Non-principal ultrafilters, program extraction and higher order reverse mathematics

Alexander P. Kreuzer

Technische Universität Darmstadt, Germany

Colloquium Logicum, Paderborn, September 2012

Higher order arithmetic

Definition (RCA_0^ω, Kohlenbach '05)

RCA_0^ω is the finite type extension of RCA_0:

- Sorted into type 0 for $\mathbb{N}$, type 1 for $\mathbb{N}^\mathbb{N}$, type 2 for $\mathbb{N}^{\mathbb{N}^\mathbb{N}}$, $\ldots$,
- contains basic arithmetic: 0, successor, $+$, $\cdot$, λ-abstraction,
- quantifier-free axiom of choice restricted to choice of numbers over functions ($\mathsf{QF}\text{-}\mathsf{AC}^{1,0}$), i.e.,

$$\forall f^1 \, \exists y^0 \, \mathsf{A}_{qf}(f, y) \rightarrow \exists G^2 \, \forall f^1 \, \mathsf{A}_{qf}(f, G(f))$$

- and a recursor R_0, which provides primitive recursion (for numbers),

$$R_0(0, y^0, f) = y, \qquad R_0(x+1, y, f) = f(R_0(x, y, f), x),$$

- Σ_1^0-induction.

The closed terms of RCA_0^ω will be denoted by T_0.
Proofs in RCA_0^ω can be simulated in RCA_0 and vice versa.

Arithmetical comprehension

Let Π^0_1-CA be the schema

$$\forall f\, \exists g\, \forall n\ (g(n) = 0 \leftrightarrow \forall x\, f(n,x) = 0)\,.$$

Define ACA^ω_0 to be $\mathsf{RCA}^\omega_0 + \Pi^0_1$-CA.

Let Feferman's μ be

$$\mu(f) := \begin{cases} \min\{x \mid f(x) = 0\} & \text{if } \exists x\, f(x) = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Denote by (μ) be the statement that μ exists.

Theorem

- $\mathsf{RCA}^\omega_0 + (\mu) \vdash \Pi^0_1$-CA
- $\mathsf{RCA}^\omega_0 + (\mu)$ *is* Π^1_2*-conservative over* ACA^ω_0

Functional interpretation

Theorem (Functional interpretation relative to μ)

If

$$\mathsf{RCA}_0^\omega + (\mu) \vdash \forall x\, \exists y\, \mathsf{A}_{qf}(x, y)$$

the one can extract a term $t \in T_0[\mu]$, *such that*

$$\mathsf{RCA}_0^\omega + (\mu) \vdash \forall x\, \mathsf{A}_{qf}(x, t(x)).$$

See Avigad, Feferman in Handbook of Proof Theory
and Kohlenbach: Applied Proof Theory.

Non-principal ultrafilters

A set $\mathcal{U} \subseteq \mathcal{P}(\mathbb{N})$ is a *non-principal ultrafilter over* $\mathbb{N}$ if

- $\forall X \left(X \in \mathcal{U} \vee \overline{X} \in \mathcal{U}\right)$,
- $\forall X, Y \ (X \in \mathcal{U} \wedge X \subseteq Y \rightarrow Y \in \mathcal{U})$,
- $\forall X, Y \ (X, Y \in \mathcal{U} \rightarrow X \cap Y \in \mathcal{U})$,
- $\forall X \ (X \in \mathcal{U} \rightarrow X$ is infinite$)$.

The existence of a non-principal ultrafilter is not provable in ZF.

Non-principal ultrafilters

A set $\mathcal{U} \subseteq \mathcal{P}(\mathbb{N})$ is a *non-principal ultrafilter over* $\mathbb{N}$ if

- $\forall X \, \big(X \in \mathcal{U} \vee \overline{X} \in \mathcal{U}\big)$,
- $\forall X, Y \, (X \in \mathcal{U} \wedge X \subseteq Y \to Y \in \mathcal{U})$,
- $\forall X, Y \, (X, Y \in \mathcal{U} \to X \cap Y \in \mathcal{U})$,
- $\forall X \, (X \in \mathcal{U} \to X$ is infinite$)$.

