Proof Mining in Analysis
Computability and Complexity

Paulo Oliva

BRICS
University of Århus
Denmark

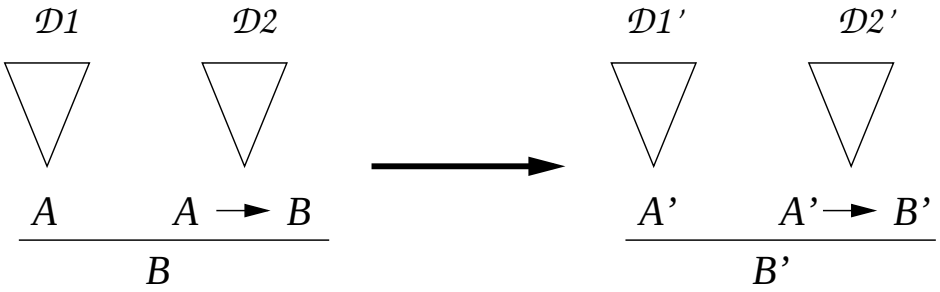
Qualifying Exam, June 2001

The Plan

1. Proof mining
   - Introduction
   - Techniques and applications
2. Case study (Uniqueness of L_1-approximation)
   - The uniform modulus of uniqueness
   - Computing the best L_1-approximation
3. Future work

Proof Mining

- Gödel'31 consistency of classical mathematics cannot be proved by finitary means.
- Gentzen'36 use transfinite induction and cut elimination.
- Gödel'58 use functionals of higher type. (Functional interpretation)
- Kreisel'58 determine the constructive content of a non-constructive concept or theorem.
- Techniques: Proof interpretations!



Applications

- ϵ-substitution: Kreisel (Hilbert's 17th problem)
- Herbrand's disjunction: Luckhardt (Roth's theorem)
- Modified realizability: Berger (Normalisation for simply typed λ-calculus)
- Monotone functional interpretation: Kohlenbach (Uniqueness and fixed point theorems)

Weak König's Lemma (WKL)

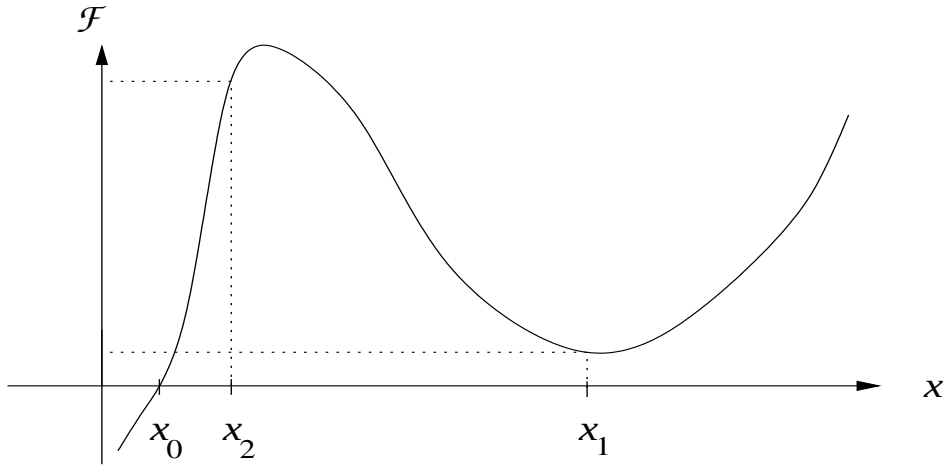
- WKL: If a binary tree is infinite then it has an infinity branch.
- In analytical terms: $\forall f \in C[0,1] \exists x \in [0,1] (fx = \inf_{y \in [0,1]} fy)$
- Thm [Kleene'52] There is an infinite recursive binary tree without infinite recursive branches.
- Thm [Ko'91] There is a polynomial-time computable function f on $[0,1]$ which has an uncountable number of maximum points in $[0,1]$, but none of them is computable.
- Conclusion: WKL relies on the existence of non-computable reals.

