Polynomial-time algorithms from ineffective proofs in feasible analysis

(To appear in LICS'03)

Paulo Oliva

BRICS
University of Århus
Denmark

Edinburgh – March 2003

The Plan

1. Motivation
   - Feasible Analysis
   - Weak König's Lemma
2. The Main Result
   - Effective procedure for extracting polynomial-time realizers from proofs (involving Π^0_1-WKL) of Π^0_2-theorems in feasible analysis.
3. Sketch of the Proof
4. Howard's use of (a different form of) binary Bar Recursion
5. Future Work

Proof Mining

- Given an arithmetical/analytical theory $\mathcal{T}$, we are interested in theorems of the form:

  Thm. If $\mathcal{T} \vdash \forall x \exists y A_0(x, y)$ then there exists *effectively* a function f in the complexity class C such that $\forall x A_0(x, fx)$ holds.

- An example:

  Thm. If $\mathsf{PA}^\omega \vdash \forall x \exists y A_0(x, y)$ then there exists *effectively* a primitive recursive function f (in the sense of Gödel's T) such that $\mathsf{HA}^\omega \vdash \forall x A_0(x, fx)$.

BRICS

Basic Analysis I

- In 76 Friedman 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!

Basic Analysis II

- The first effective version of Friedman's result was given by Sieg using cut-elimination, Herbrand analysis and a simple form of Howard's majorizability for primitive recursive terms.
- Kohlenbach extended Friedman's result to (among others) the higher types systems $\text{E-PA}^\omega + \text{QF-AC}^{1,0}$ and $\text{E-PRA}^\omega + \text{QF-AC}^{1,0}$ by means of functional interpretation and majorizability for functionals in all finite types.
- Kohlenbach's result applies to a whole class of analytical principles of which WKL is just a special case.

BRICS

Basic Feasible Analysis I

- In 94 Ferreira developed a subsystem of analysis (BTFA – Basic Theory for Feasible Analysis) whose provably recursive functionals are polynomial-time computable.

- BTFA contains Σ^b_1-IND, Δ^0_1-CA and Σ^b_∞-BC.

  Thm [Ferreira]. If 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.

- As done by Friedman to RCA_0, Ferreira then showed that the Π^0_2-theorems of BTFA $+ \forall\Sigma^b_\infty$-WKL are the same as those of BTFA. Therefore:

  Thm [Ferreira]. If BTFA $+ \forall\Sigma^b_\infty$-WKL $\vdash \forall x \exists y A_0(x, y)$ then there exists primitive recursive function f such that $\forall x A_0(x, fx)$ holds.

- Ferreira's proof is also ineffective!

BRICS

Basic Feasible Analysis II

- One can also give a basic theory for feasible analysis based on functionals of higher-type by taking Cook and Urquhart's system CPV^ω extended with quantifier-free choice $\mathsf{QF\text{-}AC}$.

  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 $\mathsf{IPV}^\omega \vdash \forall x A_0(x, fx)$.

- The system $\mathsf{CPV}^\omega + \mathsf{QF\text{-}AC}$ contains Σ^b_1-IND and proves Δ^0_1-CA. It does not seem to prove Σ^b_∞-BC though.

BRICS

Weak König's Lemma

- Weak König's Lemma states the existence of an infinite path in an infinite binary branching tree.
- The mathematical importance of WKL comes from the fact that it is equivalent (over RCA_0) to various analytical principles, e.g.
  - Heine/Borel covering lemma for $[0, 1]$.
  - Every continuous function $f : [0, 1] \to \mathbb{R}$ is uniformly continuous.
  - Every continuous function $f : [0, 1] \to \mathbb{R}$ has an infimum and attains it.
- WKL is non-computational in the sense that there are recursive infinite binary trees which have only non-recursive infinite paths.

BRICS

Main result

Thm. If $\mathsf{CPV}^\omega + \mathsf{QF\text{-}AC} + \Pi^0_1\text{-}\mathsf{WKL} \vdash \forall x \exists y A_0(x,y)$ 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 $\mathsf{CPV}^\omega + \mathsf{QF\text{-}AC} + \Pi^0_1\text{-}\mathsf{WKL} \vdash \forall x \exists y A_0(x,y,\alpha)$ 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 $\mathsf{CPV}^\omega + \mathsf{QF\text{-}AC} + \Pi^0_1\text{-}\mathsf{WKL}$ we have indicated how to formalize the proof of Heine/Borel covering lemma in it.

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]. $\mathsf{CPV}^\omega \overset{\mathsf{N+f.i.}}{\longrightarrow} \mathsf{IPV}^\omega$.

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

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

3. And, by adding binary bar recursion to IPV^ω we can even interpret Π^0_1-WKL.

   Thm. $\mathsf{CPV}^\omega + \mathsf{QF\text{-}AC} + \Pi^0_1\text{-}\mathsf{WKL} \overset{\mathsf{N+f.i.}}{\longrightarrow} \mathsf{IPV}^\omega + \mathcal{B}$.