Coding sets as characteristic function, i.e, $n \in X :\equiv [X(n) = 0]$, this can be formulated in RCA_0^ω:

$$(\mathcal{U}): \begin{cases} \exists \mathcal{U}^2 \, (\, \forall X^1 \, \big(X \in \mathcal{U} \vee \overline{X} \in \mathcal{U}\big) \\ \qquad \wedge \forall X^1, Y^1 \, (X \cap Y \in \mathcal{U} \to Y \in \mathcal{U}) \\ \qquad \wedge \forall X^1, Y^1 \, (X, Y \in \mathcal{U} \to (X \cap Y) \in \mathcal{U}) \\ \qquad \wedge \forall X^1 \, (X \in \mathcal{U} \to \forall n \, \exists k > n \, (k \in X)) \\ \qquad \wedge \forall X^1 \, (\mathcal{U}(X) =_0 \mathrm{sg}(\mathcal{U}(X)) =_0 \mathcal{U}(\lambda n. \mathrm{sg}(X(n)))) \,) \end{cases}$$

Lower bound on the strength of $\mathsf{RCA}_0^\omega + (\mathcal{U})$

Theorem (K.)

$$\mathsf{RCA}_0^\omega + (\mathcal{U}) \vdash (\mu)$$

In particular, $\mathsf{RCA}_0^\omega + (\mathcal{U})$ *proves arithmetical comprehension.*

Proof.

Let $f\colon \mathbb{N} \to \mathbb{N}$ and set $X_f := \{n \mid \exists m \leq n \; f(m) = 0\}$.
Then

$$\begin{aligned} \exists n \, (f(n) = 0) &\iff X_f \text{ is cofinite} \\ &\iff X_f \in \mathcal{U} \end{aligned}$$

Thus

$$\forall f \, (X_f \in \mathcal{U} \to \exists n \, (f(n) = 0 \land \forall n' < n \, f(n) \neq 0))$$

$\mathsf{QF\text{-}AC}^{1,0}$ yields a functional satisfying (μ). □

Upper bound on the strength of $\mathsf{RCA}_0^\omega + (\mathcal{U})$

Theorem (K.)

$\mathsf{RCA}_0^\omega + (\mathcal{U})$ *is* Π^1_2*-conservative over* $\mathsf{RCA}_0^\omega + (\mu)$ *and thus also over* ACA_0^ω*.*

Proof sketch

Suppose $\mathsf{RCA}_0^\omega + (\mathcal{U}) \vdash \forall f\, \exists g\, \mathsf{A}(f,g)$ and A does not contain $\mathcal{U}$.

1. The functional interpretation yields a term $t \in T_0[\mu]$, such that

$$\forall f\, \mathsf{A}(f, t(\mathcal{U}, f)).$$

2. Normalizing t, such that each occurrence of $\mathcal{U}$ in t is of the form

$$\mathcal{U}(t'(n^0)) \qquad \text{for a term } t'(n^0) \in T_0[\mathcal{U}, \mu, f].$$

   In particular, $\mathcal{U}$ is only used on countably many sets (for each fixed f).

3. Build in $\mathsf{RCA}_0^\omega + (\mu)$ a filter which acts on these sets as ultrafilter.

Step 1: Functional interpretation

Suppose $\mathsf{RCA}_0^\omega + (\mathcal{U}) \vdash \forall f^1\, \exists g^1\, \mathsf{A}(f,g)$
where A is arithmetical and does not contain $\mathcal{U}$.

Modulo μ the formula A is quantifier-free.
Recall $(\mathcal{U})$:

$$(\mathcal{U}):\ \begin{cases} \exists \mathcal{U}^2\, (\ \forall X^1\, \left(X \in \mathcal{U} \vee \overline{X} \in \mathcal{U}\right) \\ \qquad \wedge \forall X^1, Y^1\, (X \cap Y \in \mathcal{U} \to Y \in \mathcal{U}) \\ \qquad \wedge \forall X^1, Y^1\, (X, Y \in \mathcal{U} \to (X \cap Y) \in \mathcal{U}) \\ \qquad \wedge \forall X^1\, (X \in \mathcal{U} \to \forall n\, \exists k > n\, (k \in X)) \\ \qquad \wedge \forall X^1\, (\mathcal{U}(X) =_0 \mathrm{sg}(\mathcal{U}(X)) =_0 \mathcal{U}(\lambda n.\, \mathrm{sg}(X(n)))) \,) \end{cases}$$

