Proof-theoretical unwinding of mathematics

Pedro Pinto

Technische Universität Darmstadt
Department of Mathematics

Encontro Nacional da SPM 2024
Universidade do Minho, Braga

12 July

Outline

What is Proof Mining?

Functional Interpretations

Informally, it is a mapping F that takes a formula A of a theory $\mathcal{A}$ and maps it to a formula $A^F \equiv \exists \underline{u} A_F(\underline{u})$ of a theory $\mathcal{B}$

$$A \quad \rightsquigarrow \quad A^F \equiv \exists \underline{u} A_F(\underline{u}).$$

Functional Interpretations

Informally, it is a mapping F that takes a formula A of a theory $\mathcal{A}$ and maps it to a formula $A^F \equiv \exists \underline{u} A_F(\underline{u})$ of a theory $\mathcal{B}$

$$A \quad \rightsquigarrow \quad A^F \equiv \exists \underline{u} A_F(\underline{u}).$$

Proof interpretations: (proofs of) theorems of $\mathcal{A}$ are mapped to (proofs of) theorems of $\mathcal{B}$:

$$\mathcal{A} \vdash A \quad \rightsquigarrow \quad \mathcal{B} \vdash A^F.$$

in a way that one obtains a term $\underline{t}$ witnessing the $\exists$-quantification in A^F:

$$\mathcal{A} \vdash A \quad \Rightarrow \quad \text{there is a term} \underline{t} \text{ such that } \mathcal{B} \vdash A_F(\underline{t}).$$

Main Applications

Functional interpretations are used to show results of:

- **Relative consistency**: $\bot^F \equiv \bot$, so

$$\mathcal{A} \vdash \bot \Rightarrow \mathcal{B} \vdash \bot, \text{ i.e., } Con(\mathcal{B}) \Rightarrow Con(\mathcal{A});$$

- **Conservation**: if $A^F \equiv A$, for $A \in \Gamma$, then

$$\text{for any } A \in \Gamma, \qquad \mathcal{A} \vdash A \Rightarrow \mathcal{B} \vdash A;$$

- **Unprovability**: if $\mathcal{B} \nvdash A_F(t)$, then $\mathcal{A} \nvdash A$;

Main Applications

Functional interpretations are used to show results of:

- **Relative consistency**: $\bot^F \equiv \bot$, so
$$\mathcal{A} \vdash \bot \Rightarrow \mathcal{B} \vdash \bot, \text{ i.e., } Con(\mathcal{B}) \Rightarrow Con(\mathcal{A});$$
- **Conservation**: if $A^F \equiv A$, for $A \in \Gamma$, then
$$\text{for any } A \in \Gamma, \qquad \mathcal{A} \vdash A \Rightarrow \mathcal{B} \vdash A;$$
- **Unprovability**: if $\mathcal{B} \nvdash A_F(t)$, then $\mathcal{A} \nvdash A$;
- **Kreisel's shift of paradigm:** Functional interpretations allow for the extraction of the **computational content** hidden in the proof of the theorem – the term $\underline{t}$ captures the computational content of (the proof of) A.

Some history

- K.Gödel: Dialectica (1958)
  - $Con(T) \Rightarrow Con(HA)$

Some history

- K.Gödel: Dialectica (1958)
  - $Con(T) \Rightarrow Con(HA)$
- U.Kohlenbach: monotone functional interpretation (1996)
  - Search for bounds instead of precise witnesses
  - General Logical Metatheorems (2003-05)

Some history

- K.Gödel: Dialectica (1958)
  - $Con(T) \Rightarrow Con(HA)$
- U.Kohlenbach: monotone functional interpretation (1996)
  - Search for bounds instead of precise witnesses
  - General Logical Metatheorems (2003-05)
- F.Ferreira and P.Oliva: bounded functional interpretation (2005)
  - Completely new translation of formulas
  - Independence on bounded parameters is intrinsic/explicit

Peano Arithmetic in all finite types

The finite types $\mathcal{T}^\omega$ are defined inductively by:

$$0 \in \mathcal{T}^\omega \quad \text{(natural numbers)},$$

$$\rho, \sigma \in \mathcal{T}^\omega \Rightarrow \rho \to \sigma \in \mathcal{T}^\omega \quad \text{(functions from } \rho \text{ to } \sigma\text{)}.$$

Peano Arithmetic in all finite types

The finite types $\mathcal{T}^\omega$ are defined inductively by:

$$
\begin{aligned}
&0 \in \mathcal{T}^\omega \quad \text{(natural numbers)},\\
&\rho, \sigma \in \mathcal{T}^\omega \Rightarrow \rho \to \sigma \in \mathcal{T}^\omega \quad \text{(functions from } \rho \text{ to } \sigma\text{)}.
\end{aligned}
$$

In the language of Peano arithmetic in all finite types, we consider an appropriate notion of majorizability:

$$
\begin{cases}
n \leqslant_0^* m & \leftrightarrow \quad n \leqslant_0 m\\
x \leqslant_{\rho\to\sigma}^* y & \leftrightarrow \quad \forall u^\rho, v^\rho \big(u \leqslant_\rho^* v \to xu \leqslant_\sigma^* yv \wedge yu \leqslant_\sigma^* yv\big)
\end{cases}
$$

