Introduction to Proof Mining

Paulo Oliva

Talk at Pure Maths Seminar, QMUL, May 18, 2009

Contents

1 Proof Mining

Let us look at Table 1.1. "Proof mining" means exactly what you would expect: looking at a given proof and trying to find something valuable hidden in that proof.

Point 1. The main point of a mathematical proof is to *assert the truth* of a mathematical statement. Proofs, however, carry a lot of extra information. Proofs will normally also give you *an idea of why the theorem is true*. Example: Banach-Tarski's paradox. They might also *provide computational information*, i.e. an algorithm to construct a witness, or an upper bound on the size of the witness. Example: infinitely many primes.

Point 2. Proof mining tries to formalise these ideas, and come up with techniques that enable one to systematically analyse proofs to extract information. Step 1: Identify what information can be obtained. Step 2: Carry out the extraction. Make analogy with actual mining. In mathematical logic this idea goes back to the 1950s, but only recently really interesting results started to

	C Proof	NC Proof
C Theorem ($\Pi_{k\leq 2}$)	(I)	(II)
NC Theorem ($\Pi_{k>2}$)	(III)	(IV)

Table 1: Types of Proofs

come out of this.

Point 3. Proof mining can be viewed as a formalisation of Tao's transfer principles. A systematic link between soft and hard mathematics.

Point 4. We will try to make a distinction between mathematical complexity and computational complexity of a proof. From a computational point of view Fermat's last theorem is trivial. On the other hand, the law of excluded middle (which is mathematically trivial) is highly non-computable.

Point 5. The end-result of proof mining is again a purely mathematical proof, so no traces of logic are required for the verification. Logic is only used as a tool in the extraction of new information.

1.1 Logical Preliminaries

Throughout my talk you should keep in mind that we will have an effective reading of "there exists" and "or". So, a statement $\exists x A$ in some sense asks for information about x's having property A. This could be a program which computes x, or it could simply be a bound on a value of x that satisfies A. Similarly, a proof of $\forall n(A(n) \vee B(n))$ asks for a decision whether $A(n)$ is true or $B(n)$ is true, given n. This information is called the *witnessing information* of a statement.

1.2 Non-computational theorems

A statement A is called *computational* if a putative proof of A will give us a recursive procedure witnessing A. Otherwise is said to be non-computational. For instance, the following statements are computational:

- An equation has no solutions $\forall n > 2 \forall x, y, z(x^n + y^n \neq z^n)$
- A function on the reals is zero $(*)$
- A recursive set is infinite $\forall n \exists m(m \geq n \wedge R(m))$
- Recursive specification of a program is total, i.e. $\forall x \exists y S(x, y)$
- A function on the reals is positive $\forall x(fx >_{\mathbb{R}} 0)$
- Implication between $(*)$.

On the other hand, the following statements are not computational

- Minimum value $\forall f \exists x \forall y(fx \leq fy)$

- Sequence is Cauchy $\forall\varepsilon\exists n\forall m \geq n(|a_n - a_m| < \varepsilon)$
- Bounded increasing sequence of reals converges
- König's lemma
- Excluded middle $\forall n(\exists k A(n,k) \vee \forall k \neg A(n,k))$
- Comprehension $\exists f\forall n(fn = 0 \leftrightarrow A(n))$.

1.3 Non-computational proofs

Point 1. A non-computational proof is a proof which uses a non-computational lemma or principle. There are two things which make a proof intricate or complex: the mathematics or the logic. I will focus on the logical aspect of proofs.

Point 2. Some non-computational theorems have computational proofs, and some computational theorems need non-computational proofs.

2 Examples

2.1 Infinitely many primes (I)

Proposition 2.1. $\forall k\exists n(n > k \wedge \mathsf{Prime}(n))$.

Proof [constructive]. Given k, let $P = !k + 1$. Let p be any prime dividing P. Clearly $p > k$. □

2.2 $\exists a, b(a, b$ **irrational** $\wedge\ a^b$ **rational**$)$ **(III)**

Proposition 2.2. $\exists a, b(a, b$ *irrational* $\wedge\ a^b$ *rational*$)$.