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

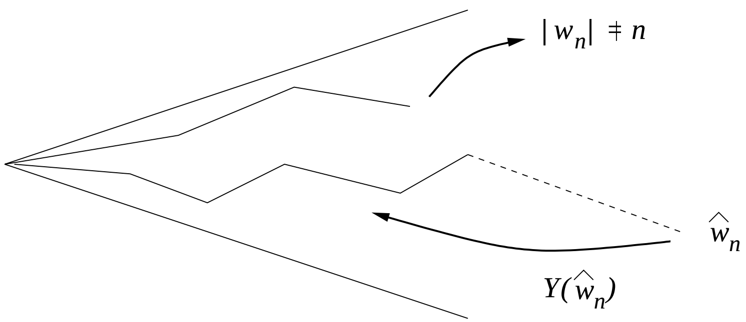
The Functional Interpretation of Π^0_1-WKL

- Realizing the functional interpretation of (the negative translation of) weak König's lemma involves solving the following problem:

  Given a tree T, a function $Y : \{0,1\}^\omega \to \mathbb{N}$ and a sequence of finite branches $(w_i)_{i \in \mathbb{N}}$, produce n and $f : \{0,1\}^\omega$ satisfying:

  $$|w_n| = n \wedge T(w_n) \to T(\overline{f}(Yf)).$$

- Two possible solutions...



Binary Bar Recursion

$$\mathcal{B}(Y, (w_i)_{i\in\mathbb{N}}, n) = \begin{cases} n & \text{if } |Y\hat{w}_n| \leq |w_n| \\ & \text{or } |w_n| \neq n \\ \mathcal{B}(Y, (w_i)_{i\in\mathbb{N}}, n+1) & \text{otherwise,} \end{cases}$$

where $Y : \{0,1\}^\omega \to \mathbb{N}$ and $w_i : \mathbb{N}$.

- It can be also formulated in the form of an unbounded search:

  $\min m \geq n\, (|Y\hat{w}_m| \leq |w_m| \vee |w_m| \neq m)$

- How to justify such recursion?

  Lem [KC'96]. For any closed term $t : \mathbb{N} \to \{0,1\}^\omega \to \mathbb{N}$ of IPV$^\omega$, there exists constants c_1 and c_2 such that

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

BRICS

Eliminating the Bar Recursion I

- Suppose we have type one term $t : \mathbb{N} \to \mathbb{N}$ in the language of $\mathsf{IPV}^\omega + \mathcal{B}$, we show how to replace $\mathcal{B}$ by limited recursion on notation.
- In fact, for the induction hypothesis we need a stronger condition:

Lem. For any term $t[x, \alpha] : \mathbb{N}$ of $\mathsf{IPV}^\omega + \mathcal{B}$, there exists a term $t'[x, \alpha] : \mathbb{N}$ of IPV^ω such that

$$\forall x : \mathbb{N} \forall \alpha : \{0, 1\}^\omega (t[x, \alpha] = t'[x, \alpha]).$$

BRICS

Eliminating the Bar Recursion II

- Let $\Psi[x]$ and $(w_i)_{i\in\mathbb{N}}[x]$ be fixed terms of $\mathsf{IPV}^\omega + \mathcal{B}$. The main step is to show that $\mathcal{B}(\Psi[x], (w_i)_{i\in\mathbb{N}}[x], 0)$, i.e. (omitting $[x]$)

$$\min n\,(|\Psi\hat{w}_n| \leq |w_n| \vee |w_n| \neq n),$$

  can be replaced by limited recursion on notation.

- This can be done since $|\Psi x\alpha|$, and hence the search, is bounded by $|x|^{c_1} + c_2$.

- Therefore, given an arbitrary term $t[x,\alpha]$ in $\mathsf{IPV}^\omega + \mathcal{B}$, we can successively normalize it and replace the innermost occurrence of $\mathcal{B}$ by limited recursion on notation.

BRICS

Howard's Binary Bar Recursion

- In 81 Howard used a different form of binary bar recursion to realize the functional interpretation of (the negative translation of) WKL.

$$\mathcal{B}^H(Y, z) = \begin{cases} 0 & \text{if } Y\hat{z} \leq |z| \\ 1 + \max\{\mathcal{B}^H(z0), \mathcal{B}^H(z1)\} & \text{otherwise.} \end{cases}$$

- This, however, seems too strong for the feasible context, since it apparently involves an exponential search.
- When analyzing the functional interpretation of WKL, Howard does not consider the bounded quantifier $\exists s$ in

$$\forall n \exists s(|s| = n \wedge T(s)) \rightarrow \exists \alpha \forall n T(\overline{\alpha} n).$$

BRICS

Summary

Thm [Friedman]. $\mathsf{RCA}_0 + \mathsf{WKL}$ is Π^0_2-conservative over PRA.

Thm [Kohlenbach'92]. $\mathsf{E\text{-}PRA}^\omega + \mathsf{WKL}$ is effectively Π^0_2-conservative over PRA.

Thm [Ferreira'94]. $\mathsf{BTFA} + \forall\Sigma^b_\infty\text{-}\mathsf{WKL}$ is Π^0_2-conservative over $\Sigma^b_1\text{-}\mathsf{NIA}$.

Thm. If $\mathsf{CPV}^\omega + \mathsf{QF\text{-}AC} + \Pi^0_1\text{-}\mathsf{WKL} \vdash \forall x \exists y A_0(x, y, \alpha)$ then there exists effectively a polynomial-time computable function f with boolean oracle such that $\forall x \forall \alpha : \{0,1\}^\omega A_0(x, fx\alpha, \alpha)$ holds.

Future Work

- Investigate whether effective proofs of WKL elimination for stronger systems (such as Sieg's and Kohlenbach's) 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 $\mathsf{CPV}^\omega + \mathsf{QF\text{-}AC} + \Pi^0_1\text{-}\mathsf{WKL}$, and carry out the extraction of polynomial-time algorithms.
- Find effective proofs of WKL elimination for the setting of feasible analysis, and compare the quality of the algorithms yielded via the two different procedures.

BRICS