Peano Arithmetic in all finite types

The finite types $\mathcal{T}^\omega$ are defined inductively by:

$$0 \in \mathcal{T}^\omega \quad \text{(natural numbers)},$$
$$\rho, \sigma \in \mathcal{T}^\omega \Rightarrow \rho \to \sigma \in \mathcal{T}^\omega \quad \text{(functions from } \rho \text{ to } \sigma\text{)}.$$

In the language of Peano arithmetic in all finite types, we consider an appropriate notion of majorizability:

$$\begin{cases} n \leqslant_0^* m & \leftrightarrow \quad n \leqslant_0 m \\ x \leqslant_{\rho\to\sigma}^* y & \leftrightarrow \quad \forall u^\rho, v^\rho \big(u \leqslant_\rho^* v \to xu \leqslant_\sigma^* yv \wedge yu \leqslant_\sigma^* yv \big) \end{cases}$$

- E.g., for $f, g : 0 \to 0$, we have $f \leqslant_1^* g$ iff f is less or equal than g pointwise and that g is nondecreasing. We say that f is *monotone* if $f \leqslant_1^* f$, which just means it is nondecreasing.

Peano Arithmetic in all finite types

The finite types $\mathcal{T}^\omega$ are defined inductively by:

$$0 \in \mathcal{T}^\omega \quad \text{(natural numbers)},$$
$$\rho, \sigma \in \mathcal{T}^\omega \Rightarrow \rho \to \sigma \in \mathcal{T}^\omega \quad \text{(functions from } \rho \text{ to } \sigma\text{)}.$$

In the language of Peano arithmetic in all finite types, we consider an appropriate notion of majorizability:

$$\begin{cases} n \trianglelefteq_0 m & \leftrightarrow \quad n \leqslant_0 m \\ x \trianglelefteq_{\rho\to\sigma} y & \to \quad \forall u^\rho, v^\rho \big(u \trianglelefteq_\rho v \to xu \trianglelefteq_\sigma yv \wedge yu \trianglelefteq_\sigma yv\big) \end{cases}$$

- E.g., for $f, g : 0 \to 0$, we have $f \leqslant_1^* g$ iff f is less or equal than g pointwise and that g is nondecreasing. We say that f is *monotone* if $f \leqslant_1^* f$, which just means it is nondecreasing.

Together with the usual logical and arithmetical constants, and the combinators from λ-abstraction, we also have:
Bounded quantification: $\forall x \trianglelefteq t$ and $\exists x \trianglelefteq t$, where $x \notin \mathrm{FV}(t)$.
Monotone quantification: $\tilde{\forall} x \equiv \forall x \trianglelefteq x$ and $\tilde{\exists} x \equiv \exists x \trianglelefteq x$.

Bounded formulas are formulas that don't contain unbounded quantifiers, for example

$$A_{\mathrm{qf}} \mid \forall n' \leqslant n\, A_{\mathrm{bd}} \mid \forall t \in [0,1]\, A_{\mathrm{bd}}.$$

Together with the usual logical and arithmetical constants, and the combinators from λ-abstraction, we also have:
Bounded quantification: $\forall x \trianglelefteq t$ and $\exists x \trianglelefteq t$, where $x \notin \mathrm{FV}(t)$.
Monotone quantification: $\tilde{\forall} x \equiv \forall x \trianglelefteq x$ and $\tilde{\exists} x \equiv \exists x \trianglelefteq x$.

Bounded formulas are formulas that don't contain unbounded quantifiers, for example

$$A_{\mathrm{qf}} \mid \forall n' \leqslant n\, A_{\mathrm{bd}} \mid \forall t \in [0,1]\, A_{\mathrm{bd}}.$$

$\mathrm{PA}^{\omega}_{\trianglelefteq}$ is Peano Arithmetic in all finite types with the (intensional) majorizability relation $\trianglelefteq$.

Characteristic Principles

- MAJ^ω – **Majorizability Axioms**:

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

- $\mathrm{mAC}^\omega_{\mathrm{bd}}$ – **Monotone Bounded Choice**:

$$\tilde{\forall} x \, \tilde{\exists} y \, A_{\mathrm{bd}}(x,y) \to \tilde{\exists} f \, \tilde{\forall} x \, \tilde{\exists} y \trianglelefteq f(x) \, A_{\mathrm{bd}}(x,y)$$

- $\mathrm{bC}^\omega_{\mathrm{bd}}$ – **Bounded Collection Principle**:

$$\forall x \trianglelefteq t \, \exists y \, A_{\mathrm{bd}}(x,y) \to \exists z \, \forall x \trianglelefteq t \, \exists y \trianglelefteq z \, A_{\mathrm{bd}}(x,y)$$

