A brief overview of applied proof theory, and some ideas for where it might be going next!

Thomas Powell
Department of Computer Science
University of Bath

Mathematical Foundations of AI seminar

Queen Mary University of London
2 February 2023

These slides will be available at
`https://t-powell.github.io/talks`

A bit about me…

- Trained as a mathematician (functional analysis, combinatorics, logic).
- PhD in mathematical logic at QMUL (Computer Science department).
- Focus on proof theory and its applications in both maths and CS. Postdoc positions in France (IHÉS and IHP), Austria (Innsbruck) and Germany (TU Darmstadt).
- Now a lecturer in the *Mathematical Foundations of Computation* group at Bath.

Structure of talk

I have two main goals:

1. Short introduction to applied proof theory.
2. Outline some new ideas.

Please feel free to interrupt and ask questions!

Applied Proof Theory: A very short introduction

What is applied proof theory?

There is a famous quote due to G. Kreisel (*A Survey of Proof Theory II*):

> *"What more do we know when we know that a theorem can be proved by limited means than if we merely know that it is true?"*

In other words, the **proof** of a theorem gives us much more information than the mere **truth** of that theorem.

Applied proof theory is a branch of logic that uses proof theoretic techniques to exploit this phenomenon.

Everyone does applied proof theory

PROBLEM. Give me an upper bound on the nth prime number p_n.

1. What is p_n? I know it exists because of Euclid…
2. Specifically, given $p_1, \ldots, p_{n-1}$, I know that $N := p_1 \cdot \ldots \cdot p_{n-1} + 1$ contains a *new* prime factor q, and so $p_n \leq q \leq N$.
3. In other words, the sequence $\{p_n\}$ satisfies

$$p_n \leq p_1 \cdot \ldots \cdot p_{n-1} + 1 \leq (p_{n-1})^{n-1}$$

4. By induction, it follows that e.g. $p_n < 2^{2^n}$.

This is a simple example of applied proof theory in action! From the **proof** that there are infinitely many primes, we have inferred a **bound** on the nth prime.

… but it's not always that simple

Theorem (Littlewood 1914)

The functions of integers

(a) $\psi(x) - x$, *and*

(b) $\pi(x) - li(x)$

change signs infinitely often, where $\pi(x)$ *is the number of prime* $\leq x$, $\psi(x)$ *is the is logarithm of the l.c.m. of numbers* $\leq x$ *and* $li(x) = \int_0^x (1/\log(u))du$.

The original proof is utterly nonconstructive, using among other things a **case distinction on the Riemann hypothesis**. At the time, no numerical value of x for which $\pi(x) > li(x)$ was known.

In 1952, Kreisel analysed this proof and extracted recursive bounds for sign changes (*On the interpretation of non-finitist proofs, Part II*):

> *"Concerning the bound … note that it is to be expected from our principle, since if the conclusion … holds when the Riemann hypothesis is true, it should also hold when the Riemann hypothesis is nearly true: not all zeros need lie on* $\sigma = \frac{1}{2}$, *but only those whose imaginary part lies below a certain bound … and they need not lie on the line* $\sigma = \frac{1}{2}$, *but near it"*

What applied proof theory looks like today

Theorem (Kirk and Sims, *Bulletin of the Polish Academy of Sciences* 1999)

Suppose that C is a closed subset of a uniformly convex Banach space and $T : C \to C$ is asymptotically nonexpansive with $\operatorname{int}(\operatorname{fix}(T)) \neq \emptyset$. Then for each $x \in C$ the sequence $\{T^n x\}$ converges to a fixed point of T.

Theorem (P., *Journal of Mathematical Analysis and Applications* 2019)

Let $T : C \to C$ be a nonexpansive mapping in L_p for $2 \leq p < \infty$, and suppose that $B_r[q] \subset \operatorname{fix}(T)$ for some $q \in L_p$ and $r > 0$. Suppose that $x \in C$ and $\|x - q\| < K$, and define $x_n := T^n x$. Then for any $\varepsilon > 0$ we have

$$\forall n \geq f(\varepsilon)(\|Tx_n - x_n\| \leq \varepsilon)$$

where

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

Is this just about quantitative information?

