Polynomial-time programs from ineffective proofs in feasible analysis

Paulo Oliva

BRICS
University of Århus
Denmark

ASL Annual Meeting, Chicago, Jun 2003

The Plan

1. Motivation
   - Ineffective principles in analysis (weak König's Lemma)
   - Feasible analysis
2. The Main Result
   - Algorithm for extracting polynomial-time realizers from proofs (involving WKL) of Π^0_2-theorems in feasible analysis.
3. Sketch of the Proof
4. Related/Future Work

Ineffective principles

- By ineffective principles we mean, e.g.

  (1) sequential Heine/Borel covering lemma for $[0,1]$,

  (2) Every continuous function $f : [0,1] \to \mathbb{R}$ attains its infimum and supremum,

  (3) Every continuous function $f : [0,1] \to \mathbb{R}$ is uniformly continuous.

- Over a basic system of analysis (RCA_0) those principles are equivalent to

  WKL : *Every infinite binary tree has an infinite branch*

- This principle is normally called binary/weak König's Lemma.

- WKL is ineffective in the sense that it only holds in models which contain non-recursive functions.

BRICS

WKL in proofs of $\forall\exists$-theorems

- What if WKL is used in the proof of a theorem $\forall x \exists y A_0(x,y)$?

- In 76 Friedman (also Parsons, Mints, Takeuti) defined the subsystem of analysis RCA_0 and showed that RCA_0 is Π^0_2-conservative over PRA, i.e.

  Thm [Friedman]. If $\mathsf{RCA}_0 \vdash \forall x \exists y A_0(x,y)$ then there exists a primitive recursive function f such that $\mathsf{PRA} \vdash A_0(x, fx)$.

- Moreover, he showed that $\mathsf{RCA}_0 + \mathsf{WKL}$ is Π^0_2-conservative over RCA_0. Therefore:

  Thm [Friedman]. If $\mathsf{RCA}_0 + \mathsf{WKL} \vdash \forall x \exists y A_0(x,y)$ then there exists primitive recursive function f such that $\mathsf{PRA} \vdash A_0(x, fx)$.

- Friedman's proof is ineffective!

BRICS

On Friedman's result

- Harrington'77 proved (also non-constructively) Π^1_1-conservation of WKL over RCA_0.
- First effective version of Friedman's result was given by Sieg'85 (based on cut-elimination).
- Extension of Friedman's result to the higher types was given by Kohlenbach'92 (based on functional interpretation).
- Avigad'96 formalized the forcing argument used in Harrington's proof obtaining an effective version of the Π^1_1-conservation result (no function extraction procedure, though).

Basic Feasible Analysis I

- Ferreira'94 defined a Basic Theory for Feasible Analysis BTFA
- The Π^0_2-theorems of BTFA have polynomial-time computable realizers.

  Thm [Ferreira]. If $\mathsf{BTFA} \vdash \forall x \exists y A_0(x, y)$ then there exists a polynomial-time computable function f such that $\forall x A_0(x, fx)$ holds.

- Ferreira also showed non-constructively that BTFA and $\mathsf{BTFA} + \mathsf{WKL}$ have the same Π^1_1-theorems (and consequently Π^0_2-theorems). Hence:

  Thm [Ferreira]. If $\mathsf{BTFA} + \mathsf{WKL} \vdash \forall x \exists y A_0(x, y)$ then there exists a polynomial-time computable function f such that $\forall x A_0(x, fx)$ holds.

BRICS

Basic Feasible Analysis II

- A different basic theory for feasible analysis (based on the language of finite types) can be obtained by taking Cook and Urquhart's system CPV^ω extended with quantifier-free choice QF-AC.
- The resulting theory can be viewed as an extension of (a version of) BTFA to all finite types.

  Thm. If $\mathsf{CPV}^\omega + \mathsf{QF\text{-}AC} \vdash \forall x \exists y A_0(x, y)$ then there exists *effectively* a polynomial-time computable function f such that $\mathsf{IPV}^\omega \vdash \forall x A_0(x, fx)$.

BRICS

Main result (to appear: LICS'03)

Thm. If $\mathsf{CPV}^\omega + \mathsf{QF\text{-}AC} + \mathsf{WKL} \vdash \forall x \exists y A_0(x, y)$ then there exists *effectively* a polynomial-time computable function f such that $\forall x A_0(x, fx)$ holds.