Numerical Analysis

Given that a continuous $\mathcal{F} : \mathbb{R} \to \mathbb{R}$ has a unique root (let x_0 be the root and $\varepsilon \in \mathbb{Q}^*_+$):

(i) Find ε-roots, i.e. x_1 such that $|\mathcal{F}(x_1)| < \varepsilon$.

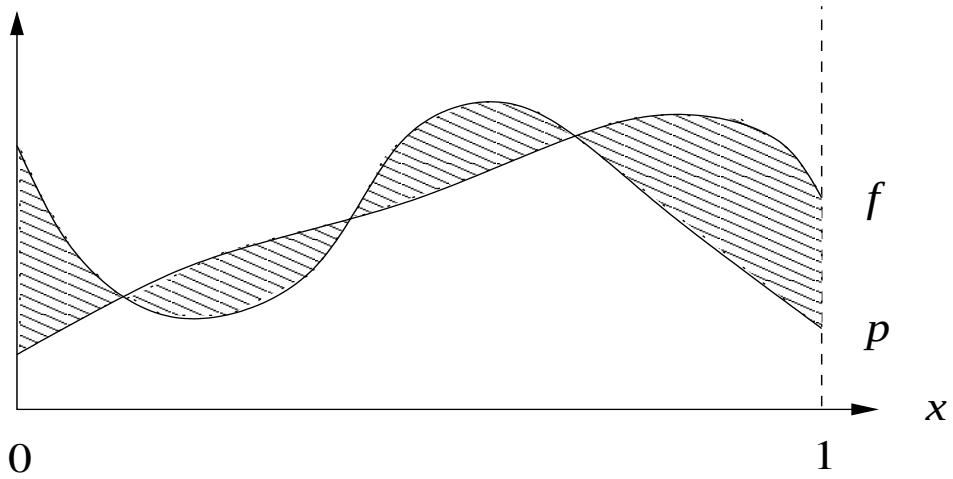
(ii) Find x_2 ε-close to x_0, i.e. $|x_2 - x_0| < \varepsilon$.



- We consider here a problem of type (ii), i.e. we look for an algorithm $B : \mathbb{Q}^*_+ \to \mathbb{Q}$ such that $|B(\varepsilon) - x_0| < \varepsilon$. We say that B computes the root x_0.

Our function $\mathcal{F}$ (L_1-approximation)

- Fix $f \in C[0,1]$ and $n \in \mathbb{N}$.
- $P_n :=$ polynomials of degree $\leq n$.
- L_1-distance, $\|f - p\|_1 := \int_0^1 |f(x) - p(x)|dx$.



- $dist_1(f, P_n) := \inf_{p \in P_n} \|f - p\|_1$.
- The problem: $\mathcal{F}(p) := \|f - p\|_1 - dist_1(f, P_n)$.

Existence of the best L_1-approximant

Theorem: For any $f \in C[0,1]$ and $n \in \mathbb{N}$, there exists a $p_n \in P_n$ such that $\mathcal{F}(p_n) = 0$.

- The existence proof is non-constructive (compactness argument) and does not supply an algorithm B for computing a root of $\mathcal{F}$.
- The roots of $\mathcal{F}$ must belong to a compact set, e.g.,

$$K_{f,n} := \{p \in P_n : \|p\|_1 \leq 2\|f\|_1\}.$$

Uniqueness of the best L_1-approximant

Theorem [Jackson, 1921]: For any $f \in C[0,1]$ and $n \in \mathbb{N}$, if $p_1, p_2 \in P_n$ are best L_1-approximants (i.e. $\bigwedge_{i=1}^{2} \mathcal{F}(p_i) = 0$) then $p_1 = p_2$.

