PROOF MINING

Lecture 4 - Proof interpretations today

Thomas Powell
University of Bath

Nordic Logic Summer School 2022

University of Bergen
16 June 2022

These slides are available at `https://t-powell.github.io/`.

Outline

1. Proof mining: Bounds for existential statements
2. Focus: The finite convergence principle and metastability
3. Case study: A fixed point theorem in uniformly convex Banach spaces
4. Formalisation and program synthesis
5. References

The potential of program extraction

We have already seen some examples of witness extraction from ∀∃ statements, our running example being

Theorem

There exists a function $X : \mathbb{N} \to \mathbb{N}$ *such that for all* n *we have* $X(n) \geq n$ *and* $X(n)$ *prime.*

But you don't need sophisticated proof theoretic techniques to be able to do this. So are there examples where the formal analysis of a proof can yield genuinely new numerical information from proofs?

The answer is an emphatic YES. This is the so-called 'proof mining' program.

Central to the success of proof mining program are the following phenomena:

- One can typically extract a witnesses for ∀∃ statements even when the underlying proofs are highly non-constructive;
- Certain mathematical principles, particularly forms of *compactness*, do not contribute to the complexity of extracted bounds, leading to surprisingly simple polynomial bounds from proofs which employ heavy machinery from analysis.

A brief history of proof mining

- Pioneered by Kreisel in the 1950s, who proposed 'unwinding' constructive content from proofs using proof theoretic methods. Case studies in number theory and abstract algebra.
- In the 1980s, both Girard and Luckhardt carry out case studies and obtain bounds (van der Waerden's theorem and Roth's theorem respectively)
- From 1990s onwards, Kohlenbach finds numerous applications, in approximation theory and fixed point theory in particular. Proof mining takes off! Textbook published in 2008.
- In the 2010s proof mining expands to ergodic theory, nonlinear analysis, commutative algebra, termination theory and other areas. A connection with Tao's metastability is discovered.
- Currently an active area of research with a small but dedicated community!
- **2022: Where to next?**

Example: Uniqueness of best approximation

Theorem

Let $n \in \mathbb{N}$ and $f \in C[0,1]$ be fixed. Let

$$dist(f, P_n) := \inf_{p \in P_n} \|f - p\|$$

where P_n is the space of all polynomials with degree $\leq n$. Then there exists a polynomial of best approximation i.e. a polynomial p^* such that

$$\|f - p^*\| = dist(f, P_n),$$

and moreover, this polynomial is unique i.e. for all $p_1, p_2 \in P_n$

$$\bigwedge_{i=1,2} (\|f - p_i\| = dist(f, P_n)) \to p_1 = p_2.$$

A proof theoretic analysis of uniqueness

Let's look a bit more closely at uniqueness:

$$\forall n \in \mathbb{N} \forall f \in C[0,1] \forall p_1, p_2 \in P_n \left(\bigwedge_{i=1,2} (\|f - p_i\| = \mathrm{dist}(f, P_n)) \to p_1 = p_2 \right).$$

Now, equality $=$ over the real numbers is actually a $\forall$-statement and so written out fully, uniqueness becomes

$$\begin{cases} \forall n \in \mathbb{N} \forall f \in C[0,1] \forall p_1, p_2 \in P_n \\ \left(\forall j \bigwedge_{i=1,2} (\|f - p_i\| - \mathrm{dist}(f, P_n) < 2^{-j}) \to \forall k \, \|p_1 - p_2\| < 2^{-k} \right). \end{cases}$$

The (partial) functional interpretation of this is the following:

$$\begin{cases} \forall n, k \in \mathbb{N} \forall f \in C[0,1] \forall p_1, p_2 \in P_n \exists j \\ \left(\bigwedge_{i=1,2} (\|f - p_i\| - \mathrm{dist}(f, P_n) < 2^{-j}) \to \|p_1 - p_2\| < 2^{-k} \right). \end{cases}$$

A modulus of uniqueness

In the case of both the uniform norm and the L_1 norm, it is possible to extract a term Φ of System T such that

$$\begin{cases}\forall n, k \in \mathbb{N} \forall f \in C[0,1] \forall p_1, p_2 \in P_n \exists j \\ \left(\bigwedge_{i=1,2} (\|f - p_i\| - \mathrm{dist}(f, P_n) < 2^{-\Phi(f,n,k)}) \to \|p_1 - p_2\| < 2^{-k} \right) . \end{cases}$$

where Φ is independent of p_1, p_2.

