Proof Mining

Lecture 2: Proof Translations

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

Lecture 1 Recap

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

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

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

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

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

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 E. 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 can be strengthened by bounding or witnessing some of the quantifications

Complete

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

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

Incomplete

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

$\sqrt{2}$ is irrational

The set of primes is unbounded

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

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

Today

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

First-order Logic
(natural deduction system)

Introduction Rules

$$\frac{\begin{array}{cc}\vdots & \vdots \\ A & B\end{array}}{A \wedge B}\ \wedge\mathrm{I}$$

$$\frac{\begin{array}{c}\vdots \\ A\end{array}}{A \vee B}\ \vee\mathrm{I} \qquad \frac{\begin{array}{c}\vdots \\ B\end{array}}{A \vee B}\ \vee\mathrm{I}$$

$$\frac{\begin{array}{c}[A]_{\alpha} \\ \vdots \\ B\end{array}}{A \to B}\ \to\mathrm{I},\alpha$$

Elimination Rules

$$\frac{\begin{array}{c}\vdots \\ A \wedge B\end{array}}{A}\ \wedge\mathrm{E} \qquad \frac{\begin{array}{c}\vdots \\ A \wedge B\end{array}}{B}\ \wedge\mathrm{E}$$

$$\frac{\begin{array}{ccc}\vdots & [A]_{\alpha} & [B]_{\beta} \\ A \vee B & \vdots & \vdots \\ & C & C\end{array}}{C}\ \vee\mathrm{E}, \alpha, \beta$$

$$\frac{\begin{array}{cc}\vdots & \vdots \\ A & A \to B\end{array}}{B}\ \to\mathrm{E}$$

Introduction Rules

$$\dfrac{\dfrac{\Gamma}{\vdots}}{\dfrac{A(x)}{\forall x\, A(x)}} \quad x \notin \mathrm{FV}(\Gamma)$$

$$\dfrac{\dfrac{\vdots}{A(t)}}{\exists x\, A(x)}$$

Elimination Rules

$$\dfrac{\dfrac{\vdots}{\forall x\, A(x)}}{A(t)}$$

$$\dfrac{\dfrac{\vdots}{\exists x\, A(x)} \qquad \dfrac{\dfrac{[A(x)]}{\vdots}}{C}}{C} \quad x \notin \mathrm{FV}(C)$$

The just system described is called Minimal Logic **ML**

Ex falso quodlibet

$$\frac{\begin{array}{c}\vdots\\ \bot\end{array}}{A}\ \text{EFQ}$$

ML + **EFQ** is called intuitionistic logic **IL**

Proof by contradiction

$$\frac{\begin{array}{c}[\neg A]_\alpha\\ \vdots\\ \bot\end{array}}{A}\ \text{PBC},\ \alpha$$

ML + **PBC** is called classical logic **CL**

Formal Proofs

$$\boxed{\neg\neg A, \neg\neg B \vdash \neg\neg(A \wedge B)}$$

$$\dfrac{\dfrac{\dfrac{[A]_\alpha \quad [B]_\beta}{A \wedge B} \quad [\neg(A \wedge B)]_\gamma}{\dfrac{\bot}{\neg A}\,\alpha \qquad \neg\neg A}}{\dfrac{\dfrac{\bot}{\neg B}\,\beta \qquad \neg\neg B}{\dfrac{\bot}{\neg\neg(A \wedge B)}\,\gamma}}$$

$$\boxed{\vdash A \vee \neg A}$$

$$\dfrac{\dfrac{\dfrac{[A]_{\alpha}}{A \vee \neg A} \qquad [\neg(A \vee \neg A)]_{\gamma}}{\bot}\ \alpha}{\neg A}$$

$$\dfrac{\dfrac{A \vee \neg A \qquad [\neg(A \vee \neg A)]_{\gamma}}{\bot}}{A \vee \neg A}\ \text{PBC}, \gamma$$

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

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. □

assumption used twice (contraction)

$$\dfrac{\dfrac{\dfrac{[p/q=\sqrt{2}]_{\alpha}}{p=q\sqrt{2}}}{p^2=2q^2}}{\exists a(p=2a)} \qquad [p=2a] \qquad \dfrac{\dfrac{[p/q=\sqrt{2}]_{\alpha}}{p=q\sqrt{2}}}{p^2=2q^2}\ \exists E,\beta$$

$$\dfrac{\exists a(p=2a)\wedge\exists b(q=2b) \qquad [\forall a(p\neq 2a)\vee\forall b(q\neq 2b)]_{\gamma}}{\dfrac{\dfrac{\dfrac{\bot}{p/q\neq\sqrt{2}}\ \to I,\alpha}{\forall a(p\neq 2a)\vee\forall b(q\neq 2b)\to p/q\neq\sqrt{2}}\ \to I,\gamma}{\forall p,q(\forall a(p\neq 2a)\vee\forall b(q\neq 2b)\to(p/q\neq\sqrt{2}))}\ \forall I}$$