Characteristic Principles

- MAJ^ω – **Majorizability Axioms**:

$$\forall x\ \exists y\ (x \trianglelefteq y)$$

- $\mathrm{mAC}^\omega_{\mathrm{bd}}$ – **Monotone Bounded Choice**:

$$\tilde{\forall} x\ \tilde{\exists} y\ A_{\mathrm{bd}}(x,y) \to \tilde{\exists} f\ \tilde{\forall} x\ \tilde{\exists} y \trianglelefteq f(x)\ A_{\mathrm{bd}}(x,y)$$

- $\mathrm{bC}^\omega_{\mathrm{bd}}$ – **Bounded Collection Principle**:

$$\forall x \trianglelefteq t\ \exists y\ A_{\mathrm{bd}}(x,y) \to \exists z\ \forall x \trianglelefteq t\ \exists y \trianglelefteq z\ A_{\mathrm{bd}}(x,y)$$

Bounded functional interpretation

$A \rightsquigarrow A^B \equiv \tilde{\forall}\underline{x}\tilde{\exists}\underline{y}\ A_B(\underline{x},\underline{y})$, w/ A_B a bounded formula.

Characteristic Principles

- MAJ^ω – **Majorizability Axioms**:

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

- $\mathrm{mAC}^\omega_{\mathrm{bd}}$ – **Monotone Bounded Choice**:

$$\tilde{\forall} x\, \tilde{\exists} y\, A_{\mathrm{bd}}(x, y) \to \tilde{\exists} f\, \tilde{\forall} x\, \tilde{\exists} y \trianglelefteq f(x)\, A_{\mathrm{bd}}(x, y)$$

- $\mathrm{bC}^\omega_{\mathrm{bd}}$ – **Bounded Collection Principle**:

$$\forall x \trianglelefteq t\, \exists y\, A_{\mathrm{bd}}(x, y) \to \exists z\, \forall x \trianglelefteq t\, \exists y \trianglelefteq z\, A_{\mathrm{bd}}(x, y)$$

Bounded functional interpretation

$A \rightsquigarrow A^B \equiv \tilde{\forall} \underline{x} \tilde{\exists} \underline{y}\, A_B(\underline{x}, \underline{y}),$ w/ A_B a bounded formula.

Characterization Theorem

$$\mathrm{PA}^\omega_\trianglelefteq + \mathrm{MAJ}^\omega + \mathrm{mAC}^\omega_{\mathrm{bd}} + \mathrm{bC}^\omega_{\mathrm{bd}} \vdash A \leftrightarrow A^B\,.$$

Soundness of the interpretation

Theorem (Soundness)

Let Δ be a set of universal sentences (with bounded matrices). If

$$\mathrm{PA}^{\omega}_{\trianglelefteq} + \mathrm{MAJ}^{\omega} + \mathrm{mAC}^{\omega}_{\mathrm{bd}} + \mathrm{bC}^{\omega}_{\mathrm{bd}} + \Delta \vdash A,$$

then there are closed monotone terms $\underline{t}$ such that

$$\mathrm{PA}^{\omega}_{\trianglelefteq} + \Delta \vdash \tilde{\forall} \underline{x}\, \tilde{\exists} \underline{y} \trianglelefteq \underline{tx}\, A_B(\underline{x}, \underline{y}).$$

Soundness of the interpretation

Theorem (Soundness)

Let Δ be a set of universal sentences (with bounded matrices). If

$$\mathrm{PA}^{\omega}_{\trianglelefteq} + \mathrm{MAJ}^{\omega} + \mathrm{mAC}^{\omega}_{\mathrm{bd}} + \mathrm{bC}^{\omega}_{\mathrm{bd}} + \Delta \vdash A,$$

then there are closed monotone terms $\underline{t}$ such that

$$\mathrm{PA}^{\omega}_{\trianglelefteq} + \Delta \vdash \tilde{\forall} \underline{x}\, \tilde{\exists} \underline{y} \trianglelefteq \underline{tx}\, A_B(\underline{x}, \underline{y}).$$

Theorem (Extraction)

$$\mathrm{PA}^{\omega}_{\trianglelefteq} + \mathrm{MAJ}^{\omega} + \mathrm{mAC}^{\omega}_{\mathrm{bd}} + \mathrm{bC}^{\omega}_{\mathrm{bd}} + \Delta \vdash \forall x\, \exists y\, A_{\mathrm{bd}}(x, y)$$

$$\Rightarrow \mathrm{PA}^{\omega}_{\trianglelefteq} + \Delta \vdash \tilde{\forall} z\, \forall x \trianglelefteq z\, \exists y \trianglelefteq tz\, A_{\mathrm{bd}}(x, y)$$

Soundness of the interpretation

Theorem (Soundness)

Let Δ be a set of universal sentences (with bounded matrices). If

$$\mathrm{PA}^{\omega}_{\trianglelefteq} + \mathrm{MAJ}^{\omega} + \mathrm{mAC}^{\omega}_{\mathrm{bd}} + \mathrm{bC}^{\omega}_{\mathrm{bd}} + \Delta \vdash A,$$

then there are closed monotone terms $\underline{t}$ such that

$$\mathrm{PA}^{\omega}_{\leqslant^*} + \Delta \vdash \tilde{\forall} \underline{x}\, \tilde{\exists} \underline{y} \leqslant^* \underline{tx}\, A_B(\underline{x}, \underline{y}).$$