Remark. Φ is known as the modulus of uniqueness.

Explicit moduli of uniqueness are given in the following papers:

- de La Vallée Poussin's proof of uniqueness of best Chebychev approximation [Kohlenbach, 1993a];
- Young's proof of uniqueness of best Chebychev approximation [Kohlenbach, 1993b];
- Cheney's proof of uniqueness of best L_1 approximation [Kohlenbach and Oliva, 2003a].

In some cases these results even improved known results in the literature.

More recent work

For a comprehensive account of proof mining see [Kohlenbach, 2008] (the standard text on the subject).

For individual expository articles see e.g.

- Kohlenbach, U. and Oliva, P. (2003b). A systematic way of analyzing proofs in mathematics.
  Proceedings of the Steklov Institute of Mathematics, 242:136–164
- Avigad, J. (2009). The metamathematics of ergodic theory.
  Annals of Pure and Applied Logic, 157:64–76
- Kohlenbach, U. (2018). Proof theoretic methods in nonlinear analysis.
  In *Proc. Int. Cong. of Math. - ICM 2018*

How are proof theoretic tools applied to new areas?

Key steps:

1. Are there theorems in this area which have the right logical structure? What kind of information could I hope to extract? Is it useful?
2. How do I formalize the proofs? How do I represent the underlying spaces?
3. Analyse some concrete proofs.
4. What is going on more generally? Can these proofs be expressed in an abstract logical framework?
5. Develop new metatheorems which *guarantee* that, under certain conditions, programs can be extracted.

Potential new areas:

- Number theory?
- Probability theory?
- Financial mathematics?

Outline

1. Proof mining: Bounds for existential statements
2. Focus: The finite convergence principle and metastability
3. Case study: A fixed point theorem in uniformly convex Banach spaces
4. Formalisation and program synthesis
5. References

The monotone convergence theorem

Recall in the last lecture we discussed the *monotone convergence principle*:

Theorem

Let (x_n) be a nondecreasing sequence of rational numbers in $[0,1]$. Then

$$\forall k \exists n \forall m (|x_{n+m} - x_n| \leq 2^{-k}).$$

We learned that in general there is no computable $N : \mathbb{N} \to \mathbb{N}$ satisfying

$$\forall k, \forall m (|x_{N(k)+m} - x_{N(k)}| \leq 2^{-k}),$$

due to the result of Specker.

But we now have a procedure for dealing with non-computable statements like this.

Let's first take a look at a proof.

Proving the monotone convergence theorem

Proof.

Suppose that the monotone convergence principle fails i.e. there exists some k such that

$$\forall n \exists m (|x_{n+m} - x_n| > 2^{-k}).$$

Then there exists a function $g : \mathbb{N} \to \mathbb{N}$ such that

$$\forall n (|x_{n+g(n)} - x_n| > 2^{-k}).$$

Define the function $\tilde{g}(n) = n + g(n)$. Then we have a sequence

$$0 \leq x_0 < x_{\tilde{g}(0)} < x_{\tilde{g}^{(2)}(0)} < \ldots <$$

with $x_{\tilde{g}^{(i+1)}(0)} - x_{\tilde{g}^{(i)}(0)} > 2^{-k}$, therefore

$$x_{\tilde{g}(2^k)} > 1$$

a contradiction. □

The computational content of the proof

Our proof gave us some indirect computational information, namely

$$\forall k, g \exists n \leq \tilde{g}^{(2^k)}(0)(|x_{n+g(n)} - x_n| \leq 2^{-k}),$$

