such that $(\forall x \in A)[(x, f(x)) \in R]$.
■

Finitary Strong Collection

Theorem[Finitary Strong Collection]: For each class B and each class R, if A is a finitely enumerable set such that

$$(\forall x \in A)(\exists y \in B)[(x, y) \in R]$$

then there is a set $B_0 \subseteq B$ such that

$$(\forall x \in A)(\exists y \in B_0)[(x, y) \in R] \;\&\; (\forall y \in B_0)(\exists x \in A)[(x, y) \in R]$$

Proof: Let $g : n \to A$ be a surjection, where $n \in Nat$, so that

$$(\forall k \in n)(\exists y \in B)[(g(k), y) \in R].$$

By the finite AC theorem there is a function $f : n \to B$ such that, for all $m \in n$, $(g(m), f(m)) \in R$. The desired finitely enumerable set B_0 is $\{f(m) \mid m \in n\}$. $\square$

Note: $B_0 = \{y \in \cup \cup f \mid (\exists x \in \cup \cup f)\ (x, y) \in f\}$.

The finitary inductive definition theorem

Theorem: Each finitary inductive definition is generating.
Proof: Let Φ be a finitary inductive definition. For each class X let

$$\Gamma X = \{y \mid (\exists Y \in Pow(X))\ [Y/y \text{ is a step in } \Phi]\}.$$

- For G a subclass of $Nat \times V$ and $n \in Nat$ let

$$G^n = \{y \mid (n, y) \in G\} \text{ and } G^{<n} = \bigcup_{m \in n} G^m.$$

- Call such a class G *good* if $G^n \subseteq \Gamma G^{<n}$ for all $n \in Nat$, and let $J = \bigcup\{G \mid G \text{ is a good set}\}$ and $I = \bigcup_{n \in Nat} J^n$.

Claim 1: (i) J is a good class and (ii) if X is a Φ-closed class then $I \subseteq X$.

Proof of Claim 1

(i) J is a good class.

Proof: Let $y \in J^n$, with $n \in Nat$.

Then $y \in G^n \subseteq \Gamma G^{<n}$ for some good set G.

As Γ is monotone $y \in \Gamma J^{<n}$. Thus $J^n \subseteq \Gamma J^{<n}$.

(ii) if X is a Φ-closed class then $I \subseteq X$.

Proof: Assume that X is Φ-closed; i.e. $\Gamma X \subseteq X$.

Then, by (i), using $MathInd$, $J^n \subseteq X$ for all $n \in Nat$.

Hence $I \subseteq X$.

Proof that I is Φ-closed, 1

Proof: Let Y/a be a Φ-step for some $Y \subseteq I$; i.e.

$$(\forall y \in Y)(\exists G)[G \text{ is a good set and } (\exists n \in Nat)\ y \in G^n].$$

By Finitary Strong Collection, as Y is finitely enumerable there is a finitely enumerable set $\mathcal{Y}$ of good sets such that

$$(\forall y \in Y)(\exists G \in \mathcal{Y})(\exists n \in Nat)\ y \in G^n.$$

Hence $(\forall y \in Y)(\exists n \in Nat)(\exists G \in \mathcal{Y})\ y \in G^n.$

So, by Finitary Strong Collection again there is a finitely enumerable subset P of Nat such that

$$(\forall y \in Y)(\exists n \in P)(\exists G \in \mathcal{Y})\ y \in G^n.$$

Proof that I is Φ-closed, 2

- $P \subseteq Nat$ is finitely enumerable such that

$$(\forall y \in Y)(\exists n \in P)(\exists G \in \mathcal{Y})\ y \in G^n$$

where $\mathcal{Y}$ is a class of good sets.

- As $P \subseteq Nat$ is finitely enumerable, $P \subseteq m$ for some $m \in Nat$.
- Let $G_0 = \bigcup \mathcal{Y}$ is good, as it is a union of good sets.
- As $P \subseteq m$, $Y \subseteq G_0^{<m}$.
- As Y/a is a Φ-step, $a \in \Gamma G_0^{<m}$.
- Hence $G = G_0 \cup \{(m, a)\}$ is good, so that $a \in G^m \subseteq J^m \subseteq I$. $\square$

Hereditarily Finite sets

- The class HF of hereditarily finitely enumerable sets is the smallest class such that every finitely enumerable subset of the class is in the class; i.e. $HF = I(\{X/X \mid X$ is a finitely enumerable set $\})$.

Theorem:

1. $HF = I(\{X/X \mid X$ is a finite set $\})$.
2. HF is the smallest class Y such that $\emptyset \in Y$ and if $a, b \in Y$ then $a \cup \{b\} \in Y$.

Transitive Closure

- A class Y is transitive if $(\forall x \in Y)\ x \subseteq Y$.
- Theorem: For each class A there is a smallest transitive class $TC(A)$ that includes A.
- Proof: $TC(A) = I(\Phi)$ where Φ is the inductive definition with steps $\emptyset/x$ for $x \in A$ and $\{y\}/x$ for sets x, y such that $x \in y$.

Adding an Infinity axiom

- Infinity Axiom: Nat is a set

- Using the Infinity axiom I have been unable to derive the following assertion.

- If Φ is a finitary inductive definition such that $\{y \mid X/y \in \Phi\}$ is a set for each set X then $I(\Phi)$ is a set.
- I believe that I can derive it if I also assume the following scheme.
- For each class A and each class function $F : A \to A$, if $a_0 \in A$ then $\{g(n) \mid n \in Nat\}$ is a set, where $g(0) = a_0$ and $g(n^+) = F(g(n))$ for $n \in Nat$.