Proof [classical]. If $\sqrt{2}^{\sqrt{2}}$ is rational take $a = b = \sqrt{2}$. Else, take $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$. □

Proof [constructive]. Let $a = \sqrt{2}$ and $b = 2\log_2(3)$. □

2.3 $\sqrt{2}$ is irrational (negative translation) (II)

Point 1. *Eliminate classical logic.* That normally comes in the form of a proof by contradiction. If you want to prove A you assume $\neg A$ and derive B, at the same time that you also know $\neg B$, contradiction. Well, if you know $\neg B$, then you can derive $\neg\neg A$ directly, so all you need is

$$\neg\neg A \to A$$

which you can derive from

$$A \vee \neg A.$$

Proof [by contradiciton]. Assume exists p, q rational and relative primes such that $\sqrt{2} = p/q$. Then we have $2q^2 = p^2$, and hence p is even $(p = 2t)$.

Therefore, we also have $q^2 = 2t^2$, and hence q is even, contradiction. □

Proof [direct]. Fix p, q rational and relative primes. In particular either (p is odd) or (p is even and q is odd). If p is odd then $2q^2 \neq p^2$, hence $\sqrt{2} \neq p/q$. Also, if p is even ($p = 2t$) and q is odd then $2q^2 \neq p^2$. □

Proposition 2.3. $\forall p, q(\mathsf{RP}(p, q) \to |2 - p/q| > 1/q^2)$.

Enriched proof. Fix p, q rational and relative primes. In particular either (p is odd) or (p is even and q is odd). If p is odd then $|2q^2 - p^2| \geq 1$, hence $|2 - p^2/q^2| \geq 1/q^2$. Similarly if p is even and q is odd. □

2.4 $\Sigma\frac{1}{p_i}$ diverges (negative translation) (II)

Proof [by contradiciton]. Assume it converges. Then

$$\Sigma_{i\geq k+1}\frac{1}{p_i} < \frac{1}{2}$$

for some k. Hence

$$\Sigma_{i\geq k+1}\frac{N}{p_i} < \frac{N}{2}$$

for all N. Call $p_1, \ldots, p_k$ the small primes. Given N, define N_b the numbers $\leq N$ divisible by some big prime, and N_s the numbers only divisible by small primes. Clearly $N = N_s + N_b$. Also,

$$N_b \leq \Sigma_{i\geq k+1}\lfloor\frac{N}{p_i}\rfloor < \frac{N}{2}$$

and

$$N_s \leq 2^k\sqrt{N} \leq \frac{N}{2},$$

when $N = 2^{2k+2}$, a contradiction. □

Proof [direct]. We want to show that $\Sigma\frac{1}{p_i}$ diverges, i.e.

$$\forall k(\Sigma_{i\geq k+1}\frac{1}{p_i} \geq \frac{1}{2}).$$

Fix k and let $N = 2^{2k+2}$. As before, we have that $N_s \geq 2^k\sqrt{N} = N/2$. So,

$$2^{2k+1} \leq N_b \leq \Sigma_{i\geq k+1}\lfloor\frac{N}{p_i}\rfloor \leq \Sigma_{i\geq k+1}\frac{N}{p_i}.$$

Hence, $1/2 \leq \Sigma_{i\geq k+1}1/p_i$. □

Proof [quantitative]. Replace last line by

$$2^{2k+1} \leq N_b \leq \Sigma_{b(k)\geq i\geq k+1}\lfloor\frac{N}{p_i}\rfloor \leq \Sigma_{b(k)\geq i\geq k+1}\frac{N}{p_i}.$$

E.g. $b(k)$ = greatest j such that $p_k \leq 2^{2k+2}$. Then $\Sigma_{b^{2^L}k\geq i\geq k+1}\frac{1}{p_i} \geq L$. □

2.5 Drinker's paradox (nci of LEM) (IV)

Point 1. *Interpreting classical logic.* In some cases classical logic (or proofs by contradiction) cannot be eliminated. In these cases, the best we can do is give them a computational interpretation. As we exemplify in the following.

Proposition 2.4. *($e-\pi$ is irrational) or ($e+\pi$ is irrational).*

Proposition 2.5. $\exists x(P(x) \to \forall y P(y))$.

Proposition 2.6. $\forall f \exists x(P(x) \to P(fx))$.

Proof. Take $x = 0$ if $P(f0)$ holds, else take $x = f0$. □

2.6 Mean ergodic theorem (nci of comprehension) (IV)

Point 1. Non-counterexample interpretation can also be applied in more complex situations.

Proposition 2.7. *T non-expansive linear operator on Hilbert space H. Then*

$$A_n f = \frac{\Sigma_{k=0}^{n-1} T^k f}{n}$$

converges (in the Hilbert space norm).