Modulo $\mathsf{RCA}_0^\omega + (\mu)$ this is of the form $\exists \mathcal{U}^2\, \forall Z^1\, (\mathcal{U})_{\mathit{qf}}(\mathcal{U}, Z)$.
Thus

$$\mathsf{RCA}_0^\omega + (\mu) \vdash \forall \mathcal{U}^2\, \forall f^1\, \exists Z^1\, \exists g^1\, \Big((\mathcal{U})_{\mathit{qf}}(\mathcal{U}, Z) \to \mathsf{A}_{\mathit{qf}}(f,g)\Big).$$

Step 1: Functional interpretation (cont.)

$$\mathsf{RCA}_0^\omega + (\mu) \vdash \forall \mathcal{U}^2 \, \forall f^1 \, \exists Z^1 \, \exists g^1 \left((\mathcal{U})_{\mathsf{qf}}(\mathcal{U}, Z) \to \mathsf{A}_{\mathsf{qf}}(f, g) \right).$$

The functional interpretation extracts terms $t_Z, t_g \in T_0[\mu]$, such that

$$\mathsf{RCA}_0^\omega + (\mu) \vdash \forall \mathcal{U}^2 \, \forall f^1 \left((\mathcal{U})_{\mathsf{qf}}(\mathcal{U}, t_Z(\mathcal{U}, f)) \to \mathsf{A}_{\mathsf{qf}}(f, t_g(\mathcal{U}, f)) \right).$$

Step 2: Term normalization

The terms t_Z, t_g are made of

- 0, successor, $+$, $\cdot$, λ-abstraction
- the primitive recursor R_0, i.e.

$$R_0(0, y, f) = y, \qquad R_0(x+1, y, f) = f(R_0(x, y, f), x),$$

- μ^2 and
- the parameters $\mathcal{U}^2, f^1$.

With coding R_0 is of type 2. The functional $\mathcal{U}$ is also of type 2.
$\Longrightarrow$ no functional can take $\mathcal{U}$ as parameter.

Lemma

The terms t_Z, t_g can be normalized, such that each occurrence of $\mathcal{U}$ is of the form

$$\mathcal{U}(t'(n^0)) \qquad \textit{for a term } t' \textit{ possible containing } \mathcal{U}, f.$$

Step 3: Construction of (a substitute for) $\mathcal{U}$

We fix an f and construct a filter $\mathcal{F}$, such that

$$\mathsf{RCA}_0^\omega + (\mu) \vdash (\mathcal{U})_{qf}(\mathcal{F}, t_Z(\mathcal{F}, f)). \qquad (*)$$

This yields then

$$\mathsf{RCA}_0^\omega + (\mu) \vdash \forall f\, \mathsf{A}_{qf}(f, t_g(\mathcal{F}, f))$$

and thus the theorem.

Let $t_1, \dots, t_k$ be the list term with $\mathcal{U}(t_j(n))$ in t_Z, t_g.

- Assume that $t_1, \dots$ is ordered according to the subterm ordering.
- We start with the trivial filter $\mathcal{F}_0 = \{\mathbb{N}\}$.
- For each t_i we build a refined $\mathcal{F}_i \supseteq \mathcal{F}_{i-1}$ such that $(\mathcal{U})_{qf}$ relativized the sets coded by $t_1, \dots, t_i$ holds.
- $\mathcal{F} := \mathcal{F}_k$ solves then $(*)$.

Step 3: Sketch of the construction of $\mathcal{F}_1$

Let $\mathcal{A} := \{A_1, A_2, \dots\}$ be the set of subsets of $\mathbb{N}$ coded by t_1.
We assume that $\mathcal{A}$ is closed under union, intersection and inverse.

