A new take on proof mining

Fernando Ferreira

Universidade de Lisboa

12th Panhellenic Logic Symposium

Anogeia, Crete, Greece, June 26-30, 2019

U LISBOA | UNIVERSIDADE DE LISBOA

Quantitative versions: metastability

$$\forall k \in \mathbb{N}\, \exists n \in \mathbb{N}\, \forall m \in \mathbb{N}\, \forall i, j \in [n, n+m]\ \left(\|u_i - u_j\| < \frac{1}{k+1} \right)$$

It is *not possible* to get a computable bound for n in terms of k.

One considers instead the *metastable* version of Cauchyness:

$$\forall k \in \mathbb{N} \forall f \in^{\mathbb{N}} \mathbb{N}\, \exists n \in \mathbb{N}\, \forall i, j \in [n, n+f(n)]\ \left(\|u_i - u_j\| < \frac{1}{k+1} \right)$$

To get a computable rate of metastability $\Phi : \mathbb{N} \times^{\mathbb{N}} \mathbb{N} \mapsto \mathbb{N}$:

$$\forall k, f\, \exists n \leq \Phi(k, f)\, \forall i, j \in [n, n+f(n)]\ \left(\|u_i - u_j\| < \frac{1}{k+1} \right)$$

Browder's fixed point theorem

Definition

Let X be a real Hilbert space. We call $U : X \to X$ a *non-expansive mapping* if, for all $x, y \in X$, $\|U(x) - U(y)\| \leq \|x - y\|$.

Theorem (Browder, 1967)

Let X be a real Hilbert space and $U : X \to X$ a non-expansive mapping. Assume that C is a closed convex subset of X, that $0 \in C$, and that U maps C into C.
For each natural number n, let $U_n : X \to X$ be the strict contraction defined by $U_n(x) = (1 - \frac{1}{n+1})U(x)$ and consider u_n the unique fixed point of U_n.
Then the sequence $(u_n)_{n \in \mathbb{N}}$ converges strongly to a fixed point $u \in C$ of U.

Take a peek at the bound

For f monotone:

$$\Phi(k, f) := 12b^2 \left(h^{(R)}(0) + 1\right)^2 + b$$

- b is a majorant of the diameter of C
- $h(m) := 1 + \max\{8b(f(12b^2(m+1)^2 + b) + 1)(k+1)^2, 12b(m+1)^2\}$
- $R := 64b^4(k+1)^4 + b^2$

Uniformity of the bounds: the bound does not depend on the Hilbert space X, nor on the non-expansive mapping U and only depends on the convex set C insofar as a majorant of its diameter appears in the bound.

Quantitative versions: the projection argument

$$\exists x \in C \ \big(U(x) = x \wedge \forall y \in C \, \big(U(y) = y \to \|x\| \ \leq \|y\| \ \big)\big)$$

$$\forall k \, \exists x \in C \ \left(U(x) = x \wedge \forall y \in C \left(U(y) = y \to \|x\| \ < \|y\| \ + \frac{1}{k+1}\right)\right)$$

Quantitative versions: the projection argument

$$\exists x \in C \ \big(U(x) = x \wedge \forall y \in C \, \big(U(y) = y \to \|x\|^2 \leq \|y\|^2\big)\big)$$

$$\forall k \, \exists x \in C \ \left(U(x) = x \wedge \forall y \in C \left(U(y) = y \to \|x\|^2 < \|y\|^2 + \frac{1}{k+1}\right)\right)$$

Quantitative versions: the projection argument

$$\exists x \in C \ \big(U(x) = x \wedge \forall y \in C \, \big(U(y) = y \to \|x\|^2 \leq \|y\|^2\big)\big)$$

$$\forall k \, \exists x \in C \ \left(U(x) = x \wedge \forall y \in C \left(U(y) = y \to \|x\|^2 < \|y\|^2 + \frac{1}{k+1}\right)\right)$$

For all $k \in \mathbb{N}$ and all $f : \mathbb{N} \to \mathbb{N}$ monotone, there exists $n \in \mathbb{N}$ and $x \in C$ such that

$$\|U(x) - x\| < \frac{1}{f(n)+1} \quad \text{and}$$

$$\forall y \in C \left(\|U(y) - y\| \leq \frac{1}{n+1} \ \to \ \|x\|^2 < \|y\|^2 + \frac{1}{k+1}\right)$$