Proposition 2.8 (nci)**.** $\forall K^{\mathbb{N}\to\mathbb{N}}, \varepsilon>0\, \exists n(||A_n f - A_{n+K(n)} f|| < \varepsilon)$.

Given any M, pick K above to the the function $K(n)$ which returns $m \in [n, n+M(n)]$ maximizing $||A_n f - A_m f||$. Then we have:

Proposition 2.9. $\forall M^{\mathbb{N}\to\mathbb{N}}, \varepsilon>0\, \exists n \forall m \in [n, n+M(n)](||A_n f - A_m f|| < \varepsilon)$.

2.7 L_1-approximation (bounded interpretation of WKL) (II)

Let us look at a mild use of comprehension, namely, König's lemma (actually only the weak version)

$$\forall n \exists s(|s| = n \wedge T(s)) \to \exists \alpha \forall n T(\overline{\alpha} n)$$

where T is a finitely branching tree.

Point 1. This is widely used. Equivalent to Heine/Borel compactness, continuous functions attain its infimum on unit interval, completeness of first order logic, etc.

Point 2. This is not computational. There exists a recursive infinite tree whose infinite branches are all non-computable.

Point 3. Nevertheless, when used in a proof of a computational theorem, uses of König's lemma can be eliminated.

Lemma 2.1 (Lemma 1)**.** *Let $f, h \in C[0,1]$. If f has at most a finite number of roots and if $\int h \,\mathsf{sgn}\, f \neq 0$ then $\exists \lambda(\int |f - \lambda h| < \int |f|)$.*

Proof. Let $x_1, \ldots, x_n$ be all the roots of f. Let A_ε the the union of closed intervals between the roots, away by ε. And B the complement of A. If $\int h \,\mathsf{sgn}\, f > 0$ (otherwise invert signs), select ε small enough so that $(*)$ $\int_A h \,\mathsf{sgn} f > \int_B |h|$. Since A is closed and contains no roots of f we have $\delta = \inf f$ is positive. Let λ be such that $0 < \lambda||h|| < \delta$. Then, on A we have $(**)$ $\mathsf{sgn}(f - \lambda h) = \mathsf{sgn} f$. Thus we have

$$\int |f - \lambda h| \overset{(**)}{=} \int_B |f - \lambda h| + \int_A (f - \lambda h)\,\mathsf{sgn} f \overset{(*)}{<} \int |f|.$$

That concludes the proof. □

Lemma 2.2 (Computational Lemma 1)**.** *Let $f, h \in C[0,1]$, $x_1, \ldots, x_n \in [0,1]$ and $\varepsilon, \eta \in \mathbb{Q}$. If $(**)$ $\forall\lambda(||f - \lambda h|| \geq ||f||)$ and $(*)$ $\int_A h \,\mathsf{sgn} f > \int_B |h|$ then f has an η-root in A.*

Proof. Let A and B as above. Thus, for all λ, we have

$$\int |f - \lambda h| \overset{(**)}{\geq} \int |f| \overset{(*)}{>} \int_B |f - \lambda h| + \int_A (f - \lambda h)\,\mathsf{sgn} f.$$

Let $\lambda = \eta/||h||$. Hence, $\int_A |f - \lambda h| > \int_A (f - \lambda h)\,\mathsf{sgn} f$, i.e. there is a point where $\mathsf{sgn}(f - \lambda h) \neq \mathsf{sgn} f$. Which implies that $|fy| \leq \lambda |h(y)|$, for some $y \in A$. □

3 Appendix A: PHP ⊆ Classical Logic + Induction

Proof by induction

$$A(0) \wedge \forall n(A(n) \to A(n+1)) \to \forall n A(n)$$

have a very clear computational interpretation via iteration (recursion). But when classical logic and induction come together they can be quite difficult to analyse. And often these proofs are related to the pigeon-hole principle.

Proposition 3.1 (Dirichlet)**.** $\forall n^{\mathbb{N}}, x^{\mathbb{R}} \exists m, k^{\mathbb{N}}((1 \leq m \leq n) \wedge |mx - k| \leq \frac{1}{n+1})$.