Theorem (Extraction)

$$\mathrm{PA}^{\omega}_{\trianglelefteq} + \mathrm{MAJ}^{\omega} + \mathrm{mAC}^{\omega}_{\mathrm{bd}} + \mathrm{bC}^{\omega}_{\mathrm{bd}} + \Delta \vdash \forall x\, \exists y\, A_{\mathrm{bd}}(x, y)$$

$$\Rightarrow \mathrm{PA}^{\omega}_{\leqslant^*} + \Delta \vdash \tilde{\forall} z\, \forall x \leqslant^* z\, \exists y \leqslant^* tz\, A_{\mathrm{bd}}(x, y)$$

Formal Theories

To apply this proof-theoretical technique is necessary to work with (semi-)formal proofs, which in general is not the case for usual mathematical theorems. We need to extend our formal setting...

- Finite types with base types 0 and X, denoted $\mathcal{T}^{\omega,X}$, are constructed in the usual way, where X is the type of objects in an abstract (metric, Banach, Hilbert, etc.) space.
- Extend the majorizability notion to $\mathcal{T}^{\omega,X}$ in an appropriate way.
- Add axioms characterizing the abstract space and all the required new constants.

We want that a soundness theorem still exists for the extended theory:

- New constants must be majorizable;
- Add moduli (of convergence, of Cauchyness, of asymptotic regularity, of metastability, etc.) witnessing problematic existential quantifiers ('computational gaps');
- Universal axiomatic (possible with bounded matrices and using the new moduli).

We want that a soundness theorem still exists for the extended theory:

- New constants must be majorizable;
- Add moduli (of convergence, of Cauchyness, of asymptotic regularity, of metastability, etc.) witnessing problematic existential quantifiers ('computational gaps');
- Universal axiomatic (possible with bounded matrices and using the new moduli).

Let $\mathrm{PA}^{\omega}_{\trianglelefteq}[X, \cdots]$ be one such theory. Then,

Soundness for extended theories

If $\mathrm{PA}^{\omega}_{\trianglelefteq}[X, \cdots] + \text{Principles}[X] \vdash A$,

then there are closed monotone terms $\underline{t}$ such that

$$\mathrm{PA}^{\omega}_{\trianglelefteq}[X, \cdots] \vdash \tilde{\forall}\underline{x}\, \tilde{\exists}\underline{y} \trianglelefteq \underline{tx}\, A_B(\underline{x}, \underline{y}).$$

What is Metastability?

Metastability

Let (x_n) be a sequence of real numbers.

- (x_n) satisfies the **Cauchy property** if

$$(\mathrm{I}) \quad \forall k \in \mathbb{N}\, \exists n \in \mathbb{N}\, \forall i, j \geq n \left(|x_i - x_j| \leq \frac{1}{k+1} \right)$$

Metastability

Let (x_n) be a sequence of real numbers.

- (x_n) satisfies the **Cauchy property** if

$$(\mathrm{I}) \quad \forall k \in \mathbb{N}\, \exists n \in \mathbb{N}\, \forall i, j \geqslant n \left(|x_i - x_j| \leqslant \frac{1}{k+1} \right)$$

- (x_n) satisfies the **metastability property** if

$$(\mathrm{II}) \quad \forall k \in \mathbb{N}\, \forall f \in \mathbb{N}^{\mathbb{N}}\, \exists n \in \mathbb{N}\, \forall i, j \in [n; f(n)] \left(|x_i - x_j| \leqslant \frac{1}{k+1} \right)$$

Metastability

Let (x_n) be a sequence of real numbers.

- (x_n) satisfies the **Cauchy property** if

$$\text{(I)} \quad \forall k \in \mathbb{N}\, \exists n \in \mathbb{N}\, \forall i, j \geqslant n \left(|x_i - x_j| \leqslant \frac{1}{k+1} \right)$$

- (x_n) satisfies the **metastability property** if

$$\text{(II)} \quad \forall k \in \mathbb{N}\, \forall f \in \mathbb{N}^{\mathbb{N}}\, \exists n \in \mathbb{N}\, \forall i, j \in [n; f(n)] \left(|x_i - x_j| \leqslant \frac{1}{k+1} \right)$$

(I) is equivalent to (II):

Clearly (I) $\rightarrow$ (II). The reverse direction, (II) $\rightarrow$ (I), is shown by contradiction: (II) states that there is no counterexample to (I).

The Cauchy (I) and the metastability (II) properties are equivalent, so... *Why look at* (II)*?*

The Cauchy (I) and the metastability (II) properties are equivalent, so... *Why look at (II)?*

- A Cauchy rate ϕ

$$\forall k \in \mathbb{N} \, \forall i, j \geqslant \phi(k) \; \left(|x_i - x_j| \leqslant \frac{1}{k+1} \right)$$

in general, is not computable (Specker sequences) and may be highly non-uniform.