or in other words

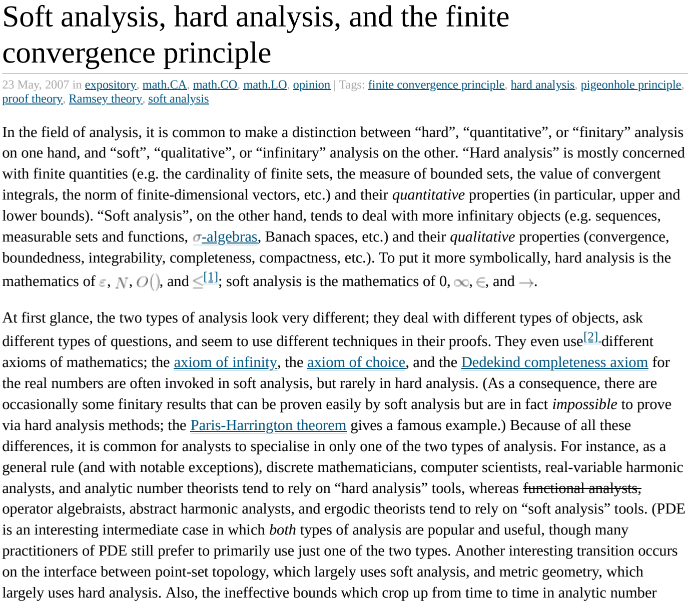
$$\forall k, g \exists n \leq \tilde{g}^{(2^k)}(0) \forall i, j \in [n, n+g(n)](|x_i - x_j| \leq 2^{-k})$$

Note that we can rephrase this statement entirely, so as only to refer to a finite part of (x_n). Let $M = \tilde{g}^{(2^k+1)}(0)$. We have the following:

Theorem (Finite convergence principle)

Let $k \in \mathbb{N}$, $g : \mathbb{N} \to \mathbb{N}$, and suppose that $0 \leq x_0 \leq x_1 \leq \ldots \leq x_M \leq 1$, where M is a sufficiently large number which depends only on k and g. Then there exists some $0 \leq n \leq n + g(n) \leq M$ such that $|x_i - x_j| \leq 2^{-k}$ for all $n \leq i, j \leq n + g(n)$.

Blog post by T. Tao, 2007



Soft analysis, hard analysis, and the finite convergence principle

23 May, 2007 in expository, math.CA, math.CO, math.LO, opinion | Tags: finite convergence principle, hard analysis, pigeonhole principle, proof theory, Ramsey theory, soft analysis

In the field of analysis, it is common to make a distinction between “hard”, “quantitative”, or “finitary” analysis on one hand, and “soft”, “qualitative”, or “infinitary” analysis on the other. “Hard analysis” is mostly concerned with finite quantities (e.g. the cardinality of finite sets, the measure of bounded sets, the value of convergent integrals, the norm of finite-dimensional vectors, etc.) and their *quantitative* properties (in particular, upper and lower bounds). “Soft analysis”, on the other hand, tends to deal with more infinitary objects (e.g. sequences, measurable sets and functions, σ-algebras, Banach spaces, etc.) and their *qualitative* properties (convergence, boundedness, integrability, completeness, compactness, etc.). To put it more symbolically, hard analysis is the mathematics of ε, N, $O()$, and $\leq$[1]; soft analysis is the mathematics of 0, ∞, $\in$, and $\to$.

At first glance, the two types of analysis look very different; they deal with different types of objects, ask different types of questions, and seem to use different techniques in their proofs. They even use[2] different axioms of mathematics; the axiom of infinity, the axiom of choice, and the Dedekind completeness axiom for the real numbers are often invoked in soft analysis, but rarely in hard analysis. (As a consequence, there are occasionally some finitary results that can be proven easily by soft analysis but are in fact *impossible* to prove via hard analysis methods; the Paris-Harrington theorem gives a famous example.) Because of all these differences, it is common for analysts to specialise in only one of the two types of analysis. For instance, as a general rule (and with notable exceptions), discrete mathematicians, computer scientists, real-variable harmonic analysts, and analytic number theorists tend to rely on “hard analysis” tools, whereas ~~functional analysts,~~ operator algebraists, abstract harmonic analysts, and ergodic theorists tend to rely on “soft analysis” tools. (PDE is an interesting intermediate case in which *both* types of analysis are popular and useful, though many practitioners of PDE still prefer to primarily use just one of the two types. Another interesting transition occurs on the interface between point-set topology, which largely uses soft analysis, and metric geometry, which largely uses hard analysis. Also, the ineffective bounds which crop up from time to time in analytic number

The correspondence principle

(emphasis mine)

> *"It is fairly well known that the results obtained by hard and soft analysis respectively can be connected to each other by various "***correspondence principles***" or "compactness principles". It is however my belief that the relationship between the two types of analysis is in fact much closer than just this … "*