Proof [non-computational]. Let n and x be fixed. Assume, for the sake of contradiction, that the fractional part of mx is always away from an integer by more than $1/(n+1)$, for all $1 \leq m \leq n$. They, by the PHP, for some $1 \leq m_1 < m_2 \leq n$ we must have that the fractional part of $m_1 x$ and $m_2 x$ are within $1/(n+1)$ of each other, which means that $(m_2 - m_1)x$ must be closer to an integer by $1/(n+1)$, contradiction. □

Proposition 3.2. $\forall n^{\mathbb{N}}, x^{\mathbb{R}}, \varepsilon^{\mathbb{Q}^*_+} \exists m, k^{\mathbb{N}}((1 \leq m \leq n) \wedge |mx - k| < \frac{1}{n+1} + \varepsilon)$.

Proof [computational]. Let x, n, ε be fixed. Compute mx $(= x_m)$ up to an error $\varepsilon/4$, for all $1 \leq m \leq n$. Either we can immediately find x_m such that $|x_m - k| \leq \frac{1}{n+1} + \frac{\varepsilon}{2}$, which implies $|x - k| < \frac{1}{n+1} + \varepsilon$, or all x_m are away from an integer by $\frac{1}{n+1} + \frac{\varepsilon}{2}$. Consider the $n-1$ intervals

$$I_i = [\tfrac{i}{n+1} - \tfrac{\varepsilon}{8}, \tfrac{i+1}{n+1} + \tfrac{\varepsilon}{8}],$$

for $1 \leq i < n$. By the PHP there are $\{x_{m_1}\}$ and $\{x_{m_2}\}$ which fall in the same interval, i.e. $|\{x_{m_1}\} - \{x_{m_2}\}| \leq \frac{1}{n+1} + \frac{\varepsilon}{4}$, which implies $|\{m_1 x\} - \{m_2 x\}| \leq \frac{1}{n+1} + \frac{3\varepsilon}{4}$. □

Remark 3.1. *One can always turn a proof which uses the PHP*

$$\forall n \forall S, T(|S| \geq n \wedge |T| < n \to \forall H^{S \to T} \exists k_0, k_1 (Hk_1 = Hk_2))$$

into a proof by induction (and classical logic). In fact, the induction proof might be more insightful computationally, as the following example illustrates.

Proposition 3.3. *Given $n+1$ numbers between 1 and $2n$ we can always find a, b such that a divides b.*

Proof [by PHP]. Write all numbers as $2^k p$, where p is odd. There are only n odd parts, so, by the PHP, two numbers must be of the form $2^{k_1} p$ and $2^{k_2} p$, with $k_1 < k_2$. □

Proof [by induction and CL]. Result trivially hold for $n = 1$. Assume it holds for n, let's show for $n+1$. Let $S \subseteq \{1, 2, \ldots, 2n+1, 2n+2\}$ such that $|S| \geq n+2$. If $2n+2$ and $n+1$ are in the set, we are done. If $2n+2$ is in the set but $n+1$ is not, consider the new set $S' = (S \backslash \{2n+1, 2n+2\}) \cup \{n+1\}$. Since $|S'| \geq n+1$ we use the IH to obtain $a, b \in S'$ such that a divides b. It is clear that $a \neq n+1$. If $b \neq n+1$ then a, b is also a solution in S. If $b = n+1$ then a also divides $2n+2$ in S. □

Proposition 3.4. $\forall K \forall f^{\mathbb{N} \to K} \exists b^K \forall n \exists m (m \geq n \wedge fm = b)$.

4 Appendix B: Theorems equivalent to WKL

The following results are equivalent to weak König's lemma and thus to WKL_0 over RCA_0:

- Heine-Borel theorem for the closed unit real interval (every covering by a sequence of open intervals has a finite subcovering).
- The Heine-Borel theorem for complete totally bounded separable metric spaces (where covering is by a sequence of open balls).
- A continuous real function on the closed unit interval is bounded.
- A continuous real function on the closed unit interval can be uniformly approximated by polynomials (with rational coefficients).
- A continuous real function on the closed unit interval is uniformly continuous.
- A continuous real function on the closed unit interval is Riemann integrable.

- The Brouwer fixed point theorem (for continuous functions on a finite product of copies of the closed unit interval).
- The separable Hahn-Banach theorem in the form: a bounded linear form on a subspace of a separable Banach space extends to a bounded linear form on the whole space.
- Gödel's completeness theorem (for a countable language).
- Every countable commutative ring has a prime ideal.
- Every countable formally real field is orderable.
- Uniqueness of algebraic closure (for a countable field).