The Cauchy (I) and the metastability (II) properties are equivalent, so... *Why look at* (II)*?*

- A Cauchy rate ϕ

$$\forall k \in \mathbb{N}\, \forall i,j \geqslant \phi(k) \left(|x_i - x_j| \leqslant \frac{1}{k+1} \right)$$

in general, is not computable (Specker sequences) and may be highly non-uniform.

- In many cases it is, instead, possible to extract an uniform computable metastability rate Φ

$$\forall k, f\, \exists n \leqslant \Phi(k,f)\, \forall i,j \in [n; f(n)] \left(|x_i - x_j| \leqslant \frac{1}{k+1} \right).$$

The Cauchy (I) and the metastability (II) properties are equivalent, so... *Why look at (II)?*

- A Cauchy rate ϕ

$$\forall k \in \mathbb{N} \forall i, j \geqslant \phi(k) \left(|x_i - x_j| \leqslant \frac{1}{k+1} \right)$$

in general, is not computable (Specker sequences) and may be highly non-uniform.

- In many cases it is, instead, possible to extract an uniform computable metastability rate Φ

$$\forall k, f \, \exists n \leqslant \Phi(k, f) \, \forall i, j \in [n; f(n)] \left(|x_i - x_j| \leqslant \frac{1}{k+1} \right).$$

A computable Φ does not entail a computable ϕ!

The Cauchy (I) and the metastability (II) properties are equivalent, so... *Why look at (II)?*

- A Cauchy rate ϕ

$$\forall k \in \mathbb{N} \forall i, j \geqslant \phi(k) \left(|x_i - x_j| \leqslant \frac{1}{k+1} \right)$$

in general, is not computable (Specker sequences) and may be highly non-uniform.

- In many cases it is, instead, possible to extract an uniform computable metastability rate Φ

$$\forall k, f \, \exists n \leqslant \Phi(k, f) \, \forall i, j \in [n; f(n)] \left(|x_i - x_j| \leqslant \frac{1}{k+1} \right).$$

A computable Φ does not entail a computable ϕ!
(The term **metastability** was coined by T.Tao in 2007 while studying the Mean Ergodic Theorem.)

An easy example

Infinite Convergence Principle

Every decreasing sequence of nonnegative real numbers is convergent.

An easy example

Infinite Convergence Principle

Every decreasing sequence of nonnegative real numbers is convergent.

We have the following metastability result for any such sequence:

Quantitative version (Kreisel, 1952)

Let (x_n) be a decreasing sequence of real numbers and $D \in \mathbb{N}$ be such that $\forall n \in \mathbb{N}\, (0 \leqslant x_n \leqslant D)$. Then

$$\forall k \in \mathbb{N}\, \forall f \in \mathbb{N}^{\mathbb{N}}\, \exists n \leqslant \Phi(k, f)\, \forall i, j \in [n; f(n)] \left(|x_i - x_j| \leqslant \frac{1}{k+1} \right),$$

where $\Phi(k, f) := \max\{f^{(i)}(0) : i < R\}$, with $R = D(k+1)$.

Proof:

Towards a contradiction, assume the result to be false. Then,

$n = 0$ fails:

$$x_0 - x_{f(0)} \geqslant x_{i_0} - x_{j_0} > \frac{1}{k+1}$$

Proof:

Towards a contradiction, assume the result to be false. Then,

$n = 0$ fails:

$$x_0 - x_{f(0)} \geqslant x_{i_0} - x_{j_0} > \frac{1}{k+1}$$

$n = f(0)$ fails:

$$x_{f(0)} - x_{f^{(2)}(0)} \geqslant x_{i_1} - x_{j_1} > \frac{1}{k+1}$$

$\ldots$

Proof:

Towards a contradiction, assume the result to be false. Then,

$n = 0$ fails:

$$x_0 - x_{f(0)} \geqslant x_{i_0} - x_{j_0} > \frac{1}{k+1}$$

$n = f(0)$ fails:

$$x_{f(0)} - x_{f^{(2)}(0)} \geqslant x_{i_1} - x_{j_1} > \frac{1}{k+1}$$

$\dots$

$n = f^{(R-1)}(0)$ fails:

$$x_{f^{(R-1)}(0)} - x_{f^{(R)}(0)} \geqslant x_{i_R} - x_{j_R} > \frac{1}{k+1}$$

Proof:

Towards a contradiction, assume the result to be false. Then,

$n = 0$ fails:

$$x_0 - x_{f(0)} \geqslant x_{i_0} - x_{j_0} > \frac{1}{k+1}$$

$n = f(0)$ fails:

$$x_{f(0)} - x_{f^{(2)}(0)} \geqslant x_{i_1} - x_{j_1} > \frac{1}{k+1}$$

...