Quantitative versions: the projection argument

$$\exists x \in C \ \big(U(x) = x \wedge \forall y \in C \, \big(U(y) = y \to \|x\|^2 \leq \|y\|^2\big)\big)$$

$$\forall k \, \exists x \in C \ \left(U(x) = x \wedge \forall y \in C \left(U(y) = y \to \|x\|^2 < \|y\|^2 + \frac{1}{k+1}\right)\right)$$

For all $k \in \mathbb{N}$ and all $f : \mathbb{N} \to \mathbb{N}$ monotone, there exists $n \in \mathbb{N}$ and $x \in C$ such that

$$\|U(x) - x\| < \frac{1}{f(n)+1} \quad \text{and}$$

$$\forall y \in C \left(\|U(y) - y\| \leq \frac{1}{n+1} \ \to \ \|x\|^2 < \|y\|^2 + \frac{1}{k+1}\right)$$

Mining: can take $n \leq (f+1)^{(r)}(0)$, with $r = b^2(k+1)$.

Nilpotency

R is a nonzero commutative ring with identity.

Definition

An element $e \in R$ is called *nilpotent* if there is a natural number n such that $e^n = 0$

Theorem

An element $e \in R$ is nilpotent if, and only if, e lies in every prime ideal of R.

Nilpotency

R is a nonzero commutative ring with identity.

Definition

An element $e \in R$ is called *nilpotent* if there is a natural number n such that $e^n = 0$

Theorem

An element $e \in R$ is nilpotent if, and only if, e lies in every prime ideal of R.

Definition

Let $f, g \in {}^{\mathbb{N}}R$. An (f, g)-prime ideal of R is a (proper) ideal X of R such that

$$\forall k \in \mathbb{N}\,(f(k)g(k) \in X \rightarrow f(k) \in X \vee g(k) \in X).$$

Quantitative versions: nilpotency

$$\forall n\,(e^n \neq 0) \to \exists X(X \text{ is an } (f,g)\text{-prime ideal of } R \text{ and } e \notin X)$$

Definition

Given a natural number ℓ, an (f,g)-prime ideal of R up to ℓ is a (proper) ideal X of R such that

$$\forall k \leq \ell\,(f(k)g(k) \in X \to f(k) \in X \vee g(k) \in X).$$

For all $\ell \in \mathbb{N}$, there exists $n \in \mathbb{N}$ such that, for all $e \in R$ and $f, g \in {}^{\mathbb{N}}R$,

$$e^n \neq 0 \to \exists X(X \text{ is an } (f,g)\text{-prime ideal of } R \text{ up to } \ell \text{ and } e \notin X)$$

Quantitative versions: nilpotency

$$\forall n\,(e^n \neq 0) \to \exists X(X \text{ is an } (f,g)\text{-prime ideal of } R \text{ and } e \notin X)$$

Definition

Given a natural number ℓ, an (f,g)-prime ideal of R up to ℓ is a (proper) ideal X of R such that

$$\forall k \leq \ell\,(f(k)g(k) \in X \to f(k) \in X \vee g(k) \in X).$$

For all $\ell \in \mathbb{N}$, there exists $n \in \mathbb{N}$ such that, for all $e \in R$ and $f, g \in {}^{\mathbb{N}}R$,

$$e^n \neq 0 \to \exists X(X \text{ is an } (f,g)\text{-prime ideal of } R \text{ up to } \ell \text{ and } e \notin X)$$

Can take $n := 2^\ell$.

An application

Theorem

Let $P(Z) = \sum_{i=0}^{n} a_i Z^i$ *and* $Q(Z) = \sum_{j=0}^{k} b_j Z^j$ *be polynomials of* $R[Z]$ *such that* $P(Z)Q(Z) = 1$. *Then, for each* $1 \leq i \leq n$, a_i *is nilpotent.*

Proof.