The following is lifted directly from Kohlenbach (*Some logical metatheorems with applications in functional analysis, Trans. Amer. Math. Soc 2005*):

Corollary

Let P (resp. K) be a $\mathcal{A}^\omega$ definable Polish space (resp. compact metric space) and $B_\forall$, $C_\exists$ be as before $\forall$- resp. $\exists$-formulas. If $\mathcal{A}^\omega[X, d, W]$ proves that

$$\forall x \in P\, \forall y \in K\, \forall z^X, f : X \to X\, (f \text{ n. e. } \wedge \operatorname{Fix}(f) \neq \emptyset \wedge \forall u \in \mathbb{N}\, B_\forall \Rightarrow \exists v \in \mathbb{N}\, C_\exists),$$

then we can extract from the proof a computable functional $\Phi : \mathbb{N}^\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ (on representatives $r_x : \mathbb{N} \to \mathbb{N}$ of elements $x \in P$) such that for all $r_x \in \mathbb{N}^\mathbb{N}$, $b \in \mathbb{N}$

$$\forall y \in K\, \forall z \in X, f : X \to X\, (f \text{ n. e. } \wedge \forall u \leq \Phi(r_x, b)\, B_\forall \Rightarrow \exists v \leq \Phi(r_x, b)\, C_\exists)$$

holds in any (nonempty) hyperbolic space (X, d, W) whose metric is bounded by $b \in \mathbb{N}$.

How does it work? (The official version)

We obtained a bound on the nth prime from Euclid's proof without any special techniques. However, serious applications usually involve some of the following, either implicitly or explicitly:

- proof interpretations, particularly Gödel's Dialectica interpretation
- computability and complexity in higher types, logical relations (particularly *majorizability*)
- axiomatic systems and type theory.

In all cases, one also needs to do some serious *mathematics*! (It is helpful to have collaborators from the fields of application).

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 know result, which I shall call the "finite convergence principle" … It is the finitary analogue of an utterly trivial infinitary result – namely, that every bouned monotone sequence convergences – but sometimes, a careful analysis of a trivial result can be surprisingly revealing, as I hope to demonstrate here."*

An even more utterly trivial infinitary result: The drinkers paradox

In any pub there is someone such that if they are drinking, then everyone is drinking

ALTERNATIVELY:

$$\exists x \in P \; (D(x) \to \forall y \in P \; D(y))$$

Proof.

Either everyone is drinking, so we can pick $x := c$ to be some canonical drinker $c \in P$
OR there is at least someone $y \in D$ *not* drinking, in which case we pick $x := y$. □

In a pub with infinitely many drinkers, this becomes computationally problematic…
There is no effective way of finding x.

The drinkers paradox is an infinitary theorem.

Let's finitise it!

$$
\begin{aligned}
& \exists x \in P\ (D(x) \to \forall y \in P\ D(y)) \\
\Leftrightarrow\ & \exists x \in P\ \forall y \in P\ (D(x) \to D(y)) \\
\Leftrightarrow\ & \neg\neg \exists x \in P\ \forall y \in P\ (D(x) \to D(y)) \\
\Leftrightarrow\ & \neg \forall x \in P\ \exists y \in P\ \neg (D(x) \to D(y)) \\
\Leftrightarrow\ & \neg \exists f : P \to P\ \forall x \in P\ \neg (D(x) \to D(fx)) \\
\Leftrightarrow\ & \underline{\forall f : P \to P\ \exists x \in P\ (D(x) \to D(fx))} \quad (*)
\end{aligned}
$$

We can now solve x in f: Either fx is drinking, so we can set $x := c$, OR fx is not drinking, in which case set $x := fc$.

Original DP: *In any pub there is a person x such that if they are drinking, then <u>everyone</u> is drinking*

Finitary DP: *Given a pub and <u>any function f</u>, there is a person $x \in \{c, fc\}$ such that if they are drinking, then person fx is drinking*

The formula $(*)$ corresponds to the classical Dialectica interpretation of the original DP! The witnesses $\{c, fc\}$ give rise to the corresponding Herbrand disjunction.

Tao's example

Monotone convergence principle (MCP): Let $\{x_n\}$ be an increasing sequence in $[0,1]$. Then for any $\varepsilon > 0$ there exists some $N \in \mathbb{N}$ such that $|x_m - x_n| \leq \varepsilon$ for all $m, n \geq N$.