$n = f^{(R-1)}(0)$ fails:

$$x_{f^{(R-1)}(0)} - x_{f^{(R)}(0)} \geqslant x_{i_R} - x_{j_R} > \frac{1}{k+1}$$

Hence,

$$x_0 \geqslant x_0 - x_{f^{(R)}(0)} > \tfrac{R}{k+1} = D,$$

which gives the contradiction. □

Unwinding mathematical proofs

Proof Mining

G.Kreisel (1951) was the first to formulate the program of **unwinding proofs** under the general question:

> *"What more do we know if we have proved a theorem by restricted means than if we merely know that it is true?"*

By suggestion of D. Scott, "unwinding proofs" evolved into the more appealing term "**proof mining**".

Goals of proof mining

The main idea is to analyse an ineffective mathematical proof in order to obtain additional information:

- effective bounds, algorithms (rates of convergence, of metastability, of asymptotic regularity, ...);
- results of independence of certain parameters;
- generalization of the proof by weakening of premises.

The good choices for study

The quality of these applications of proof theory seems to rest on two distinct aspects:

1st The chosen result must be **of interest** to the community with its finitary information wanted;

2nd The extracted information must be of a **simple** nature if not new

The good choices for study

The quality of these applications of proof theory seems to rest on two distinct aspects:

1st The chosen result must be **of interest** to the community with its finitary information wanted;

2nd The extracted information must be of a **simple** nature if not new

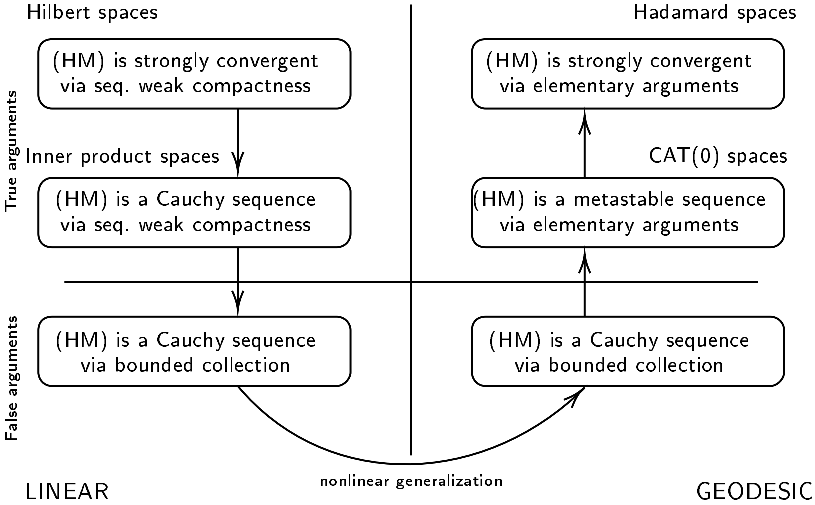
- The analysis of arithmetical comprehension (lurking in common place mathematical arguments, e.g. compactness principles) would require the use of Spector's bar-recursive functionals.
- However, that goes against the goal of "simple information" and would not be appreciated by the general mathematician.
- In most cases the use of such comprehension principles can actually be avoided: it may happen via an 'arithmetization' of the argument, ε-weakening, or by other simplifications to the proof.

Removal by False principles

- In [1], a macro was developed in which certain sequential weak compactness arguments (arithmetical comprehension) were bypassed by instead relying on a (set-theoretically false) bounded collection argument.
- Moreover, the bounded collection argument is computationally tame, in the sense that it does not contribute to an increase in the complexity of the final finitary information.
- This perspective was applied in the study of strong convergence for several Halpern-type iterations and, recently, in the study of the convergence of Dykstra's algorithm (which follows a completely different proof strategy).

[1] F.Ferreira, L.Leuştean, P.Pinto. On the removal of weak compactness arguments in proof mining. *Advances in Mathematics*, 354:106728, 55pp, 2019.

The alternating Halpern-Mann



[2] B.Dinis, P.Pinto. Strong convergence for the alternating Halpern-Mann iteration in CAT(0) spaces. *SIAM Journal on Opt.*, 33(2), 785-815, 2023.

Generalizations

- Proof mining provides a deeper understanding of the proof, stripping it to its essential arguments: **generalizations!**
- In the previous slide, we already saw an example of a generalization from inner product spaces to CAT(0) spaces.

Generalizations

- Proof mining provides a deeper understanding of the proof, stripping it to its essential arguments: **generalizations!**
- In the previous slide, we already saw an example of a generalization from inner product spaces to CAT(0) spaces.
- Successful in generalizations from a linear to nonlinear setting.
  - "Lion-Man" game – weakening of compactness assumption;[2]
  - Suzuki's theorem reducing the convergence of a generalized iterative schema to that of its original version;[3]
  - Abstract versions of proximal algorithm in CAT(0);[4]

[2] U.Kohlenbach, G.López-Acedo, and A.Nicolae. A uniform betweenness property in metric spaces and its role in the quantitative analysis of the "Lion-Man" game. Pacific J. Math., 310(1):181–212, 2021.

