Proof Mining

Lecture 1: Identifying Incomplete Statements

Paulo Oliva
Queen Mary University of London

Proof Society - Summer School

Swansea, 8-11 September 2019

Plan

Lecture 1: **Incomplete Statements**

Lecture 2: Proof Translations

Lecture 3: Proof Interpretations

Today

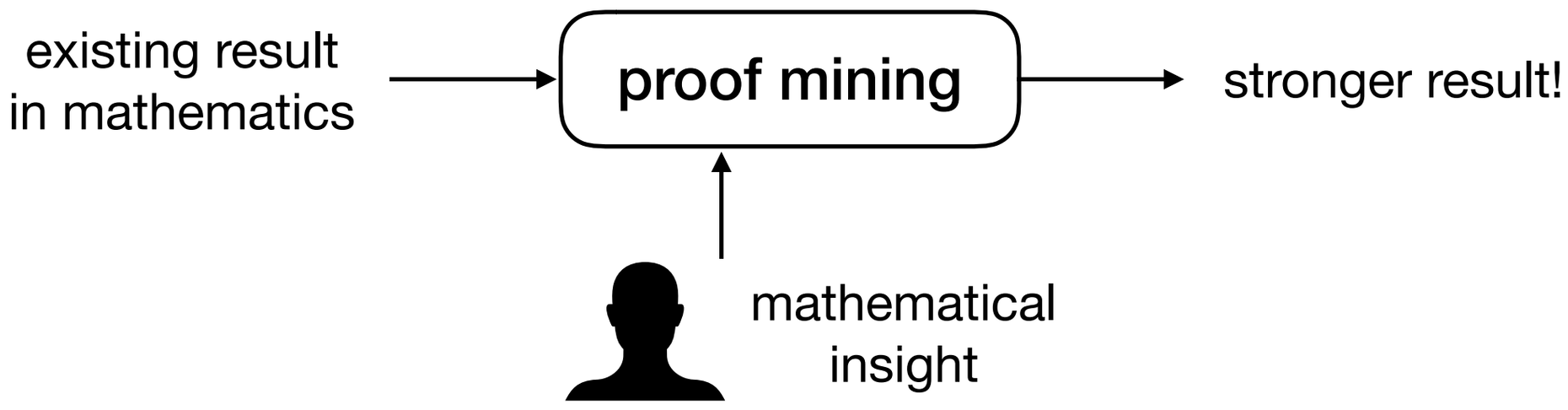
- Proof mining
- Formal language
- Complete vs incomplete statements
- Lots of examples!

Proof Mining

Proof Mining

research program to obtain extra information from (nonconstructive) mathematical proofs

- Originated with Kreisel's applications of his "no-counterexample interpretation"
- Resurgence in 1990s with Kohlenbach's application of his monotone functional interpretation



Proof Mining

some success stories...

- [1993] Chebyshev approximation of functions by polynomials
- [2001] L_1 approximation of functions by polynomials
- [2001-3] Krasnoselski fixed point theorem
  (nonexpansive maps on normed and hyperbolic spaces)
- [2009] Mean ergodic theorem for Banach spaces
- [2011] Browder/Wittmann fixed point theorems
  (nonexpansive maps on Hilbert spaces)
- [2012-6] Generalisations for CAT(0) and CAT(k) spaces
- [2019] Generalisations for smooth/convex Banach spaces

Formal Language

Atomic formulas

$\bot$ (contradiction)

$n \in \mathbb{N}$, $x \in \mathbb{R}$,...

$n =_{\mathbb{N}} m$, $n \leq_{\mathbb{N}} m$,...

Connectives

$A \wedge B$ (A and B)

$A \vee B$ (A or B)

$A \to B$ (A implies B)

Quantifiers

$\forall x\, A$ (A holds for all x)

$\exists x\, A$ (A holds for some x)

Abbreviations

$$\neg A \equiv A \to \bot$$

$$\forall n^{\mathbb{N}} A(n) \equiv \forall n(n \in \mathbb{N} \to A(n))$$

$$\exists x^{\mathbb{R}} A(n) \equiv \exists x(x \in \mathbb{R} \wedge A(n))$$

$$x \in \mathbb{Q}^{+} \equiv x \in \mathbb{Q} \wedge (x > 0)$$

Examples

The function $f:\mathbb{R}\to\mathbb{R}$ is continuous

$$\forall x^{\mathbb{R}},\varepsilon^{\mathbb{Q}^+}\exists\delta^{\mathbb{Q}^+}\forall y^{\mathbb{R}}(|x-y|<_{\mathbb{R}}\delta\to|fx-fy|<_{\mathbb{R}}\varepsilon)$$