> *"I wish to illustrate this point here using a simple but not terribly well known result, which I shall call the "finite convergence principle" … It is the finitary analogue of an utterly trivial infinitary result - namely, that every bounded monotone sequence converges - but sometimes,* **a careful analysis of a trivial result can be surprisingly revealing***, as I hope to demonstrate here."*

The correspondence principle

This is the so-called *finite convergence principle*, made explicit by T. Tao's in

Tao, T. (2008a). Soft analysis, hard analysis, and the finite convergence principle. Essay, published as Ch. 1.3 of [Tao, 2008b], original version available online at
`http://terrytao.wordpress.com/2007/05/23/soft-analysis-hard-analysis-and-the-finite-convergence-principle/`

- The finite convergence principle is not just an esoteric logical reformulation of a well-known concept. It is actually used in mathematics in e.g. the proof of the Szemerédi regularity lemma.

- In his essay, Tao draws attention to the fact that many infinitary ('soft', qualitative') statements have finitary ('hard', 'quantitative') analogous, which have useful applications.

- It was later observed that this correspondence between soft and hard statements is just the classical functional interpretation!

Idea. Proof interpretations do much more that just extracting numerical information. They help us understand and formalize the connection between infinitary and finintary statements in mathematics.

Finitizing statements

Convergence principles are widely studied in proof mining. Here, the functional which witnesses the corresponding finitary principle is knows as a rate of metastability.

Too see the functional interpretation applied to obtain finitary versions of other infinitary principles see e.g.

- Gaspar, J. and Kohlenbach, U. (2010). On Tao's "finitary" infinite pigeonhole principle.
  Journal of Symbolic Logic, 75(1):355–371
- Safarik, P. and Kohlenbach, U. (2010). On the interpretation of the Bolzano-Weierstrass principle.
  Mathematical Logic Quarterly, 56(5):508–532
- P. (2020). Well quasi-orders and the functional interpretation.
  Schuster, P., Seisenberger, M. and Weiermann, A. editors, *Well Quasi-Orders in Computation, Logic, Language and Reasoning*, Trends in Logic, Springer

Outline

1. Proof mining: Bounds for existential statements

2. Focus: The finite convergence principle and metastability

3. Case study: A fixed point theorem in uniformly convex Banach spaces

4. Formalisation and program synthesis

5. References

Starting point: Banach fixed point theorem

Let (X, d) be a complete metric space and $C \subseteq X$ a closed subset of X. A mapping $T : C \to C$ is a contraction if there exists some $0 \leq q < 1$ such that

$$d(Tx, Ty) \leq q \cdot d(x, y).$$

for all $x, y \in C$. The following is a classic result in metric fixed point theory.

Theorem (Banach, 1922)

If T is a contraction, then its Picard iterates $(T^n x)_{n \in \mathbb{N}}$ converge to a fixpoint of T.

This theorem no longer holds if we weaken the premise by allowing T to be nonexpansive i.e.

$$d(Tx, Ty) \leq d(x, y)$$

for all $x, y \in C$. E.g. For $X = \mathbb{R}$, $C = [0, 1]$ and $Tx = 1 - x$ we have

$$(T^n 0)_{n \in \mathbb{N}} = (0, 1, 0, 1, 0, 1, \ldots)$$

Picard iterates of nonexpansive maps

A natural question is the following: Under what additional conditions can we ensure that the Picard iterates $(T^n x)_{n\in\mathbb{N}}$ converges for *nonexpansive* T. For Hilbert spaces, a nonempty interior condition sufficies.

Theorem (Moreau)

Let X be a Hilbert space, $C \subseteq X$ closed and $T : C \to C$ nonexpansive. If the fixed point set $\mathrm{Fix}(T)$ has nonempty interior, then the Picard iterates converge to a point of $\mathrm{Fix}(T)$.

This result holds more generally in **uniformly convex** Banach spaces.

Uniform convexity

A Banach space is uniformly convex if for any $0 < \varepsilon \leq 2$ there is some $\delta > 0$ such that for any $\|x\| = \|y\| = 1$,

$$\frac{1}{2}\|x + y\| \geq 1 - \delta \Rightarrow \|x - y\| \leq \varepsilon$$

Intuitively: the center of a line segment inside the unit ball must lie deep inside the unit ball unless the segment is short.