[3] U.Kohlenbach, and P.Pinto. Quantitative translations for viscosity approximation methods in hyperbolic spaces. J. Math. Anal. Appl., 507, 2022.

[4] A.Sipoş. Abstract strongly convergent variants of the proximal point algorithm. Comput. Optim. Appl., 83(1):349–380, 2022.

Nonlinear spaces

Let us briefly recall certain settings of geodesic spaces:

$$\begin{aligned} \text{W-hyperbolic spaces} &\Rightarrow \text{normed spaces} \\ \text{UCW-hyperbolic spaces} &\Rightarrow \text{uniformly convex normed spaces} \\ CAT(0)\text{spaces} &\Rightarrow \text{inner product spaces} \end{aligned}$$

Nonlinear spaces

Let us briefly recall certain settings of geodesic spaces:

$$\begin{aligned} \text{W-hyperbolic spaces} &\Rightarrow \text{normed spaces} \\ \text{UCW-hyperbolic spaces} &\Rightarrow \text{uniformly convex normed spaces} \\ CAT(0)\text{spaces} &\Rightarrow \text{inner product spaces} \end{aligned}$$

- Several results that hold in Hilbert spaces, still hold in a more general setting of (uniformly) **smooth normed spaces** where ‘inner product’-like arguments are still available. In this instance, one assumes some additional conditions on the norm which are more general than assuming it to arise from an inner-product.
- Despite the relevance of these spaces, no geodesic counterpart existed in the literature.

Smooth Hyperbolic spaces

In [5], the notion of nonlinear smooth space was introduced as a space (X, d, W, π) satisfying:

(P1) $\pi(\overrightarrow{xy}, \overrightarrow{xy}) = d^2(x, y)$

(P2) $\pi(\overrightarrow{xy}, \overrightarrow{uv}) = -\pi(\overrightarrow{yx}, \overrightarrow{uv}) = -\pi(\overrightarrow{xy}, \overrightarrow{vu})$

(P3) $\pi(\overrightarrow{xy}, \overrightarrow{uv}) + \pi(\overrightarrow{yz}, \overrightarrow{uv}) = \pi(\overrightarrow{xz}, \overrightarrow{uv})$

(P4) $\pi(\overrightarrow{xy}, \overrightarrow{uv}) \leqslant d(x, y)d(u, v)$

(P5) $d^2(W(x, y, \lambda), z) \leqslant (1-\lambda)^2 d^2(x, z) + 2\lambda\pi(\overrightarrow{yz}, \overrightarrow{W(x, y, \lambda)z})$,

where $\pi : X \times X \to \mathbb{R}$ and $\overrightarrow{xy}$ denotes the pair $(x, y) \in X \times X$.
The function π is a nonlinear analogue of the normalized duality map in the normed setting.

[5] P.Pinto. Nonexpansive maps in nonlinear smooth spaces. To appear in: *Transactions of the American Mathematical Society*, 48pp, 2024.

Smooth Hyperbolic spaces

In [5], the notion of nonlinear smooth space was introduced as a space (X, d, W, π) satisfying:

(P1) $\pi(\overrightarrow{xy}, \overrightarrow{xy}) = d^2(x, y)$

(P2) $\pi(\overrightarrow{xy}, \overrightarrow{uv}) = -\pi(\overrightarrow{yx}, \overrightarrow{uv}) = -\pi(\overrightarrow{xy}, \overrightarrow{vu})$

(P3) $\pi(\overrightarrow{xy}, \overrightarrow{uv}) + \pi(\overrightarrow{yz}, \overrightarrow{uv}) = \pi(\overrightarrow{xz}, \overrightarrow{uv})$

(P4) $\pi(\overrightarrow{xy}, \overrightarrow{uv}) \leqslant d(x, y)d(u, v)$

(P5) $d^2(W(x, y, \lambda), z) \leqslant (1-\lambda)^2 d^2(x, z) + 2\lambda\pi(\overrightarrow{yz}, \overrightarrow{W(x, y, \lambda)z})$,

where $\pi : X \times X \to \mathbb{R}$ and $\overrightarrow{xy}$ denotes the pair $(x, y) \in X \times X$. The function π is a nonlinear analogue of the normalized duality map in the normed setting.

- In [5], it was shown that this notion extends both CAT(0) spaces as well as smooth normed spaces, providing an unifying framework for several important results in functional analysis.

[5] P.Pinto. Nonexpansive maps in nonlinear smooth spaces. To appear in: *Transactions of the American Mathematical Society*, 48pp, 2024.