In logical terms:

$$\forall f \in C[0,1]; n \in \mathbb{N}; p_1, p_2 \in P_n(\bigwedge_{i=1}^{2}(\mathcal{F}(p_i) = 0) \to \|p_1 - p_2\|_1 = 0).$$

which is equivalent to,

$$\forall f \in C[0,1]; n \in \mathbb{N}; p_1, p_2 \in K_{f,n}$$
$$(\bigwedge_{i=1}^{2}(\mathcal{F}(p_i) = 0) \to \|p_1 - p_2\|_1 = 0).$$

From the uniqueness proof (even though it is non-constructive) we can extract information for computing the best L_1-approximation of a given function.

Extracting the uniform modulus of uniqueness

$$\forall f \in C[0,1]; n \in \mathbb{N}; p_1, p_2 \in K_{f,n}$$

$$(\bigwedge_{i=1}^{2}(\mathcal{F}(p_i) =_{\mathbb{R}} 0) \to \|p_1 - p_2\|_1 =_{\mathbb{R}} 0).$$

$$\forall f \in C[0,1]; n \in \mathbb{N}; p_1, p_2 \in K_{f,n}; k \in \mathbb{N}\ \exists l \in \mathbb{N}$$

$$(\bigwedge_{i=1}^{2}(|\mathcal{F}(p_i)| \leq 2^{-l}) \to \|p_1 - p_2\|_1 < 2^{-k}).$$

Cheney's proof [1965] of Jackson's theorem can be formalized in $\mathbf{PA}^{\omega} + AC_{qf}^{1,0} + WKL$ [Kohlenbach, 90]. From that proof we extracted a Φ s.t.

$$\forall f \in C[0,1]; n \in \mathbb{N}; p_1, p_2 \in K_{f,n}; k \in \mathbb{N}$$

$$(\bigwedge_{i=1}^{2}(|\mathcal{F}(p_i)| \leq 2^{-\Phi(f,n,k)}) \to \|p_1 - p_2\|_1 < 2^{-k}).$$

BRICS

The metatheorem

Theorem [Kohlenbach, 1993]: Let X, K be **PA**$^\omega$-definable Polish spaces, K compact and consider a sentence which can be written (when formalized in the language of **PA**$^\omega$) in the form

$$A := \forall x \in X; n \in \mathbb{N}; y \in K \; \exists k \in \mathbb{N} \, A_1(n, x, y, k),$$

where A_1 is a purely existential. Then the following rule holds:

$\left\{ \begin{array}{l} \mathbf{PA}^\omega + AC^{1,0}_{qf} + WKL \vdash \forall x \in X; n \in \mathbb{N}; y \in K \; \exists k \in \mathbb{N} \, A_1(n, x, y, k) \\ \text{then one can extract a primitive recursive (in the sense of} \\ \text{Gödel'58) term } \Phi \text{ s.t.} \\ \mathbf{HA}^\omega \vdash \forall x \in X; n \in \mathbb{N}; y \in K \exists k \leq \Phi(n, x) \, A_1(n, x, y, k). \end{array} \right.$

The uniform modulus of uniqueness

Let

$$\Phi(\omega, n, \varepsilon) := \min\{\tfrac{c_n\varepsilon}{3^{n+2}(n+1)^{n+1}}, \tfrac{c_n\varepsilon}{2}\omega_n(\tfrac{c_n\varepsilon}{2})\},\ where$$
$$c_n := \frac{\lfloor n/2\rfloor!\lceil n/2\rceil!}{2^{n+3}3^{n^2+2n}(n+1)^{n^2+2n+1}}\ and$$
$$\omega_n(\varepsilon) := \min\{\omega(\tfrac{\varepsilon}{4}), \frac{\varepsilon}{40(n+1)^4\lceil\frac{1}{\omega(1)}\rceil}\}.$$

The functional Φ is a uniform modulus of uniqueness for the best L_1-approximation of any function f in $C[0,1]$ (having modulus of uniform continuity ω) from P_n, i.e.