The function $f:\mathbb{R}\to\mathbb{R}$ is uniformly continuous

$$\forall\varepsilon^{\mathbb{Q}^+}\exists\delta^{\mathbb{Q}^+}\forall x^{\mathbb{R}},y^{\mathbb{R}}(|x-y|<_{\mathbb{R}}\delta\to|fx-fy|<_{\mathbb{R}}\varepsilon)$$

The sequence $(a_n)_{n\in\mathbb{N}}\in\mathbb{R}$ converges to $x\in\mathbb{R}$

$$\forall\varepsilon^{\mathbb{Q}^+}\exists n^{\mathbb{N}}\forall m\geq n\,(|a_m-x|<_{\mathbb{R}}\varepsilon)$$

$$\sqrt{2} \notin \mathbb{Q}$$

Theorem. $\sqrt{2} \notin \mathbb{Q}$

What more can we say about this theorem?

Proof.

Assume we have $p, q \in \mathbb{N}$ such that $\frac{p}{q} = \sqrt{2}$

W.l.g., we can assume that $p, q \in \mathbb{N}$ are relatively prime

Then $\frac{p^2}{q^2} = 2$, and hence $p^2 = 2q^2$, so p must be even

Let $p = 2a$. Then $4a^2 = 2q^2$, and hence $2a^2 = q^2$, so q must be even

This contradicts the assumption that p,q are relatively prime. □

What extra information does this proof carry?

Theorem A. $\sqrt{2} \notin \mathbb{Q}$

Theorem B. For all $p,q \in \mathbb{N}$ with $q > 0$, if $p/q = \sqrt{2}$ then p, q are even

Theorem C. For all $p,q \in \mathbb{N}$ with $q > 0$, if either p or q is not even then $p/q \neq \sqrt{2}$

Theorem D. For all $p,q \in \mathbb{N}$ with $q > 0$, if either p or q is not even then $|p/q - \sqrt{2}| > \delta$, for some $\delta > 0$

Theorem D. For all $p,q \in \mathbb{N}$ with $q>0$, if either p or q is not even then $|p/q-\sqrt{2}|>\delta$, for some $\delta>0$

Theorem E. For all $p,q>0$ with p or q not even, we have

$$|\frac{p}{q}-\sqrt{2}|>\frac{1}{pq+2q^2}$$

Lemma. If $x,y>0$ and $|x^2-y^2|\geq\delta$ then $|x-y|\geq\delta/(x+y)$

Proof. Follows from $(x^2-y^2)=(x+y)(x-y)$. □

Lemma. If $x, y > 0$ and $|x^2 - y^2| \geq \delta$ then $|x - y| \geq \delta / (x + y)$

Theorem E. For all $p,q > 0$ with p or q not even, we have

$$|\frac{p}{q} - \sqrt{2}| > \frac{1}{pq + 2q^2}$$

Proof. Fix p, $q > 0$ and assume they are not both even.

It follows that $p^2 \neq 2q^2$ and $|p^2 - 2q^2| \geq 1$

Hence $|p^2 / q^2 - 2| \geq 1 / q^2$, and by the lemma above

$$|\frac{p}{q} - \sqrt{2}| \geq \frac{1}{q(p + q\sqrt{2})} > \frac{1}{pq + 2q^2} \quad \square$$

Theorem. $\sqrt{2} \notin \mathbb{Q}$

?

1. What strengthening of the theorem is possible?

2. How to obtain strengthening from the proof?

3. What extra lemmas are needed?

Theorem. For all $p,q>0$ with p or q not even, we have

$$\left|\frac{p}{q}-\sqrt{2}\right|>\frac{1}{pq+2q^2}$$

Incomplete Statements

(opportunity for proof mining)

Incomplete Statements

An **incomplete statement** contains a “positive” quantification which can be (non-trivially) bounded or witnessed precisely

No three positive integers a,b,c satisfy $a^n + b^n = c^n$, for $n > 2$
(Fermat's last theorem) ?

Every even interger greather than 2 can be expressed
as the sum of two primes (Goldbach conjecture) ?

Any continuous $f : [0,1] \to [0,1]$ has a fixed point
(Brouwer fixed-point theorem) ?

Any contractive $f : [0,1] \to [0,1]$ has at most one fixed point
(Edelstein fixed-point theorem) ?