Theorem 6.6. *Let X be a uniformly smooth hyperbolic space with ω_X a modulus of uniform continuity for π. Assume that (z_m) is a Cauchy sequence with rate of metastability ξ, and let (x_n) be generated by ($\mathrm{H}_{\mathrm{ppa}}$). Then, for all $\varepsilon > 0$ and $f \in \mathbb{N}^{\mathbb{N}}$,*

$$\exists n \leq \Omega\ \exists w \in C\ \forall i \in [n; n + f(n)] \left(d(w, T_i(w)) \leq \frac{\varepsilon}{2} \wedge d(x_i, w) \leq \frac{\varepsilon}{2} \right),$$

with $\Omega := \Omega(\varepsilon, f, \sigma_1, \sigma_2, \widetilde{\alpha}, b, \mu, \Delta, \xi, \omega_X) := \hat{\chi}(\theta^M(\hat{\xi}))$, where $\hat{\xi} := \tilde{\xi}(\varepsilon_0, f_0, N_0)$ as per the construction in Lemma 2.2,

$$\varepsilon_0 := \min\left\{ \frac{\tilde{\varepsilon}}{2}, \omega_X\left(b, \frac{\tilde{\varepsilon}}{2}\right) \right\},\ f_0(k) := \left\lceil \frac{b}{\delta_1(k)} \right\rceil,\ N_0 := \left\lfloor \frac{3b}{2\tilde{\varepsilon}} \right\rfloor,\ \tilde{\varepsilon} := \frac{\varepsilon^2}{48b},$$

and, taking χ from Lemma 2.6 and writing g^M for $g^M(k) := \max\{g(k') : k' \leq k\}$,

$$\delta_1(k) := \frac{\min\left\{ \frac{\varepsilon}{2}, \Delta\left(b, \frac{\eta_k}{\mu(0)}\right), \Delta\left(b, \frac{\omega_X(b,\tilde{\varepsilon})}{2}\right), 3\widetilde{\alpha}(K(k)) \cdot \tilde{\varepsilon}, \frac{2\tilde{\varepsilon}}{K(k)} \right\}}{\mu(K(k))},$$

$$\eta_k := \frac{\tilde{\varepsilon}}{3(k+1)},\ K(k) := \max\{k' + f_\chi(k') : k' \leq \theta(k)\},$$

$$f_\chi(k) \underset{10}{:=} \hat{\chi}(k) - k + f^M(\hat{\chi}(k)) + 2,\ \hat{\chi}(k) := \chi\left[\sigma_2, b^2\right]\left(\frac{\varepsilon^2}{4}, k\right),$$

and also, with ψ as in Lemma 6.4,

$$\theta(k) := \psi(\varepsilon_1(k), f_\chi, N_1(k), b) := f_\chi^{+\left(\left\lceil \frac{b}{\varepsilon_1(k)} \right\rceil\right)}(N_1(k))$$

$$\varepsilon_1(k) := \frac{1}{2}\Delta\left(b, \frac{\eta_k}{\mu(0)}\right),\ N_1(k) := \sigma_1\left(\frac{\delta_2(k)}{b}\right),$$

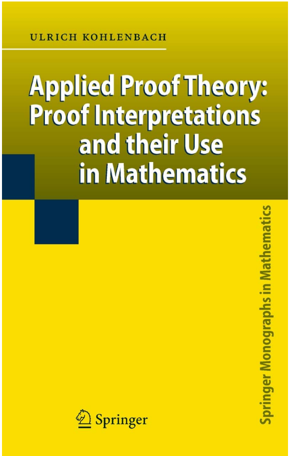
$$\delta_2(k) := \min\left\{ \varepsilon_1(k), \Delta\left(b, \frac{\omega_X(b,\tilde{\varepsilon})}{2}\right), \frac{\omega_X(b,\tilde{\varepsilon})}{2} \right\}.$$

In particular, (x_n) is a Cauchy sequence with rate of metastability Ω.

... which, by easy ('elementary') mathematical arguments, entails the following infinitary result:

Corollary 6.7. *Let X be a complete uniformly smooth UCW hyperbolic space, C a nonempty closed convex subset of X, and $\{T_n\}$ a resolvent-like family of nonexpansive maps on C. For given $x_0, u \in C$, if (x_n) is generated by $(\mathrm{H}_{\mathrm{ppa}})$ with $\{T_n\}$ and a sequence $(\alpha_n) \subseteq (0,1]$ satisfying $\lim \alpha_n = 0$ and $\sum \alpha_n = \infty$, then (x_n) converges towards $Q(u)$, where Q is the sunny nonexpansive retraction of C onto $\mathrm{Fix}(\{T_n\})$.*

The book



U.Kohlenbach. Applied Proof Theory: Proof Interpretations and their Use in Mathematics. Springer Science & Business Media, 2008.

Other selected sources

- U. Kohlenbach. Proof-theoretic Methods in Nonlinear Analysis. In B. Sirakov, P.N. de Souza, and M. Viana, editors, *Proceedings of the International Congress of Mathematicians 2018*, volume 2, pages 62–82. World Scientific, 2019.
- The Proof Theory Blog,
  'What proof mining is about" by Andrei Sipoș:
  https://prooftheory.blog/
- The Proof Mining Bibliography by Nicholas Pischke:
  https://sites.google.com/view/nicholaspischke/
- Tutorial by Andrei Sipoș at Logic Colloquium 2024:
  notes available in his homepage.
- My homepage:
  https://www2.mathematik.tu-darmstadt.de/~pinto/

Thank you