Polynomial-time programs from ineffective proofs in feasible analysis

Paulo Oliva

LICS, Ottawa, Jun 2003
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 \( \Pi^0_2 \)-theorems in feasible analysis.

3. Sketch of the Proof

4. Related/Future Work
Ineffective principles

- By ineffective principles we mean, e.g.
  1. Heine/Borel covering lemma for \([0, 1]\),
  2. Every continuous function \(f : [0, 1] \rightarrow \mathbb{R}\) attains its infimum and supremum,
  3. Every continuous function \(f : [0, 1] \rightarrow \mathbb{R}\) is uniformly continuous.

- Over a basic system of analysis (\(\text{RCA}_0\)) those principles are equivalent to

  \(\text{WKL} : \text{Every infinite binary tree has an infinite branch}\)

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

- \(\text{WKL}\) is ineffective in the sense that it only holds in models which contain non-recursive functions.
What if WKL is used in the proof of a theorem $\forall x \exists y A_0(x, y)$?

In 1976 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 $\text{PRA} \vdash A_0(x, f(x))$.

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 $\text{PRA} \vdash A_0(x, f(x))$.

Friedman’s proof is ineffective!
On Friedman’s result

- Harrington’77 proved (also non-constructively) $\Pi_1^1$-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 $\Pi_1^1$-conservation result (no function extraction procedure, though)
Ferreira’94 defined a Basic Theory for Feasible Analysis BTFA.

The $\Pi^0_2$-theorems of BTFA have polynomial-time computable realizers.

**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 $\forall x A_0(x, f(x))$ holds.

Ferreira also showed non-constructively that BTFA and $\text{BTFA} + \text{WKL}$ have the same $\Pi^0_2$-theorems. Hence:

**Thm [Ferreira].** If $\text{BTFA} + \text{WKL} \vdash \forall x \exists y A_0(x, y)$ then there exists a polynomial-time computable function $f$ such that $\forall x A_0(x, f(x))$ holds.
A different basic theory for feasible analysis (based on the language of finite types) can be obtained by taking Cook and Urquhart’s system $\text{CPV}^\omega$ extended with quantifier-free choice $\text{QF-AC}$.

The resulting theory can be viewed as an extension of (a version of) $\text{BTFA}$ to all finite types.

**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 $\text{IPV}^\omega \vdash \forall x A_0(x, f(x))$. 
Main result

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

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

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

- In order to illustrated the mathematical significance of the system $\text{CPV}^\omega + \text{QF-AC} + \text{WKL}$ 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]. $\text{CPV}^\omega \overset{N+f.i.}{\longrightarrow} \text{IPV}^\omega$.

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

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

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

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

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

Thm. $[\text{IPV}^\omega + \mathcal{B}]_1 \equiv \text{P}$.
The Functional Interpretation of WKL

\[ \hat{w}_n := w_n \ast 0000 \ldots \quad \overline{\alpha}_k := \alpha(0)\alpha(1) \ldots \alpha(k - 1) \]

**Problem:** Given a binary tree \( T \), a function \( A : \{0, 1\}^\omega \to \mathbb{N} \) and a sequence of finite branches \((w_i)_{i \in \mathbb{N}}\), produce \( n \) and \( \alpha : \{0, 1\}^\omega \) satisfying:

\[ |w_n| = n \land T(w_n) \to T(\overline{\alpha}(A\alpha)). \]

- Two possible solutions:
Binary Bar Recursion

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

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

- It can be also formulated in the form of an unbounded search:
  \[
  \min m \geq n (|A \hat{w}_m| \leq |w_m| \lor |w_m| \neq m)
  \]

- How to justify such recursion?

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

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

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

Eliminating the Bar Recursion I
Let $\Psi[x, \alpha]$ and $(w_i)_{i \in \mathbb{N}}[x, \alpha]$ be fixed terms of $\text{IPV}^\omega + B$. The main step is to show that $B(\Psi[x, \alpha], (w_i)_{i \in \mathbb{N}}[x, \alpha], 0)$, i.e. (omitting $[x, \alpha]$)

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

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 $\text{IPV}^\omega + B$, we can successively normalize it and replace the innermost occurrence of $B$ by limited recursion on notation.
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 $\Pi^0_2$-theorems which can be formalized in $CPV^\omega + QF-AC + WKL$, 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.