Examples of uniformly convex spaces include

- all Hilbert spaces
- L^p spaces for $1 < p < \infty$

A result of Kirk and Sims

I carried out a quantitative analysis of a proof by Kirk and Sims of the following result.

Theorem ([Kirk and Sims, 1999])

Suppose that C is a closed subset of a uniformly convex Banach space and $T : C \to C$ is a nonexpansive mapping with $\mathrm{Int}(\mathrm{Fix}(T)) \neq \varnothing$ *for all $q \in \mathrm{Fix}(T)$. Then for each $x \in C$, the Picard iterates $(T^n x)_{n \in \mathbb{N}}$ converge to a fixed point of T.*

Structure of the theorem

We are given $T : C \to C$ for $C \subseteq X$, and some $x \in C$.

Our assumptions are

- X uniformly convex
- $\mathrm{Int}(\mathrm{Fix}(T)) \neq \varnothing$
- T is nonexpansive

Our conclusion is

- $(T^n x)_{n \in \mathbb{N}}$ converges.

We will now examine each of these in turn from a **quantitative** point of view.

Conclusion: Cauchy convergence of $(T^n x)_{n\in\mathbb{N}}$

Our aim is to produce a quantitative version of the Cauchy convergence of the Picard iterates:

$$\forall\varepsilon > 0\exists n\forall i,j \geq n(\|T^i x - T^j x\| \leq \varepsilon)$$

Our first question: Can we hope to extract a *direct* rate of convergence i.e. a function $\varphi(\varepsilon)$ such that

$$\forall\varepsilon > 0\exists n \leq \varphi(\varepsilon)\forall i,j \geq n(\|T^i x - T^j x\| \leq \varepsilon)$$

Theorem ([Neumann, 2015, Kohlenbach, 2019])

Already for $X = \mathbb{R}$ there exists a nonexpansive mapping $T : [0,1] \to [0,1]$ (which can easily be extended to one with $\mathrm{Int}(\mathrm{Fix}(T)) \neq \varnothing$) such that $(T^n 0)_{n\in\mathbb{N}}$ has no computable rate of convergence.

A metastable formulation of convergence

The combination of negative translation and functional interpretation, when applied to the statement that $(T^n x)_{n\in\mathbb{N}}$ is Cauchy convergent, yields:

$$\forall \varepsilon > 0, g : \mathbb{N} \to \mathbb{N} \exists n \forall i, j \in [n, n + g(n)](\|T^i x - T^j x\| \leq \varepsilon).$$

Our aim will be to produce a rate of metastability for the Picard iterates i.e. a functional $\Omega(\varepsilon, g)$ such that

$$\forall \varepsilon > 0, g : \mathbb{N} \to \mathbb{N} \exists n \leq \Omega(\varepsilon, g) \forall i, j \in [n, n + g(n)](\|T^i x - T^j x\| \leq \varepsilon).$$

In addition to ε and g, Ω will also dependent on quantitative data from each of our assumptions.

Assumption I: X is uniformly convex

Recall the definition of uniform convexity:

$$\forall \varepsilon \in (0,2] \exists \delta > 0 \forall x, y \in B_1[0] (\tfrac{1}{2}\|x+y\| \geq 1 - \delta \to \|x-y\| \leq \varepsilon).$$

This can be given a quantitative form by considering a *modulus of uniform convexity*: This is a function $\Phi : (0,2] \to (0,1]$ satisfying

$$\forall \varepsilon \in (0,2]\ \forall x, y \in B_1[0]\ \left(\tfrac{1}{2}\|x+y\| \geq 1 - \Phi(\varepsilon) \to \|x-y\| \leq \varepsilon\right). \tag{1}$$

Moduli of uniform convexity are **widely used** in proof mining, see [Kohlenbach, 2008, Chapter 17] for a more detailed discussion.

Example

For $X = L_p$ with $2 \leq p < \infty$, a modulus of uniform convexity is given by

$$\Phi(\varepsilon) := \frac{\varepsilon^p}{p2^p}$$

ERSITY OF BATH

Assumption 2: $\mathrm{Int}(\mathrm{Fix}(T)) \neq \varnothing$

$\mathrm{Int}(\mathrm{Fix}(T)) \neq \varnothing$ if there exists some $p \in \mathrm{Fix}(T)$ and $r > 0$ such that $B_r^o[p] \subseteq \mathrm{Fix}(T)$ i.e.

$$\forall x \in X(\underbrace{\|x - p\| <_{\mathbb{R}} r}_{\Sigma_1^0} \to \underbrace{\|Tx - x\| =_{\mathbb{R}} 0}_{\Pi_1^0})$$

The above is a *universal* statement, and thus has no computational content.