Finite convergence principle (FCP): If $\varepsilon > 0$ and $f : \mathbb{N} \to \mathbb{N}$ and

$$0 \leq x_0 \leq \ldots \leq x_M \leq 1$$

is such that M is sufficiently large depending of ε and f, then there exists $0 \leq N \leq N + f(N) \leq M$ such that $|x_m - x_n| \leq \varepsilon$ for all $N \leq m, n \leq N + f(N)$.

Two interesting observations:

1. FCP $\approx$ classical Dialectica intepretation of MCP
2. By analysing the proof of MCP we can extract a bound on M, which is $\tilde{f}^{\lfloor 1/\varepsilon \rfloor}(0)$ for $\tilde{f}(x) := x + f(x)$.

Why is Tao interested in finitary theorems?

> *"So, we've now extracted a quantitative finitary equivalent of the infinitary principle that every bounded monotone sequence converges. But can we actually use this finite convergence principle for some non-trivial finitary application? The answer is a definite yes: the finite convergence principle (implicitly) underlies the famous Szemerédi regularity lemma, which is a major tool in graph theory, and also underlies some rather less well known regularity lemmas, such as the arithmetic regularity lemma of Green. More generally, this principle seems to often arise in any finitary application in which tower-exponential bounds are inevitably involved."*

Quantitative, finitary versions of mathematical principles are of interest in their own right, and play a role in mathematics **entirely independently of proof theory**.

But actually *finding* the correct finitization of a give principle is surprisingly hard!

Why are we interested in finitary theorems?

Purely existential theorems typically use infinitary principles as lemmas i.e.

$$\text{infinitary principle} \Rightarrow \exists x\, A(x)$$

On the face of it, these proofs are *nonconstructive*, and we have no way of finding x.

But there is a formal way (Dialectica interpretation) to replace the infinitary principle with its finitary counterpart.

$$\text{finitary principle} \Rightarrow \exists x \leq t\, A(x)$$

Typically, we can then use a bound for the finitary principle to compute a bound on x.

Remember Kreisel:

> *"if the conclusion … holds when the Riemann hypothesis is true, it should also hold when the Riemann hypothesis is nearly true"*

What can we achieve with applied proof theory?

1. Computational information from proofs (including those which are at first glance completely nonconstructive).

2. Qualitative generalisations of theorems, unifying frameworks.

3. Finitary formulations of infinitary principles, complete with relevant numerical data.

4. Logical metatheorems and abstract variants of proofs in the literature, which explain and generalise mathematical phenomena.

What makes an area of mathematics amenable to proof theoretic techniques?

1. Numerical information is relevant in that area.

2. *Proofs* are non-trivial, and use subtle nonconstructive lemmas, but *theorems* are 'nice' from a proof theoretic perspective.

3. There are many variations of core ideas in different settings.

The situation in 2023

Applied proof theory is a small community. Main strongholds are:

- Germany (TU Darmstadt).
- USA (Carnegie Mellon, Pennsylvania).
- Smaller centres include Romania (Bucharest, Cluj-Napoca) and Portugal (Lisbon).

In the UK, it's essentially just Bath (me) and QMUL (Paulo Oliva).

Over the last 20 years or so, several hundred papers, main areas of application being:

- Nonlinear analysis
- Fixed point theory
- Approximation theory
- Ergodic theory
- Convex optimization

Results typically published in specialist journals within areas of application, or general mathematical journals.

A simple sketch

Contraction mappings

We work in a Banach space X.

A mapping $T : E \to E$ for $E \subseteq X$ is called *strongly contractive* (or often just a *contraction mapping*) if there exists $k \in [0, 1)$ such that $\forall x, y \in E$:

$$\|Tx - Ty\| \leq (1 - k) \|x - y\|$$

Theorem (Banach fixed point theorem)

If T is strongly contractive then it possesses a fixpoint q. Moreover, from any starting point x_0 the sequence $\{x_n\}$ defined by $x_{n+1} := Tx_n$ converges to q, with rate of convergence

$$\|x_n - q\| \leq \frac{(1 - k)^n}{k} \|x_1 - x_0\|$$

space X + mapping T + algorithm $\{x_n\}$ $\Longrightarrow$ convergence to fixpoint

A generalisation of the Banach fixed point theorem:

A mapping $T : E \to E$ for $E \subseteq X$ is called *ψ-weakly contractive* if $\psi : [0, \infty) \to [0, \infty)$ is a nondecreasing function with $\psi(0) = 0$ and $\psi(t) > 0$ for $t > 0$, and $\forall x, y \in E$:

$$\|Tx - Ty\| \leq \|x - y\| - \psi(\|x - y\|)$$

In the case that $\psi(t) := kt$ then T is strongly contractive.