- We can also allow "set parameters" in the theorem above, i.e.

  Thm. If $\mathsf{CPV}^\omega + \mathsf{QF\text{-}AC} + \mathsf{WKL} \vdash \forall x \exists y A_0(x, y, \alpha)$ then there exists *effectively* a polynomial-time computable function *with boolean oracle* f such that $\forall x \forall \alpha : \{0,1\}^\omega A_0(x, fx\alpha, \alpha)$ holds.

- In order to illustrated the mathematical significance of the system $\mathsf{CPV}^\omega + \mathsf{QF\text{-}AC} + \mathsf{WKL}$ we have indicated how to formalize the proof of Heine/Borel covering lemma in it.

BRICS

Sketch of the proof

1. Cook and Urquhart showed that CPV^ω has a functional interpretation, via negative translation, in IPV^ω.

   Thm [CU'93]. $\mathsf{CPV}^\omega \stackrel{\mathsf{N+f.i.}}{\longrightarrow} \mathsf{IPV}^\omega$.

2. We extend this interpretation to $\mathsf{CPV}^\omega + \mathsf{QF\text{-}AC}$.

   Lem. $\mathsf{CPV}^\omega + \mathsf{QF\text{-}AC} \stackrel{\mathsf{N+f.i.}}{\longrightarrow} \mathsf{IPV}^\omega$.

3. And, by adding a new form of binary bar recursion $\mathcal{B}$ to IPV^ω we can even interpret WKL.

   Thm. $\mathsf{CPV}^\omega + \mathsf{QF\text{-}AC} + \mathsf{WKL} \stackrel{\mathsf{N+f.i.}}{\longrightarrow} \mathsf{IPV}^\omega + \mathcal{B}$.

4. Finally, we show that the functions of $\mathsf{IPV}^\omega + \mathcal{B}$ are polynomial-time computable.

   Thm. $[\mathsf{IPV}^\omega + \mathcal{B}]_1 \equiv \mathbf{P}$.

BRICS

Binary Bar Recursion

$A : \{0,1\}^\omega \to \mathbb{N} \qquad w_n : \{0,1\}^* \qquad \hat{w}_n := w_n * \lambda k.0$

- The binary bar recursion we use can be formulated in terms of the following unbounded search:

  $\mathcal{B}(A, (w_n)_{n \in \mathbb{N}}) := \min n \, (|w_n| \neq n \vee |A\hat{w}_n| \leq |w_n|)$

- Why is this functional total?

  Lem [KC'96]. For any closed term $\Psi : \mathbb{N} \to \{0,1\}^\omega \to \mathbb{N}$ of IPV^ω, there exist constants c_1 and c_2 such that

  $$\forall x : \mathbb{N} \forall \alpha : \{0,1\}^\omega (|\Psi x \alpha| \leq |x|^{c_1} + c_2)$$

- **Lemma**. For any closed term $t[x, \alpha]$ in $\mathsf{IPV}^\omega + \mathcal{B}$ there exists effectively a closed term $t'[x, \alpha]$ of IPV^ω such that $t = t'$ for all input x and 0-1 functions α.

BRICS

Related Work

- Howard'81 used a different form of binary bar recursion to realize the functional interpretation of (the negative translation of) WKL.
- Howard's binary bar recursion, however, seems to be too strong for the feasible context, since it apparently involves an exponential search.
- Sieg's proof of WKL-elimination (based on cut elimination) was successfully adapted to the feasible setting by Kauffmann'00.
- Our approach directly extracts a polynomial-time computable realizer out of the WKL-proof, rather than eliminating it first.

Future Work

- Investigate whether Kohlenbach's effective proofs of WKL elimination can be translated into the feasible setting, by making a careful treatment of bounded quantifiers.
- Find ineffective proofs of Π^0_2-theorems which can be formalized in $\mathsf{CPV}^\omega + \mathsf{QF\text{-}AC} + \mathsf{WKL}$, and carry out the extraction of polynomial-time algorithms (cf. analysis of WKL-proofs e.g. in approximation theory).
- Compare the quality of the polynomial-time algorithms yielded via the approach based on cut elimination and our approach.