It is enough to show that each a_i $(1 \leq i \leq n)$ is in every prime ideal X of R. Of course, the equation $P(Z)Q(Z) = 1$ also holds in the cocient ring R/X. Since this cocient ring is an integral domain, we may conclude that both $P(Z)$ and $Q(Z)$ have degree zero over the ring R/X. Therefore, for each $1 \leq i \leq n$, $a_i \in X$. □

An application

Theorem

Let $P(Z) = \sum_{i=0}^{n} a_i Z^i$ *and* $Q(Z) = \sum_{j=0}^{k} b_j Z^j$ *be polynomials of* $R[Z]$ *such that* $P(Z)Q(Z) = 1$. *Then, for each* $1 \leq i \leq n$, a_i *is nilpotent.*

Proof.

It is enough to show that each a_i $(1 \leq i \leq n)$ is in every prime ideal X of R. Of course, the equation $P(Z)Q(Z) = 1$ also holds in the cocient ring R/X. Since this cocient ring is an integral domain, we may conclude that both $P(Z)$ and $Q(Z)$ have degree zero over the ring R/X. Therefore, for each $1 \leq i \leq n$, $a_i \in X$. □

Mining: the index of nilpotency of a_i is bounded by $2^{(n-i+1)(k+1)}$.

Forms of compactness: the closed unit interval

Sequential compactness: every sequence of elements in $[0,1]$ has a convergent subsequence.

Heine/Borel compactness: every open covering of $[0,1]$ has a finite subcovering.

$$\forall x \in [0,1]\, \exists n\, (x \in \Omega_n) \to \exists n\, \forall x \in [0,1]\, \exists k \leq n\, (x \in \Omega_k)$$

$$\forall n\, \exists x \in [0,1]\, \forall k \leq n\, (x \notin \Omega_k) \to \exists x \in [0,1]\, \forall n\, (x \notin \Omega_n)$$

The first formulation is of FAN type. The second is of WKL type.

Forms of compactness: weak and strong convergence

Let X be a Hilbert space, $(u_n)_{n\in\mathbb{N}}$ a sequence of elements of X and $u \in X$.

We say that (u_n) converges *strongly* to u if $\lim_n \|u_n - u\| = 0$.

We say that (u_n) converges *weakly* to u if, for all $w \in X$,

$$\lim_n \langle u_n, w\rangle = \langle u, w\rangle$$

In an infinite dimensional Hilbert space, the closed unit ball is never strongly compact.

Forms of compactness: a conservation result

Theorem

Let C be a closed bounded convex subset of X. Every sequence of elements in C has a subsequence that converges weakly (to a point in C).

What about Heine/Borel compactness (for the strong topology)?

$$\forall x \in C\, \exists n\, (x \in \Omega_n) \to \exists n\, \forall x \in C\, \exists k \leq n\, (x \in \Omega_k)$$

Within certain formal theories, the use of the above principle can be *removed* from proofs of quantitative statements. This is a conservation result.

From the point of view of the *bounded functional interpretation*, the explanatory root of the above result is the same as Harvey Friedman's conservation result of WKL_0 over RCA_0.

Three technical facts (of the proof of Browder's theorem)

(I)

$$\forall n \left(\|U(u_n) - u_n\| \leq \frac{b}{n+1} \right)$$

(II)

$$\forall k \exists u \in C \left(U(u) = u \wedge \forall v \in C \left(U(v) = v \rightarrow \langle u, u - v \rangle < \frac{1}{k+1} \right) \right)$$

(III)

$$\forall n \forall u \in C \left(U(u) = u \rightarrow \|u_n - u\|^2 \leq \langle u, u - u_n \rangle \right)$$

We need to prove that $(u_n)_n$ is a Cauchy sequence.

Setting up the argument

Fix $k \in \mathbb{N}$.

By (II), take $\tilde{u} \in C$ such that $U(\tilde{u}) = \tilde{u}$ and

$$\forall v \in C \left(U(v) = v \to \langle \tilde{u}, \tilde{u} - v \rangle < \frac{1}{k+1} \right)$$

By (III), it is enough to show that

$$\exists n \forall i \geq n \left(\langle \tilde{u}, \tilde{u} - u_i \rangle < \frac{1}{k+1} \right)$$

The sequential weak compactness argument

Assume not.

Then

$$\forall n \, \exists i \geq n \left(\langle \tilde{u}, \tilde{u} - u_i \rangle \geq \frac{1}{k+1} \right)$$

Take (v_n) a subsequence of (u_n) such that

$$\forall n \left(\langle \tilde{u}, \tilde{u} - v_n \rangle \geq \frac{1}{k+1} \right)$$

At this point, we invoke a sequential weak compactness argument. Take (w_n) a subsequence of (v_n) weakly converging to a certain point $w \in C$. Using (I), Browder showed that $U(w) = w$. By weak convergence, we get $\langle \tilde{u}, \tilde{u} - w \rangle \geq \frac{1}{k+1}$. This is a contradiction.