Theorem (Alber and Guerre-Delabriere 1997)

If T is weakly contractive then it possesses a fixpoint q. Moreover, from any starting point x_0 the sequence $\{x_n\}$ defined by $x_{n+1} := Tx_n$ converges to q, with rate of convergence

$$\|x_n - q\| \leq \Psi^{-1}(\Psi(\|x_0 - q\|) - n)$$

where Ψ is given by

$$\Psi(s) := \int^s \frac{dt}{\psi(t)}$$

space X + mapping T + algorithm $\{x_n\}$ $\Longrightarrow$ convergence to fixpoint

Example of a weakly contractive mapping

Define $X = \mathbb{R}$ and $T : [0,1] \to [0,1]$ by $Tx := \sin x$. Then we can show that

$$|\sin x - \sin y| \leq |x-y| - \frac{1}{8}|x-y|^3$$

and so $\sin$ is ψ-weakly contractive for $\psi(t) = \frac{1}{8}t^3$.

The unique fixpoint of $\sin$ is $x = 0$, and defining $x_{n+1} := \sin x_n$ we have $x_n \to 0$ with rate of convergence

$$x_n \leq \frac{1}{\sqrt{x_0^{-2} + \frac{n-1}{4}}}$$

There have been lots of generalisations e.g.

A mapping $T : E \to E$ for $E \subseteq X$ is called totally asymptotically ψ-weakly contractive if $\psi, \phi : [0, \infty) \to [0, \infty)$ are nondecreasing functions with $\psi(0) = \phi(0) = 0$ and $\psi(t), \phi(t) > 0$ for $t > 0$, and $\forall x, y \in E$:

$$\|T^n x - T^n y\| \leq \|x - y\| - \psi(\|x - y\|) + k_n \phi(\|x - y\|) + l_n$$

for $k_n, l_n \to 0$. In the case that $k_n = l_n := 0$ then T is ψ-weakly contractive.

Theorem (Adapted from Alber, Chidume and Zegeye 2006)

Suppose that $E \subseteq X$ is convex, T is asymptotically ψ-weakly contractive and q is a fixpoint of T. Moreover, from any starting point x_0 define the sequence $\{x_n\}$ by

$$x_{n+1} = (1 - \alpha_n)x_n + \alpha_n T^n x_n$$

where $\{\alpha_n\}$ is some sequence of nonnegative reals with $\sum_{n=0}^{\infty} \alpha_n = \infty$. Suppose that $\|x_n - q\|$ is bounded. Then $x_n \to q$.

A clear closed form expression for a rate of convergence is not given.

space X + mapping T + algorithm $\{x_n\}$ $\Longrightarrow$ convergence to fixpoint

The general strategy for proving convergence to fixpoints of ψ-weakly contractive mappings

Step 1: Show that, under suitable conditions, the sequence $\mu_n := \|x_n - q\|$ satisfies

$$(*) \quad \mu_{n+1} \leq \mu_n - \alpha_n \psi(\mu_n) + \gamma_n$$

where $\{\alpha_n\}$ are typically step-sizes that define the algorithm $\{x_n\}$, and $\{\gamma_n\}$ are error terms.

Step 2: Appeal to properties of abstract recurrence inequalities:

Lemma

Suppose that $\{\mu_n\}$ is a sequence of nonnegative reals satisfying $(*)$ for some nondecreasing function $\psi : [0, \infty) \to [0, \infty)$ which is positive on $(0, \infty)$, and sequences $\{\alpha_n\}$ and $\{\gamma_n\}$ of nonnegative reals satisfying

- $\sum_{i=0}^{\infty} \alpha_i = \infty$
- $\gamma_n / \alpha_n \to 0$ *as* $n \to \infty$

Then $\mu_n \to 0$ as $n \to \infty$

Proof.