To summarise, we just need $p \in \mathrm{Fix}(T)$ and $r > 0$ with $B_r^o[p] \subseteq \mathrm{Fix}(T)$.

Assumption 3: T is nonexpansive

This is also a universal statement and has no computational content. However, nonexpansivity i.e.

$$\|Tx - Ty\| \leq \|x - y\|$$

is only ever used for $y = q$ for $q \in \mathrm{Fix}(T)$. So we can replace it with the weaker assumption that

$$\|Tx - q\| \leq \|x - q\|$$

for all $q \in \mathrm{Fix}(()T)$.

Note. The result can actually be generalised with a more complex condition, namely:

$$\lim_{n \to \infty} \|T^n x - q\| = \inf_{n \in \mathbb{N}} \|T^n x - q\| \quad \text{for all } q \in \mathrm{Fix}(T)$$

but we don't discuss that here!

Main result

Theorem ([P., 2019])

Let X be a Banach space with $C \subseteq X$, $T : C \to C$ a mapping and $x \in C$. Suppose that

- $\|Tx - q\| \leq \|x - q\|$ for all $q \in \mathrm{Fix}(T)$
- $B_r[p] \subseteq \mathrm{Fix}(T)$ for $p \in X$ with $\|x - p\| \leq K$ and $r > 0$;
- Φ is a modulus of uniform convexity for X;

Then

$$\forall \varepsilon > 0, g : \mathbb{N} \to \mathbb{N} \exists n \leq \Omega(\Phi, \Gamma, K, r, \varepsilon, g) \forall i, j \in [n, n + g(n)] (\|T^i x - T^j x\| \leq \varepsilon)$$

for Ω defined as follows:

- $\Omega(\Phi, K, r, \varepsilon, g) := f^{(\lceil K/\eta \rceil)}(0)$;
- $f(j) := j + g^*(j)$;
- $\eta := \frac{r}{4} \cdot \min\{1, \Psi(\min\{\frac{1}{4}, \frac{r}{K}\}, \frac{\varepsilon}{2K})\}$;
- $\Psi(h, \varepsilon') := \min\{\frac{\varepsilon'}{2}, 2h\Phi(\frac{\varepsilon'}{2})\}$.

UNIVERSITY OF BATH

Asymptotic regularity of the Picard iterates

If the Picard iterates converge, then in particular, they must be asymptotically regular:

$$\forall \varepsilon > 0 \exists n \forall i \geq n (\|T^{i+1}x - T^i x\| \leq \varepsilon).$$

In the case that T is nonexpansive, asymptotic regularity is equivalent to the following $\forall\exists$ statement:

$$\forall \varepsilon > 0 \exists n \left(\|T^{n+1}x - T^n x\| \leq \varepsilon\right).$$

This would suggest it is possible to extract a *direct* rate of asymptotic regularity in our setting i.e. a function $f(\varepsilon)$ such that

$$\forall \varepsilon > 0, i \geq f(\varepsilon)(\|T^{i+1}x - T^i x\| \leq \varepsilon).$$

A rate of asymptotic regularity

Theorem ([P., 2019])

Let X be a Banach space with $C \subseteq X$, $T : C \to C$ a mapping and $x \in C$. Suppose that

- $\|Tx - q\| \leq \|x - q\|$ *for all* $q \in \mathrm{Fix}(T)$
- $B_r[p] \subseteq \mathrm{Fix}(T)$ *for* $p \in X$ *with* $\|x - p\| \leq K$ *and* $r > 0$*;*
- Φ *is a modulus of uniform convexity for* X*;*

Then

$$\forall \varepsilon > 0, i \geq f(\varepsilon)(\|T^{i+1}x - T^{i}x\| \leq \varepsilon)$$

where

- $f(\varepsilon) := \lceil K/\eta \rceil$*;*
- $\eta := \frac{r}{4} \cdot \min\{1, \Psi(\min\{\frac{1}{4}, \frac{r}{K}\}, \frac{\varepsilon}{2K})\}$*;*
- $\Psi(h, \varepsilon') := \min\{\frac{\varepsilon'}{2}, 2h\Phi(\frac{\varepsilon'}{2})\}$.

