Polynomial-time algorithms from ineffective proofs in feasible analysis

(To appear in LICS’03)

Paulo Oliva

BRICS
University of Århus
Denmark

Edinburgh – March 2003
1. Motivation
   - Feasible Analysis
   - Weak König’s Lemma
2. The Main Result
   - Effective procedure for extracting polynomial-time realizers from proofs (involving $\Pi^0_1$-WKL) of $\Pi^0_2$-theorems in feasible analysis.
3. Sketch of the Proof
4. Howard’s use of (a different form of) binary Bar Recursion
5. Future Work
Given an arithmetical/analytical theory $T$, we are interested in theorems of the form:

**Thm.** If $T \vdash \forall x \exists y A_0(x, y)$ 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 $PA^\omega \vdash \forall x \exists y A_0(x, y)$ then there exists **effectively** a primitive recursive function $f$ (in the sense of Gödel’s $T$) such that $HA^\omega \vdash \forall x A_0(x, fx)$. 
• In 76 Friedman defined the subsystem of analysis $\text{RCA}_0$ and showed that $\text{RCA}_0$ is $\Pi^0_2$-conservative over $\text{PRA}$, i.e.

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

• Moreover, he showed that $\text{RCA}_0 + \text{WKL}$ is $\Pi^0_2$-conservative over $\text{RCA}_0$. Therefore:

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

• Friedman’s proof is ineffective!
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 $E\text{-PA}^\omega + QF\text{-AC}^{1,0}$ and $E\text{-PRA}^\omega + QF\text{-AC}^{1,0}$ 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.
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 $\Sigma^b_1$-IND, $\Delta^0_1$-CA and $\Sigma^b_{\infty}$-BC.

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

- As done by Friedman to $\text{RCA}_0$, Ferreira then showed that the $\Pi^0_2$-theorems of $\text{BTFA} + \forall \Sigma^b_{\infty}$-WKL are the same as those of $\text{BTFA}$. Therefore:

  Thm [Ferreira]. If $\text{BTFA} + \forall \Sigma^b_{\infty}$-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!
One can also give a basic theory for feasible analysis based on functionals of higher-type by taking Cook and Urquhart’s system $\text{CPV}^\omega$ extended with quantifier-free choice $\text{QF-AC}$.

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

- The system $\text{CPV}^\omega + \text{QF-AC}$ contains $\Sigma^b_1$-IND and proves $\Delta^0_1$-CA. It does not seem to prove $\Sigma^b_\infty$-BC though.
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 RCA₀) 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.
Main result

**Thm.** If $\text{CPV}^\omega + \text{QF-AC} + \Pi_1^0\text{-WKL} \vdash \forall x \exists y A_0(x, y)$ 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 $\text{CPV}^\omega + \text{QF-AC} + \Pi_1^0\text{-WKL} \vdash \forall x \exists y A_0(x, y, \alpha)$ 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 $\text{CPV}^\omega + \text{QF-AC} + \Pi_1^0\text{-WKL}$ we have indicated how to formalize the proof of Heine/Borel covering lemma in it.
1. Cook and Urquhart showed that $\text{CPV}^\omega$ has a functional interpretation, via negative translation, in $\text{IPV}^\omega$.

   **Thm [CU’93].** $\text{CPV}^\omega \overset{N+f.i.}\rightarrow \text{IPV}^\omega$.

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

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

3. And, by adding binary bar recursion to $\text{IPV}^\omega$ we can even interpret $\Pi^0_1\text{-WKL}$.

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

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

   **Thm.** $[\text{IPV}^\omega + \mathcal{B}]_1 \equiv \text{P}$.
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:

\[
|w_n| = n \land T(w_n) \rightarrow T(f(Yf)) .
\]

Two possible solutions...
Binary Bar Recursion

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

where \( Y : \{0, 1\}^\omega \rightarrow \mathbb{N} \) and \( w_i : \mathbb{N} \).

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

\[ \min m \geq n \ (|Y\hat{w}_m| \leq |w_m| \lor |w_m| \neq m) \]

- How to justify such recursion?

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

\[ \forall x : \mathbb{N} \forall \alpha : \{0, 1\}^\omega (|\Psi x\alpha| \leq |x|^{c_1} + c_2) \]
Suppose we have type one term \( t : \mathbb{N} \rightarrow \mathbb{N} \) in the language of \( \text{IPV}^\omega + B \), we show how to replace \( B \) 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 \( \text{IPV}^\omega + B \), there exists a term \( t'[x, \alpha] : \mathbb{N} \) of \( \text{IPV}^\omega \) such that

\[
\forall x : \mathbb{N} \forall \alpha : \{0, 1\}^\omega (t[x, \alpha] = t'[x, \alpha]).
\]
Let $\Psi[x]$ and $(w_i)_{i \in \mathbb{N}}[x]$ be fixed terms of $\text{IPV}^\omega + \mathcal{B}$. The main step is to show that $\mathcal{B}(\Psi[x], (w_i)_{i \in \mathbb{N}}[x], 0)$, i.e. (omitting $[x]$)

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

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 $\text{IPV}^\omega + \mathcal{B}$, we can successively normalize it and replace the innermost occurrence of $\mathcal{B}$ by limited recursion on notation.
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) $\text{WKL}$. 

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

- This, however, seems too strong for the feasible context, since it apparently involves an exponential search.

- When analyzing the functional interpretation of $\text{WKL}$, Howard does not consider the bounded quantifier $\exists s$ in

\[ \forall n \exists s(|s| = n \land T(s)) \rightarrow \exists \alpha \forall n T(\overline{\alpha} n). \]
Thm [Friedman]. $\text{RCA}_0 + \text{WKL}$ is $\Pi^0_2$-conservative over $\text{PRA}$.

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

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

Thm. If $\text{CPV}^\omega + \text{QF-AC} + \Pi^0_1\text{-WKL} \vdash \forall x \exists y A_0(x, y, \alpha)$ then there exists effectively a polynomial-time computable function $f$ with boolean oracle such that $\forall x \forall \alpha : \{0, 1\}^\omega A_0(x, f x \alpha, \alpha)$ 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 $\Pi^0_2$-theorems which can be formalized in $\text{CPV}^\omega + \text{QF-AC} + \Pi^0_1$-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.