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

Alexander P. Kreuzer

ENS Lyon

Mathematical Structures of Computation
Week 1: Recent developments in Type Theory
January 13th, 2014

Outline

Reverse mathematics

Reverse mathematics is a program which establishes which set existence axioms are necessary to prove a theorem.

- The usual systems of reverse mathematics are two-sorted.
  - One sort for $\mathbb{N}$ and
  - one for subsets of $\mathbb{N}$.
- Base system RCA_0.
  RCA_0 contains
  - basic arithmetic, Σ^0_1-induction,
  - the statement that all computable sets exist.
- Question in Reverse mathematics is:
  To what (set-existence) axioms is a theorem equivalent relative to RCA_0?

Example: Monotone convergence principle

Each increasing sequence of $(x_n) \subseteq \mathbb{Q}$ in $[0,1]$ has a supremum.

- This can be formulated in RCA_0 in the following way.
  - Rational numbers $x = \frac{p}{q}$ will be coded as a pair $\langle p, q \rangle := 2^p \cdot 3^q$.
  - The sequence $x_n = \frac{p_n}{q_n}$ will be coded as the set

$$\{\langle n, 2^{p_n} \cdot 3^{q_n} \rangle \colon n \in \mathbb{N}\}.$$

  - Want: for each n a 2^{-n} good approximation to the supremum.
- Solution:

$$\{\langle n, q_m \rangle \mid \forall m' > m \; (q_{m'} -_{\mathbb{Q}} q_m <_{\mathbb{Q}} 2^{-n})\}$$

- This set is build by arithmetical quantification, i.e. contains quantification of natural numbers.
- The monotone convergence principle is equivalent to the corresponding system ACA_0.

Reverse mathematics

- Many theorems form mathematics can be analyzed this way.
- Most of them can be show to be equivalent to one of the big five systems.

$$\mathsf{RCA}_0 \leftarrow \mathsf{WKL}_0 \leftarrow \mathsf{ACA}_0 \leftarrow \mathsf{ATR}_0 \leftarrow \Pi^1_1\text{-}\mathsf{CA}_0$$

Higher order statement cannot be formulated in these systems.

Higher order arithmetic

Definition (RCA_0^ω, Recursive comprehension, 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 ($\mathsf{QF\text{-}AC}^{1,0}$), i.e.,

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

- 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.
In Kohlenbach's books this system is denoted by $\widehat{\mathsf{E\text{-}PA}}^\omega\!\restriction + \mathsf{QF\text{-}AC}^{1,0}$.

Functional interpretation

Theorem (Functional interpretation)

If

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

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

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

Sketch of proof.

Apply the following proof translations:

- Elimination of extensionality,
- a negative translation,
- Gödel's Dialectica translation.

□

See Kohlenbach: Applied Proof Theory.

The intuition behind the functional interpretation

Each formula can be assigned an equivalent $\forall\exists$-formula.
E.g.

$$A :\equiv \forall x\, \exists y\, \forall z\, A_{qf}(x, y, z)$$

will be assigned

$$A^{ND} \equiv \forall x\, \forall f_z\, \exists y\, A_{qf}(x, y, f_z(y)).$$

- This assignment preserves logical rules, like

$$\frac{A \qquad A \to B}{B},$$

  and exhibits programs.
- Thus, to prove the program extraction theorem we only have to provide programs for the axioms.

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

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*

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

We interpreted ACA_0^ω non-constructively using μ.
One can also interpret ACA_0^ω directly using bar recursion.
See Avigad, Feferman in Handbook of Proof Theory

Filter

Filter

A set $\mathcal{F} \subseteq \mathcal{P}(\mathbb{N})$ is a *filter over* $\mathbb{N}$ if

- $\forall X, Y \ (X \in \mathcal{F} \wedge X \subseteq Y \rightarrow Y \in \mathcal{F})$,
- $\forall X, Y \ (X, Y \in \mathcal{F} \rightarrow X \cap Y \in \mathcal{F})$,
- $\emptyset \notin \mathcal{F}$

Ultrafilter

A filter $\mathcal{F}$ is an *ultrafilter* if it is maximal, i.e.,
$\forall X \ \left(X \in \mathcal{F} \vee \overline{X} \in \mathcal{F}\right)$

$\mathcal{P}_n := \{X \subseteq \mathbb{N} \mid n \in X\}$ is an ultrafilter. These filters are called *principal*.

The Fréchet filter $\{X \subseteq \mathbb{N} \mid X \text{ cofinite}\}$ is a filter but not an ultrafilter.

Non-principal ultrafilters

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

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

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

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

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

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

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

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

$\mathsf{QF\text{-}AC}^{1,0}$ 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 2: Term normalization (cont.)

Proof.

Consider $t[\mathcal{U}, f, n^0]$, where $\mathcal{U}, f, n^0$ are variables.
Assume that all possible λ-reductions haven been carried out. Then one of the following holds:

1. $t = 0$,
2. $t = S(t'_1)$, $t = f(t'_1)$, $t = t'_1 + t'_2$, $t(n) = t'_1 \cdot t'_2$,
3. $t = \mu(t'_g)$, $t = \mathcal{U}(t'_g)$, $t = R_0(t'_1, t'_2, t'_g)$.

Restart the procedure with t'_1, t'_2 and $t'_g m^0$. □

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 $t \in T$. □

The general concept

The proof theory

- Functional interpretation (Step 1)
- Term normalization (Step 2)

Extension to

- abstract types (Günzel, ongoing work),
- type 3 operators, e.g. Lebesgue measure defined on all subsets of unit interval. (K. '13)

The combinatorics

Construction of the partial ultrafilter on the countable algebra. (Step 3)

Extension to

- idempotent ultrafilters by using *iterated Hindman's theorem* (K. '12),
- possibly other type 2 operators.

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

- Program extraction and conservativity for non-principal ultrafilters.
- The Π^1_2-consequences of $\mathsf{RCA}_0^\omega + (\mathcal{U})$ and the Π^1_2-consequences of ACA_0^ω are the same.

Thank you for your attention!

References

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

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

Alexander P. Kreuzer
Minimal idempotent ultrafilters and the Auslander-Ellis theorem
preprint, `arXiv:1305.6530`.

Alexander P. Kreuzer
Measure theory and higher order arithmetic
preprint, `arXiv:1312.1531`.