$$\forall n \in \mathbb{N}; p_1, p_2 \in P_n; \varepsilon \in \mathbb{Q}_+^*$$
$$\big(\bigwedge_{i=1}^{2}(|\mathcal{F}(p_i)| \leq \Phi(\omega, n, \varepsilon)) \to \|p_1 - p_2\|_1 < \varepsilon\big).$$

Computing the best L_1-approximation

$$\forall f \in C[0,1]; n \in \mathbb{N}; p_1, p_2 \in P_n; \varepsilon \in \mathbb{Q}^*_+$$

$$\Big(\bigwedge_{i=1}^{2} (|\mathcal{F}(p_i)| \leq \Phi(\omega_f, n, \varepsilon)) \to \|p_1 - p_2\|_1 < \varepsilon \Big).$$

Take p_1 to be the best L_1-approximation of f from P_n (say p_n),

$$\forall f \in C[0,1]; n \in \mathbb{N}; p \in P_n; \varepsilon \in \mathbb{Q}^*_+$$

$$\Big(|\mathcal{F}(p)| \leq \Phi(\omega_f, n, \varepsilon) \to \|p - p_n\|_1 < \varepsilon \Big).$$

We only need Ψ such that:

$$\forall f \in C[0,1]; n \in \mathbb{N}; \varepsilon \in \mathbb{Q}^*_+ \Big(\Psi(f, n, \varepsilon) \in P_n \wedge |\mathcal{F}(\Psi(f, n, \varepsilon))| < \varepsilon \Big)$$

Then,

$$B_{f,n}(\varepsilon) := \Psi(f, n, \Phi(\omega_f, n, \varepsilon))$$

computes the best L_1-approximation of f from P_n.

The functional Ψ

Main idea: if $\|p_n - p'\|_1 \leq \varepsilon$ then

$$\begin{aligned} \|f - p'\|_1 &\leq \underbrace{\|f - p_n\|_1}_{=dist_1(f,P_n)} + \underbrace{\|p_n - p'\|_1}_{\leq \varepsilon} \\ \|f - p'\|_1 - dist_1(f, P_n) &\leq \varepsilon \\ |\mathcal{F}(p')| &\leq \varepsilon \end{aligned}$$

So, we just need a set of points N such that for at least one of them (say p') $\|p_n - p'\|_1 \leq \varepsilon$.

1. Compute $\|f - p'\|_1$ for each $p' \in N$.
2. Output some p' which gave minimum value.

History

- 1921 [Jackson] Proof of the uniqueness of best L_1-approximation.
- 1965 [Cheney] 'Elementary' proof of Jackson's theorem (highly non-constructive, WKL).
- 1975 [Björnestål] Existence of a uniform modulus of uniqueness of the form $c\,\varepsilon\,\omega_f(c\,\varepsilon)$, where the constant c depends on f and n (but the constant c is not produced).
- 1979 [Kroó] Björnestål's result is improved: the constant c need not to depend on any particular value of f but only on its modulus of uniform continuity ω_f (again the constant c is not produced). Moreover, Björnestål's ε-dependency is optimal.
- 2001 [Kohlenbach, Oliva] Fully explicit uniform modulus of uniqueness.

Future Work

- Proof mining (applied)
  - Extend the result to other Haar subspaces of $C[0,1]$.
  - Analyze the computational complexity of computing the best L_1-approximation of a continuous functions from P_n.
  - Other test cases...
- Proof mining (theoretical)
  - Relation between the different approaches to proof mining.
  - Semi-classical systems
  - Weak fragments of analysis
- Computable analysis
  - Computable analysis $\times$ domain theory.

Bounding the coefficients

From a bound on the L_1-norm of a polynomial $p := a_0 + \ldots + a_n x^n$ we can produce a bound on the coefficients a_i:

$$\|p\|_1 \leq M \rightarrow |a_i| \leq \frac{(2(n+1)^2)^{i+1}}{i!} M$$

or

$$\|p - p_n\|_1 \leq \frac{\varepsilon}{2^{n+1}(n+1)^{2n+2}} \rightarrow \|p - p_n\|_{max} \leq \varepsilon$$