A concrete result for L^p spaces

Theorem ([P., 2019])

Let $T : C \to C$ be a nonexpansive mapping for $C \subseteq L^p$ and $x \in C$. Suppose that $B_r[p'] \subseteq \mathrm{Fix}(T)$ for $p' \in X$ with $\|x - p'\| \leq K$ and $r > 0$. Then

$$\forall \varepsilon > 0, i \geq f(\varepsilon)(\|T^{i+1}x - T^i x\| \leq \varepsilon)$$

where

$$f(\varepsilon) := \left\lceil \frac{p \cdot 2^{3p+1} \cdot K^{p+2}}{\varepsilon^p \cdot r^2} \right\rceil$$

Note that this is a *purely mathematical* result. There is no mention of proof interpretations, higher-order functionals, metastability etc.

Outline

1. Proof mining: Bounds for existential statements
2. Focus: The finite convergence principle and metastability
3. Case study: A fixed point theorem in uniformly convex Banach spaces
4. Formalisation and program synthesis
5. References

In Lecture 2 we ‘extracted’ a list reversing program. Our input was a proof that

$$\forall a \exists b \mathrm{Rev}(a, b)$$

and the result was a term t of System T (i.e. a program) satisfying

$$\forall a \mathrm{Rev}(a, t(a)).$$

Can we automate proof interpretations i.e. write a piece of software which transforms a formal proof to a program:

$$\boxed{\text{Formal proof}} \mapsto \boxed{\text{Program}}$$

Again, the answer is YES! There is even a proof assistant - MINLOG - dedicated to program extraction via functional interpretations:

http://www.mathematik.uni-muenchen.de/~logik/minlog/

What do we get out of formal extraction?

A program is written to satisfy a given specification:

$$\forall x \exists y S(x, y)$$

where $S(x, y)$ specifies how the input should be related to the output.

What a programmer might do.

- Write a program satisfying the specification.
- Debug until they are convinced that it works as it should.

What a proof theorist might do.

- Write a formal proof that for any input, an output satisfying the specification exists.
- Push a button and extract a program.
- No debugging required!
- We may even get additional information, such as a bound on its complexity.

It's not quite as easy as that…

Sounds great! Why aren't programmers using proof interpretations?

- *"Is your list sorting program as good as one a human would write?"*
- *"We use C++. What good to us is a program written in System T?"*
- *"Your extracted program takes up ten pages of text. How does it even work?"*
- *"Group X can already do formal verification and have developed an extremely successful tool."*
- *"Could your technique for synthesising programs be easily used by someone working at the Guardian newspaper?"*

These are all valid points…

Obstacles to overcome

... which highlight the following problems:

Efficiency: It's easy to extract a brute force algorithm, but much more difficult to produce something intelligent, comparable to what a human would write.

Language: Formally extracted programs are typically presented in an abstract language like System T. Real programming languages tend to follow a completely different paradigm, with concepts such as global state, concurrency, and so on...

Scale: Formal verification is a huge business and lots of sophisticated tools have already been developed. On top of this, most big proof assistants (Coq, NUPRL, etc) can extract programs from proofs. A small community in proof theory, dedicated to a particular style of program extraction, cannot possibly compete with this directly.

Accessibility: Ultimately, methods for synthesising verified programs are only useful if they can be used by a non-specialist.

Some first steps

The synthesis of verified programs using proof interpretations like the functional interpretation is a young area with lots of challenges to overcome, but there are already some steps in this direction.

- Berger, U., Miyamoto, K., Schwichtenberg, H., and Seisenberger, M. (2011).