No three positive integers a,b,c satisfy $a^n + b^n = c^n$, for $n > 2$
(Fermat's last theorem)

complete statement!

$$\forall n\,(n \in \mathbb{N} \wedge n > 2 \rightarrow \neg \exists a,b,c \in \mathbb{N}(a^n + b^n = c^n))$$

equivalent to...

$$\forall n\,(n \in \mathbb{N} \wedge n > 2 \rightarrow \forall a,b,c \in \mathbb{N}(a^n + b^n \neq c^n))$$

purely universal statement

Every even interger greather than 2 can be expressed as the sum of two primes (Goldbach conjecture)

complete statement!

$$\forall n\,(n \in \mathbb{N} \wedge n \in \text{Even} \wedge n > 2 \rightarrow \exists p_1, p_2 \in \text{Prime}\,(n = p_1 + p_2)$$

existence without explicit witness!

BUT

$$\forall n\,(n \in \mathbb{N} \wedge n \in \text{Even} \wedge n > 2 \rightarrow \exists p_1, p_2 \leq n\,(p_1, p_2 \in \text{Prime} \wedge n = p_1 + p_2)$$

existence can be easily bounded

Any continuous $f:[0,1]\to[0,1]$ has a fixed point

(Brouwer fixed-point theorem)

incomplete statement!

$$\mathrm{Cont}(f)\equiv\forall x^{[0,1]},\varepsilon^{\mathbb{Q}^+}\exists\delta^{\mathbb{Q}^+}\forall y^{[0,1]}(|x-y|<\delta\to|fx-fy|<\varepsilon)$$

$$\forall f^{[0,1]\to[0,1]}(\mathrm{Cont}(f)\to\exists x\in[0,1]\,(fx=x))$$

existence without explicit witness!

Any contractive $f:[0,1]\to[0,1]$ has at most one fixed point

(Edelstein fixed-point theorem)

incomplete statement!

$$\text{Contractive}(f)\equiv\forall x,y\in[0,1](|fx-fy|<|x-y|)$$

$$\forall f^{[0,1]\to[0,1]}$$

$$\text{Contractive}(f)\to$$

$$\forall x_1,x_2(x_1=fx_1\wedge x_2=fx_2\to x_1=x_2)$$

how close should x_i be to $f(x_i)$ to ensure x_1 is close to x_2?

Other Examples

Is this a complete or incomplete statement?

Theorem. There are $a,b \in \mathbb{R}$ such that $a,b \notin \mathbb{Q}$ but $a^b \in \mathbb{Q}$

$$\exists a,b \in \mathbb{R}(a,b \notin \mathbb{Q} \wedge a^b \in \mathbb{Q})$$

Proof.

Case 1: $\left(\sqrt{2}\right)^{\sqrt{2}} \in \mathbb{Q}$: Take $a = b = \sqrt{2}$

Case 2: $\left(\sqrt{2}\right)^{\sqrt{2}} \notin \mathbb{Q}$: Take $a = \left(\sqrt{2}\right)^{\sqrt{2}}$ and $b = \sqrt{2}$ □

Does this proof have enough information to "complete" the statement?

Infinity of Primes

Is this a complete or incomplete statement?

Theorem. There are infinitely many prime numbers

$$\forall n^{\mathbb{N}} \exists p > n \ \mathrm{Prime}(p)$$

Proof (Euclid).

Fix n and let $p_1, \ldots, p_m$ be all primes $\leq n$

Look at any prime factor p of $N = p_1 \ldots p_m + 1$

Clearly p is different from all p_i

Hence p is a prime greater than n □

Does this proof have enough information to "complete" the statement?

Theorem. $\forall n^{\mathbb{N}} \exists p > n \ \mathrm{Prime}(p)$

Proof (Euclid).

If $n = 0$ or $n = 1$ this is easy

Fix $n \geq 2$ and let $p_1, \ldots, p_m$ be all primes less than n

Look at any prime factor p of $N = p_1 \ldots p_m + 1$

Clearly $p \leq N \leq n! + 1$ is different from all p_i

Hence p is a prime greater than n □

Theorem (complete). $\forall n^{\mathbb{N}} \exists p^{\mathbb{N}} \in (n, n! + 2] \ \mathrm{Prime}(p)$

Next time…

- First-order logic, arithmetic and analysis
- Formal proofs, natural deduction
- Minimal, intuitionistic and classical logic
- Double negation translation