The Heine/Borel argument

We have:

$$\forall v \in C \left(\forall m \in \mathbb{N} \left(\|U(v) - v\| \leq \frac{1}{m+1} \right) \rightarrow \langle \tilde{u}, \tilde{u} - v \rangle < \frac{1}{k+1} \right).$$

Hence, $C \subseteq \bigcup_m \Omega_m$, where

$$\Omega_m := \left\{ v \in X : \|U(v) - v\| > \frac{1}{m+1} \right\} \cup \left\{ v \in X : \langle \tilde{u}, \tilde{u} - v \rangle < \frac{1}{k+1} \right\}.$$

By Heine/Borel compactness, there is $\ell \in \mathbb{N}$ such that $C \subseteq \Omega_\ell$. Therefore

$$\forall v \in C \left(\|U(v) - v\| \leq \frac{1}{\ell+1} \rightarrow \langle \tilde{u}, \tilde{u} - v \rangle < \frac{1}{k+1} \right).$$

Using (I), the result follows.

Collection principles

$$\forall^{\mathrm{b}} x\, \exists n\, A_{\mathrm{b}}(x, n) \to \exists n \forall^{\mathrm{b}} x\, \exists k \leq n\, A_{\mathrm{b}}(x, k)$$

where $\forall^{\mathrm{b}} x$ is a bounded quantifier and A_{b} is a bounded formula.

- In the case of Browder's theorem: $\exists^{\mathrm{b}} x$ is $\exists x \in C$.
- In the case of weak König's lemma: $\exists^{\mathrm{b}} x$ is $\exists x \in {}^{\mathbb{N}}2$.
- In the case of nilpotency: $\exists^{\mathrm{b}} x$ is $\exists X \in {}^{R}2$.

Extended weak König's principle (introduction of *ideal elements*):

$$\forall n\, \exists^{\mathrm{b}} x\, \forall k \leq n\, A_{\mathrm{b}}(x, k) \to \exists^{\mathrm{b}} x\, \forall n\, A_{\mathrm{b}}(x, n)$$

A macro of metatheorems

Macro of metatheorems

Suppose that $\mathcal{T}^+ \vdash A$, *where* A *is in* quantitative form, *then* $\mathcal{T} \vdash A$.

Quantitative forms include

$$\forall k \in \mathbb{N} \forall f \in^{\mathbb{N}} \mathbb{N} \exists n \in \mathbb{N}\, A_{\mathrm{b}}(k, \tilde{f}, n),$$

where $\tilde{f}(m) = \max_{i \leq m} f(i)$.

The metatheorems also guarantee the existence of a computable functional $\phi : \mathbb{N} \times^{\mathbb{N}} \mathbb{N} \mapsto \mathbb{N}$ such that

$$\mathcal{T} \vdash \forall k \in \mathbb{N} \forall f \in^{\mathbb{N}} \mathbb{N} \exists n \leq \phi(k, f)\, A_{\mathrm{b}}(k, \tilde{f}, n)$$

Quantitative versions: nilpotency again

$$\forall e, f, g\,[\forall n\,(e^n \neq 0) \to \exists X(X \text{ is an } (f,g)\text{-prime ideal of } R \text{ and } e \notin X)]$$

$$\forall e, f, g\,[\forall n\,(e^n \neq 0) \to \exists X \forall \ell(X \text{ is an } (f,g)\text{-prime ideal of } R \text{ up to } \ell \text{ and } e \notin X)]$$

$$\forall e, f, g\,[\forall n\,(e^n \neq 0) \to \forall \ell \exists X(X \text{ is an } (f,g)\text{-prime ideal of } R \text{ up to } \ell \text{ and } e \notin X)]$$

$$\forall \ell \forall e, f, g \exists n\,[(e^n \neq 0) \to \exists X(X \text{ is an } (f,g)\text{-prime ideal of } R \text{ up to } \ell \text{ and } e \notin X)]$$

$$\forall \ell \exists n\,[\forall e, f, g\,((e^n \neq 0) \to \exists X(X \text{ is an } (f,g)\text{-prime ideal of } R \text{ up to } \ell \text{ and } e \notin X))]$$