We want a filter $\mathcal{F}_1$, such that

- $\forall X \in \mathcal{A} \left(X \in \mathcal{F}_1 \vee \overline{X} \in \mathcal{F}_1 \right)$,
- $\forall X, Y \in \mathcal{A} \, (X \in \mathcal{F}_1 \wedge X \subseteq Y \rightarrow Y \in \mathcal{F}_1)$,
- $\forall X, Y \in \mathcal{A} \, (X, Y \in \mathcal{F}_1 \rightarrow X \cap Y \in \mathcal{F}_1)$,
- $\forall X \in \mathcal{A} \, (X \in \mathcal{F}_1 \rightarrow X$ is infinite$)$.

Construction:

- We decide for each $i = 1, 2, \dots$ whether we put A_i or $\overline{A_i}$ into $\mathcal{F}_1$.
- We put A_i into $\mathcal{F}_1$ if the *intersection of A_i with the previously chosen sets* is infinite. Otherwise we put $\overline{A_i}$ into $\mathcal{F}_1$.

Program extraction

Corollary (to the proof)

If $\mathsf{RCA}_0^\omega + (\mathcal{U}) \vdash \forall f\, \exists g\, \mathsf{A}_{qf}(f,g)$ *and* A_{qf} *does not contain* $\mathcal{U}$ *then one can extract a term* $t \in T_0[\mu]$*, such that*

$$\mathsf{RCA}_0^\omega + (\mu) \vdash \mathsf{A}_{qf}(f, t(f)).$$

Corollary

If $\mathsf{RCA}_0^\omega + (\mathcal{U}) \vdash \forall f\, \exists g\, \mathsf{A}_{qf}(f,g)$ *and* A_{qf} *does not contain* $\mathcal{U}$ *then one can extract a term* t *in Gödel's System* T*, such that*

$$\mathsf{A}_{qf}(f, t(f))$$

Proof.

- The previous corollary yields a term primitive recursive in μ.
- Interpreting the term using the bar recursor $B_{0,1}$ and then using Howard's ordinal analysis gives a term $t \in T$. □

Extension: Idempotent ultrafilters

- The set of all ultrafilter on $\mathbb{N}$ can be identified with the Stone-Čech compactification $\beta\mathbb{N}$ of $\mathbb{N}$.
- Addition $+$ can be extended from $\mathbb{N}$ to $\beta\mathbb{N}$:

$$X \in \mathcal{U} + \mathcal{V} \qquad \text{iff} \qquad \{n \mid (X - n) \in \mathcal{U}\} \in \mathcal{V}$$

Theorem (Ellis '58)

Every left-topological compact semi-group contains an idempotent.

Thus, there exists an *idempotent* ultrafilter, i.e. a $\mathcal{U}$ with $\mathcal{U} + \mathcal{U} = \mathcal{U}$.
Let $(\mathcal{U}_{\mathrm{idem}})$ be the statement that an idempotent ultrafilter exists.

Theorem (K.)

- $\mathsf{RCA}_0^\omega \vdash (\mathcal{U}_{idem}) \to \mathsf{IHT}$
- $\mathsf{ACA}_0^\omega + (\mu) + \mathsf{IHT} + (\mathcal{U}_{idem})$ *is* Π^1_2*-conservative over* $\mathsf{ACA}_0^\omega + \mathsf{IHT}$*.*

Possible Applications

Possible Applications:

- Program extraction for ultralimit arguments e.g.,
  - from fixed point theory,
  - Gromov's Theorem,
  - Ergodic theory.
- Program extraction for non-standard arguments.

Summary

- The Π^1_2-consequences of $\mathsf{RCA}^\omega_0 + (\mathcal{U})$ and the Π^1_2-consequences of ACA^ω_0 are the same.
- Program extraction for $\mathsf{RCA}^\omega_0 + (\mathcal{U})$.
- The Π^1_2-consequences of $\mathsf{RCA}^\omega_0 + (\mathcal{U}_{\mathrm{idem}})$ and the Π^1_2-consequences of $\mathsf{ACA}^\omega_0 + \mathsf{IHT}$ are the same.

Thank you for your attention!

References

Alexander P. Kreuzer
Non-principal ultrafilters, program extraction and higher order reverse mathematics
Journal of Mathematical Logic **12** (2012), no. 1.

Alexander P. Kreuzer
On idempotent ultrafilters in higher-order reverse mathematics
preprint, `arXiv:1208.1424`.