  Minlog - A tool for program extraction supporting algebras and coalgebras.
  In *Proceedings of CALCO 2011*, volume 6859 of *LNCS*, pages 393–399

- Berger, U., Seisenberger, M., and Woods, G. (2014). Extracting imperative programs from proofs: In-place quicksort.
  In *Proceedings of TYPES 2013*, volume 26 of *LIPIcs*, pages 84–106

- Berger, U., Miyamoto, K., Schwichtenberg, H., and Tsuiki, H. (2016). Logic for Gray-code computation.
  In *Concepts of Proof in Mathematics, Philosophy, and Computer Science*, pages 69–110.
  De Gruyter

- P. (2018). A functional interpretation with state.
  In *Proceedings of Logic in Computer Science (LICS 2018)*

Outline

1. Proof mining: Bounds for existential statements
2. Focus: The finite convergence principle and metastability
3. Case study: A fixed point theorem in uniformly convex Banach spaces
4. Formalisation and program synthesis
5. References

References I

Avigad, J. (2009).
The metamathematics of ergodic theory.
Annals of Pure and Applied Logic, 157:64–76.

Berger, U., Miyamoto, K., Schwichtenberg, H., and Seisenberger, M. (2011).
Minlog - A tool for program extraction supporting algebras and coalgebras.
In *Proceedings of CALCO 2011*, volume 6859 of *LNCS*, pages 393–399.

Berger, U., Miyamoto, K., Schwichtenberg, H., and Tsuiki, H. (2016).
Logic for Gray-code computation.
In *Concepts of Proof in Mathematics, Philosophy, and Computer Science*, pages 69–110. De Gruyter.

Berger, U., Seisenberger, M., and Woods, G. (2014).
Extracting imperative programs from proofs: In-place quicksort.
In *Proceedings of TYPES 2013*, volume 26 of *LIPIcs*, pages 84–106.

Gaspar, J. and Kohlenbach, U. (2010).
On Tao's "finitary" infinite pigeonhole principle.
Journal of Symbolic Logic, 75(1):355–371.

Kirk, W. A. and Sims, B. (1999).
Convergence of picard iterates of nonexpansive mappings.
Bulletin of the Polish Academy of Sciences, 47:147–155.

References II

Kohlenbach, K. and Oliva, P. (2003a).
Proof mining in the L_1-approximation.
Annals of Pure and Applied Logic, 121:1–38.

Kohlenbach, U. (1993a).
Effective moduli from ineffective uniqueness proofs. an unwinding of de la vallée poussin's proof for chebycheff approximation.
Annals of Pure and Applied Logic, 64:27–94.

Kohlenbach, U. (1993b).
New effective moduli of uniqueness and uniform a-priori estimates for constants of strong unicity by logical analysis of known proofs in best approximation theory.
Numer. Funct. Anal. Optim., 14:581–606.

Kohlenbach, U. (2008).
Applied Proof Theory - Proof Interpretations and their Use in Mathematics.
Springer Monographs in Mathematics. Springer.

Kohlenbach, U. (2018).
Proof theoretic methods in nonlinear analysis.
In *Proc. Int. Cong. of Math. - ICM 2018*.

References III

Kohlenbach, U. (2019).
On the reverse mathematics and Weihrauch complexity of moduli of regularity and uniqueness.
Computability.

Kohlenbach, U. and Oliva, P. (2003b).
A systematic way of analyzing proofs in mathematics.
Proceedings of the Steklov Institute of Mathematics, 242:136–164.

Neumann, E. (2015).
Computational problems in metrix fixed point theory and their Weihrauch degrees.
Logical Methods in Computer Science, 11:1–44.

P. (2018).
A functional interpretation with state.
In *Proceedings of Logic in Computer Science (LICS 2018)*.

P. (2019).
A new metastable convergence criterion and an application in the theory of uniformly convex Banach spaces.
Journal of Mathematical Analysis and Applications, 478(2):790–805.

References IV

P. (2020).
Well quasi-orders and the functional interpretation.
Schuster, P., Seisenberger, M. and Weiermann, A. editors, *Well Quasi-Orders in Computation, Logic, Language and Reasoning*, Trends in Logic, Springer.

Safarik, P. and Kohlenbach, U. (2010).
On the interpretation of the Bolzano-Weierstrass principle.
Mathematical Logic Quarterly, 56(5):508–532.

Tao, T. (2008a).
Soft analysis, hard analysis, and the finite convergence principle.
Essay, published as Ch. 1.3 of [Tao, 2008b], original version available online at `http://terrytao.wordpress.com/2007/05/23/soft-analysis-hard-analysis-and-the-finite-convergence-principle/`.

Tao, T. (2008b).
Structure and Randomness: Pages from Year 1 of a Mathematical Blog.
American Mathematical Society.