Some Weak Axiom Systems for CST

Kanazawa workshop on Constructive Aspects of Logic and Mathematics,

March 8-12, 2010

.

Peter Aczel

petera@cs.man.ac.uk

Manchester University, visiting LMU, Munich

Part I: Rudimentary CST

Part II: Arithmetical CST

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 Replacement Rule (RR) instead of the Replacement Scheme.

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

The Replacement Rule

- Recall the Replacement Scheme:

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

for each formula $\phi[\underline{x}, z, y]$, where $\underline{x}$ is a list $x_1, \ldots, x_n$ of distinct variables.

Replacement Rule (RR):

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

Rudimentary CST (RCST):

Extensionality, Emptyset, Pairing, Union, Binary Intersection

and RR

The Rudimentary Functions (à la Jensen)

Definition: *[Ronald Jensen (1972)] A function $f : V^n \longrightarrow V$ 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 $h : V^m \longrightarrow V$, $\underline{g} = g_1, \ldots, g_m : V^n \longrightarrow V$ and $g : V^{n+1} \longrightarrow V$ 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 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

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

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 $\mathcal{L}_\in^*$:

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

The axiom system $RCST^*$, 2

Theorem: *For each term t and each Δ_0-formula $\phi[z]$ of $\mathcal{L}^*_\in$ there is a term t' of $\mathcal{L}^*_\in$ such that $RCST^* \vdash (z \in t' \leftrightarrow z \in t \wedge \phi[z])$. We write $\{z \in t \mid \phi[z]\}$ for this term t'.*

Some Definitions: Note: $(x, y) \in t \to x, y \in \cup\cup t$.

$$\{t\} \equiv \{t, t\}, \qquad (t_1, t_2) \equiv \{\{t_1\}, \{t_1, t_2\}\}$$

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

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

$$t_1 \times t_2 \equiv \cup_{x_1 \in t_1} \cup_{x_2 \in t_2} \{(t_1, t_2)\}$$

$$dom(t) \equiv \{x \in \cup\cup t \mid \exists y \in \cup\cup t\ (x, y) \in t\}$$

$$ran(t) \equiv \{y \in \cup\cup t \mid \exists x \in \cup\cup t\ (x, y) \in t\}$$

$$t_1{}' t_2 \equiv \cup\{y \in ran(t_1) \mid (t_2, y) \in t_1\}, \qquad t_1{}'' t_2 \equiv \{t_1' x \mid x \in t_2\}$$

Note: $f'x = f(x)$ and $f''y = \{f(x) \mid x \in y\}$ if $f : a \to b$ and $x \in a, y \subseteq a$.

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 axiom system $RCST^*$, 4

We simultaneously define formulae $\phi_t[x]$ 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 $RCST^*$, 5

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. $RCST^* \vdash (\phi \leftrightarrow \phi^\sharp)$,
2. $\vdash (\phi \leftrightarrow \phi^\sharp)$ *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 $RCST^*$, 6

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.

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

$$x \in A \ \leftrightarrow \ \phi[x].$$

Let $0 = \emptyset$ and $t^+ = t \cup \{t\}$. A class X is inductive if

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

or equivalently, if $\Gamma X \subseteq X$ where $\Gamma X \equiv \{0\} \cup \{z^+ \mid z \in X\}$.
Definition: $Nat \equiv \{x \mid \forall y \in x^+(Trans(y) \wedge y \in \Gamma y)\}$ *where* $Trans(y) \equiv \forall z \in y\ z \subseteq y$.

Note that Nat is inductive.

The Mathematical Induction Scheme

The Scheme: $\Gamma X \subseteq X \to Nat \subseteq X$ 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.*

If $Trans(y)$ is left out of the definition of Nat this does not seem possible.

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.

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 $f : A \rightarrow B$, 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 $(\forall x \in A)(\exists y \in B)[(x, y) \in R]$ 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 $g : n \rightarrow A$ 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 $f : n \rightarrow B$ 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

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

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.