Program extraction and ultrafilters

Alexander P. Kreuzer

ENS Lyon

Logic Colloquium 2013
Special Session: Logical analysis of mathematical proofs

Outline

1. Program extraction for non-principal ultrafilters
   - The logical systems and the functional interpretation
   - Ultrafilters
   - The results
2. The general concept
   - Combinatorial Π^1_2-principles and Ramsey's theorem for pairs
3. Summary

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.,

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

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

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

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

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

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

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

$\mathsf{QF\text{-}AC}^{1,0}$ 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 $(\mathcal{U})$:

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

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.)

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

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

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

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

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

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

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

This yields then

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

and thus the theorem.

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

- Assume that $t_1, \ldots$ 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 $(\mathcal{U})_{\mathit{qf}}$ relativized the sets coded by $t_1, \ldots, t_i$ 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

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

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),
- minimal idempotent ultrafilters by using a refinement of the *Auslander-Ellis theorem* (K. '13),
- possibly other type 2 operators.

Combinatorial Π^1_2-principles

Combinatorial Π^1_2-Principles are principles of the form

$$\forall f\, \exists g\, \mathsf{A}_{\mathrm{ar}}(f, g)$$

where $\mathsf{A}_{\mathrm{ar}}(f, g)$ is arithmetical.
We will restrict our attention to principles of this form

$$\forall f\, \exists g\, \forall x\, \mathsf{A}_{qf}(f, g, x).$$

Example

Ramsey's theorem for pairs (RT^2_2)

The operator

The functional interpretation applied to P yields the following.

$$\begin{array}{llll} & \forall f^1 & \exists g^1 \, \forall x^0 & \mathsf{A}_{qf}(f, g, x) \\ & \forall f^1 \, \forall X^2 & \exists g^1 & \mathsf{A}_{qf}(f, g, Xg) \\ \exists \mathcal{G}^3 & \forall f^1 \, \forall X^2 & & \mathsf{A}_{qf}(f, \mathcal{G}fX, X(\mathcal{G}fX)) \end{array}$$

$\mathcal{G}$ is called the solution functional to the principle P.
Note that this functional is of type 3.

Theorem (Functional interpretation)

If

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

the one can extract a term $t \in T_0[\mathcal{G}]$, *such that*

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

- After normalization every occurrence of $\mathcal{G}$ in t is of the form $\mathcal{G}(t_1[h^1], t_2[h^1])$.
  The parameter h is of type 1 because $\mathcal{G}$ is of type 3 and not 2.
- Roughly, only finitely many nested applications of (P) relative to the fixed parameter h^1 are used.

The combinatorics for RT^2_2

Theorem (Cholak, Jockusch, Slaman '01)

$\mathsf{RCA}_0 + \Sigma^0_2\text{-}\mathsf{IA} + \mathsf{RT}^2_2$ *is* Π^1_1*-conservative over* $\mathsf{RCA}_0 + \Sigma^0_2\text{-}\mathsf{IA}$.

Theorem (Chong, Slaman, Yang '13)

$\mathsf{RCA}_0 + \mathsf{RT}^2_2 \nvdash \Sigma^0_2\text{-}\mathsf{IA}$.

- Full Π^1_0-CA:

$$\Pi^0_1\text{-}\mathsf{CA}\colon\ \forall f\, \exists X\, \forall k\ (k \in X \leftrightarrow \forall n\, f(k,n) \neq 0)\,.$$

- Instance of Π^0_1-CA:

$$\Pi^0_1\text{-}\mathsf{CA}(f)\colon\ \exists X\, \forall k\ (k \in X \leftrightarrow \forall n\, f(k,n) \neq 0)\,.$$

The combinatorics for RT^2_2 (cont.)

- For all f there exists an f', such that uniform WKL_0 proves

$$\forall c \text{ coloring } \Big(\Pi^0_1\text{-CA}(f'(c)) \\ \rightarrow \exists H\,(H \text{ solves } \mathsf{RT}^2_2 \text{ for } c \land \Pi^0_1\text{-CA}(f(c,H)))\Big)$$

- Single non-iterated instances of Π^0_1-CA suffices to interpret nested applications of RT^2_2 (relative to roughly RCA_0 plus weak König's lemma).
- Single non-iterated use of the bar recursor $B_{0,1}$ suffices to interpret the term t.

This is based on CJS '01 but not on the forcing construction to prove the above theorem.
We called this property *proofwise low*.

Program extraction for RT^2_2

Theorem (K., Kohlenbach '12)

If $\mathsf{WKL}_0^\omega + \Sigma^0_2\text{-}\mathsf{IA} + \mathsf{RT}^2_2 \vdash \forall x^1\, \exists y^0\, \mathsf{A}_{qf}(x,y)$ *then one can extract a term* $t \in T_1$ *(provably total in* $\Sigma^0_2\text{-}\mathsf{IA}$*) with*

$$\mathsf{A}_{qf}(x, tx).$$

Similar program extraction results hold for

- Choesive principle (COH), ascending-descending ADS, chain-antichain principle (CAC), (K. '12)
- 2-RAN. (K. '13)

Summary

- Program extraction and conservativity for non-principal ultrafilters.
  - 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.
- Other use of the combination of functional interpretation and term normalization.
  - Combinatorial Π^1_2-principles and RT^2_2.

Thank you for your attention!

References I

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`.

Peter Cholak, Carl Jockusch, and Theodore Slaman
On the strength of Ramsey's theorem for pairs
J. of Symbolic Logic **66** (2001), 1–55.

References II

Alexander P. Kreuzer and Ulrich Kohlenbach
Term extraction and Ramsey's theorem for pairs
J. Symbolic Logic **77** (2012), no. 3, pp. 853–895.

Alexander P. Kreuzer
Primitive recursion and the chain antichain principle
Notre Dame J. Formal Logic, **53** (2012), no. 2, 245–265.

Alexander P. Kreuzer
Program extraction for 2-random reals
Archive for Mathematical Logic, **52** (2013), no. 5–6, 659–666.