Quantitative versions: the projection argument again

$$\forall k \exists x \in C \left[U(x) = x \wedge \forall y \in C \left(U(y) = y \to \|x - v_0\|^2 < \|y - v_0\|^2 + \frac{1}{k+1} \right) \right]$$

$$\forall k \exists x \in C \left[U(x) = x \wedge \forall y \in C \left(\forall n \left(\|U(y) - y\| \leq \frac{1}{n+1} \right) \to \|x - v_0\|^2 < \|y - v_0\|^2 + \frac{1}{k+1} \right) \right]$$

$$\forall k \exists x \in C \left(U(x) = x \wedge \forall y \in C \, \exists n \left(\|U(y) - y\| \leq \frac{1}{n+1} \to \|x - v_0\|^2 < \|y - v_0\|^2 + \frac{1}{k+1} \right) \right)$$

$$\forall k \exists x \in C \left(U(x) = x \wedge \exists n \forall y \in C \left(\|U(y) - y\| \leq \frac{1}{n+1} \to \|x - v_0\|^2 < \|y - v_0\|^2 + \frac{1}{k+1} \right) \right)$$

$$\forall k \exists x \in C \exists n \left(U(x) = x \wedge \forall y \in C \left(\|U(y) - y\| \leq \frac{1}{n+1} \to \|x - v_0\|^2 < \|y - v_0\|^2 + \frac{1}{k+1} \right) \right)$$

$$\forall k \exists n \exists x \in C \forall m \left(\|U(x) - x\| \leq \frac{1}{m+1} \wedge \forall y \in C \left(\|U(y) - y\| < \frac{1}{n+1} \to \|x - v_0\|^2 \leq \|y - v_0\|^2 + \frac{1}{k+1} \right) \right)$$

$$\forall k \exists n \forall m \exists x \in C \left(\|U(x) - x\| \leq \frac{1}{m+1} \wedge \forall y \in C \left(\|U(y) - y\| < \frac{1}{n+1} \to \|x - v_0\|^2 \leq \|y - v_0\|^2 + \frac{1}{k+1} \right) \right)$$

$$\forall k \forall f \exists n \, \exists x \in C \left(\|U(x) - x\| \leq \frac{1}{\tilde{f}(n)+1} \wedge \forall y \in C \left(\|U(y) - y\| < \frac{1}{n+1} \to \|x - v_0\|^2 \leq \|y - v_0\|^2 + \frac{1}{k+1} \right) \right)$$

$$\forall k \forall f \exists n \, \exists x \in C \left(\|U(x) - x\| < \frac{1}{\tilde{f}(n)+1} \wedge \forall y \in C \left(\|U(y) - y\| \leq \frac{1}{n+1} \to \|x - v_0\|^2 < \|y - v_0\|^2 + \frac{1}{k+1} \right) \right)$$

References on Browder and nilpotency

F. E. Browder, "Convergence of approximants to fixed points of nonexpansive nonlinear mappings in Banach spaces". *Archive for Rational Mechanics and Analysis*, 24:82-90, 1967.

U. Kohlenbach, "On quantitative versions of theorems due to F. E. Browder and R. Wittmann." *Advances in Mathematics*, 226:2764-2795, 2011.

F. Ferreira, L. Leustean & P. Pinto, "On the removal of weak compactness arguments in proof mining." Accepted for publication in *Advances in Mathematics*.

F. Ferreira, "Bounds for indexes of nilpotency in commutative ring theory: a proof mining approach" (submitted for publication).

Monotone and bounded functional interpretations

U. Kohlenbach, "Analysing proofs in analysis." In W. Hodges *et al.* (editors), *Logic: from Foundations to Applications*, pp. 225-260. Oxford University Press, 1996.

U. Kohlenbach, *Applied Proof Theory: Proof Interpretations and their Use in Mathematics*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2008.

F. Ferreira & P. Oliva, "Bounded functional interpretation." Annals of Pure and Applied Logic, 135:73-112, 2005.

P. Engrácia, *Proof-theoretic studies on the bounded functional interpretation*. PhD dissertation, Universidade de Lisboa, 2009.

Thank you