Typically a nonconstructive argument involving liminfs and convergent subsequences. □

Lemma (Quantitative convergence for recurrence inequality)

Let $\{\mu_n\}$ be a sequence of nonnegative reals such that for any $\delta > 0$ we have

$$\mu_{n+1} \leq \mu_n - \alpha_n \psi(\mu_n) + \alpha_n \delta$$

for all $n \geq \sigma(\delta)$, where:

- *$\psi : [0, \infty) \to [0, \infty)$ is a nondecreasing function with $\psi(t) > 0$ for $t > 0$;*
- *$\{\alpha_n\} \subset [0, \alpha]$ is a sequence of nonnegative real numbers such that $\sum_{n=0}^{\infty} \alpha_n = \infty$ with rate of divergence $r : (0, \infty) \times (0, \infty) \to \mathbb{N}$ i.e.*

$$\forall N \in \mathbb{N}, x > 0 \left(\sum_{n=N}^{r(N,x)} \alpha_n > x \right)$$

Then $\mu_n \to 0$, and moreover, for any $\varepsilon > 0$ we have

$$\forall n \geq \Phi(\varepsilon)(\mu_n \leq \varepsilon)$$

where Φ is defined by

$$\Phi(\varepsilon) := r\left(\sigma\left(\frac{1}{2}\min\left\{\psi\left(\frac{\varepsilon}{2}\right), \frac{\varepsilon}{\alpha}\right\}\right), 2\int_{\varepsilon/2}^{c} \frac{dt}{\psi(t)}\right)$$

and c is an upper bound for $\{\mu_n\}$.

Theorem (Adapted from P. and Wiesnet 2021)

Suppose that $E \subseteq X$ is convex, $\{A_n\}$ is quasi asymptotically ψ-weakly contractive w.r.t q and with modulus σ, in the sense that for all $\delta, c > 0$ and $x, y \in E$:

$$\|x - q\| \leq c \implies \forall n \geq \sigma(\delta, c)(\|A_n x - q\| \leq \|x - q\| - \psi(\|x - q\|) + \delta)$$

Moreover, from any starting point x_0 define the sequence $\{x_n\}$ by

$$x_{n+1} = (1 - \alpha_n)x_n + \alpha_n A_n x_n$$

where $\{\alpha_n\} \in [0, \alpha]$ is some sequence of nonnegative reals with $\sum_{n=0}^{\infty} \alpha_n = \infty$. Suppose that $\|x_n - q\|$ is bounded by $c > 0$. Then $x_n \to q$, with rate of convergence

$$\|x_n - q\| \leq F^{-1}\left(2\Psi(c) - \sum_{i=0}^{n-2} \alpha_i\right)$$

where $F : (0, \infty) \to \mathbb{R}$ is any strictly increasing and continuous function satisfying

$$F(\varepsilon) \geq 2\Psi\left(\frac{\varepsilon}{2}\right) - \alpha \cdot \sigma\left(\frac{1}{2}\min\left\{\psi\left(\frac{\varepsilon}{2}\right), \frac{\varepsilon}{\alpha}\right\}, c\right)$$

and Ψ is given by

$$\Psi(s) := \int^{s} \frac{dt}{\psi(t)}$$

Plans for the future

Probabilistic convergence

Almost all research in applied proof theory has focused on ordinary convergence, but there has been some fascinating work in measure theory/probability theory, where notions of convergence are more subtle.

A finitized version (along the lines of Tao) of ordinary Cauchy convergence of a sequence $\{x_n\}$ is:

For all $\varepsilon > 0$ *and* $f : \mathbb{N} \to \mathbb{N}$ *there exists* m *such that*

$$(\forall n, n')\,(m \leq n, n' \leq f(m) \implies |x_n - x_{n'}| < \varepsilon)$$

The following is a finitized version (i.e. Dialectica interpretation) of almost uniform convergence for a sequence of random variables $\{X_n\}$ due to Avigad et al. 2012.:

For all $\lambda, \varepsilon > 0$ *and* $f : \mathbb{N} \to \mathbb{N}$ *there exists* M *such that*

$$\mathbb{P}\{\omega : (\forall m \leq M)\,(\exists n, n')\,(m \leq n, n' \leq f(m) \text{ and } |X_n(\omega) - X_{n'}(\omega)| \geq \varepsilon)\} < \lambda$$

Proof theory in stochastic optimization

Can we extend proof theoretic work in ordinary optimization to **stochastic algorithms**? These rely heavily on things like the *Robbins-Siegmund lemma* (which in turn relies on Martingale theory):

Lemma (Robbins-Siegmund 1971)

Let $\{\mu_n\}$, $\{\delta_n\}$, $\{\varepsilon_n\}$ *and* $\{\theta_n\}$ *be sequences of nonnegative reals such that* $\sum_{i=0}^{\infty} \varepsilon_i < \infty$, $\sum_{i=0}^{\infty} \delta_i < \infty$

$$E[\mu_{n+1} \mid \mathcal{F}_n] \leq (1 + \delta_n)\mu_n + \varepsilon_n - \theta_n \quad a.s.$$

for some filtration $\{\mathcal{F}_n\}$. *Then* $\sum_{i=0}^{\infty} \theta_i < \infty$ *and* $\{\mu_n\}$ *converges a.s.*

- Can we give results of this kind a computational interpretation?
- Are there applications in stochastic optimization?

Computer-formalizing applied proof theory (and the areas of application!) in theorem provers

This is particularly pertinent for applied proof theory:

- We are already focused on understanding the abstract, logical structure of proofs.
- Results in many areas of application have been explained as instances of general metatheorems, formalised within specialised type theories.
- Lots of standard techniques (e.g. 'finitization' of theorems via proof interpretations) could be automated using tactics.

I'm aware of two projects on developing libraries for applied proof theory (both in Lean):

- H. Cheval: `https://github.com/hcheval`
- M. Neri: `https://github.com/mneri123/Proof-mining-`

Keji is building a library on convergence results for sequences of reals, along with rates of convergence/metastability.

This is what it looks like

```
lemma abstract_lemma1 (θ : nnseq )(α : nnseq)(K: {x: ℝ // x > 0}) (r: ℕ → {x: ℝ // x > 0} → ℕ )
(N : {x:ℝ // x > 0 }  → ℕ ) (ϕ : {x:ℝ // x > 0 }  → {x:ℝ // x > 0 })
(h1 : ∀(n:ℕ), (θ.1 n) < K) (h2: RoD r α)
(h3: ∀ ε : {x:ℝ // x > 0 } , ∀ n ≥ N(ε), (ε:ℝ) < θ.1 (n + 1)  → θ.1 (n + 1) ≤ θ.1 n - (α.1 n)*ϕ(ε)):
RoC (λ ε : {x: ℝ // x > 0},  (r (N ε) ⟨K/(ϕ ε), div_pos K.2 (ϕ ε).2 ⟩+1)) θ  :=
begin
have
H1 : ∀ ε : {x:ℝ // x > 0 },∀ n ≥ N(ε), θ.1 n ≤ ε  → θ.1 (n + 1) ≤ ε,
by_contradiction p1,
push_neg at p1,
cases p1 with ε p2,
cases p2 with n p3,
have p5 : ε < ε,
calc ε.1 < θ.1 (n+1): (p3.2).2
... ≤ θ.1 n - (α.1 n)*ϕ(ε): h3 ε n p3.1 (p3.2).2
... ≤ θ.1 n : sub_le_self (θ.1 n) (mul_nonneg (α.2 n) (le_of_lt (ϕ ε).2 ))
... ≤ ε :(p3.2).1,
exact (lt_self_iff_false ε).mp p5,
have H2 : ∀ ε : {x :ℝ // x > 0}, ∃ n ∈ finset.Ico (N ε) ((r (N ε) ⟨↑K / ↑(ϕ ε), _⟩)+1), θ.1 (n + 1) ≤
by_contradiction,
push_neg at h,
```

Automated reasoning

In applied proof theory we often organise proofs into

- Critical components (with computational content)
- Routine components (with little or no computational content)

Can we develop specialist automated reasoning algorithms to:

1. Help us generate proofs,
2. Automatically produce quantitative information?

Thank you!