Tree Style **Sequent Style**

$$\dfrac{\begin{array}{cc}\vdots & \vdots \\ A & B\end{array}}{A\wedge B}\ \wedge\mathrm{I} \qquad\longrightarrow\qquad \dfrac{\Gamma\vdash A \quad \Gamma\vdash B}{\Gamma\vdash A\wedge B}\ \wedge\mathrm{I}$$

$$\dfrac{\begin{array}{ccc}\vdots & \overset{[A]_\alpha}{\vdots} & \overset{[B]_\beta}{\vdots} \\ A\vee B & C & C\end{array}}{C}\ \vee\mathrm{E},\alpha,\beta \qquad\longrightarrow\qquad \dfrac{\Gamma\vdash A\vee B \quad \Gamma,A\vdash C \quad \Gamma,B\vdash C}{\Gamma\vdash C}\ \vee\mathrm{E}$$

$$\dfrac{\begin{array}{c}\overset{[A]_\alpha}{\vdots} \\ B\end{array}}{A\to B}\ \to\mathrm{I},\alpha \qquad\longrightarrow\qquad \dfrac{\Gamma,A\vdash B}{\Gamma\vdash A\to B}\ \to\mathrm{I}$$

Meta Theorems

(theorems about theorems)

Proposition (Disjunction property).

If IL proves $A \vee B$ then either IL proves A or IL proves B

Proposition (Existence property).

If IL proves $\exists x\, A(x)$ then IL proves $A(t)$ for some term t

Proposition (Disjunction property failure in CL).

CL always proves $A \vee \neg A$ while it might not prove either A or $\neg A$

Proposition (Existence property failure in CL, Drinker paradox).

CL proves $\exists x(A(x) \to \forall y A(y))$ but doesn't prove $A(t) \to \forall y A(y)$ for any term t

Double Negation Translation

$$\boxed{\vdash A \vee \neg A}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{[A]_{\alpha}}{A \vee \neg A}}{\neg A}\,\alpha}{A \vee \neg A} \qquad [\neg(A \vee \neg A)]_{\gamma}}{\dfrac{\bot}{A \vee \neg A}\,\text{PBC},\gamma}$$

Proof in Classical Logic

$$\boxed{\vdash \neg\neg\neg(A \vee \neg A)}$$

Proof in Intuitionistic Logic

$$\dfrac{\dfrac{\dfrac{\dfrac{[A]_{\alpha}}{A \vee \neg A} \qquad [\neg(A \vee \neg A)]_{\gamma}}{\bot}\alpha}{\neg A}}{A \vee \neg A} \qquad [\neg(A \vee \neg A)]_{\gamma}}{\dfrac{\bot}{\neg\neg(A \vee \neg A)} \to \mathrm{I}, \gamma}$$

$$\boxed{\vdash A \vee \neg A}$$

$$\dfrac{\dfrac{\dfrac{[A]_{\alpha}}{A \vee \neg A} \qquad [\neg(A \vee \neg A)]_{\gamma}}{\dfrac{\bot}{\neg A}\,\alpha}}{\dfrac{\bot}{A \vee \neg A}\,\text{PBC},\gamma}$$

$$\boxed{\vdash \neg\neg(A \vee \neg A)}$$

$$\dfrac{\dfrac{\dfrac{[A]_{\alpha}}{A \vee \neg A} \qquad [\neg(A \vee \neg A)]_{\gamma}}{\dfrac{\bot}{\neg A}\,\alpha}}{\dfrac{\bot}{\neg\neg(A \vee \neg A)}\,\to\text{I},\gamma}$$

Intuitionistic Logic
(ex falso quodlibet)

$$\dfrac{\dfrac{\vdots}{\bot}}{A}\ \text{EFQ}$$

Classical Logic
(proof by contraction)

$$\dfrac{\dfrac{\dfrac{[\neg A]_{\alpha}}{\vdots}}{\bot}}{A}\ \text{PBC},\ \alpha$$

Proposition (Gentzen 1933).

If CL proves $\Gamma \vdash A$ then IL proves $\Gamma^N \vdash A^N$ where

$$\begin{array}{lcllcl}
(A \wedge B)^N & \equiv & A^N \wedge B^N & (P)^* & \equiv & \neg\neg P \\
(A \vee B)^N & \equiv & \neg\neg(A^N \vee B^N) & (\forall x\, A)^N & \equiv & \forall x\, A^N \\
(A \to B)^N & \equiv & A^N \to B^N & (\exists x\, A)^N & \equiv & \neg\neg \exists x A^N
\end{array}$$

What would its double negation translation be?

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

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 $b = \sqrt{2}$ □

Proof uses classical logic
(in the form of LEM — law of excluded middle)

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

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

$$\downarrow$$

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

equivalently

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

$$\begin{array}{lcl@{\qquad}lcl}
(A \wedge B)^N & \equiv & A^N \wedge B^N & (P)^* & \equiv & \neg\neg P \\
(A \vee B)^N & \equiv & \neg\neg(A^N \vee B^N) & (\forall x\, A)^N & \equiv & \forall x\, A^N \\
(A \to B)^N & \equiv & A^N \to B^N & (\exists x\, A)^N & \equiv & \neg\neg\exists x A^N
\end{array}$$

$$
\dfrac{\dfrac{\dfrac{[\forall a,b\in\mathbb{R}\neg(a,b\notin\mathbb{Q}\wedge a^{b}\in\mathbb{Q})]_{\alpha}}{\neg(\sqrt{2}\notin\mathbb{Q}\wedge(\sqrt{2})^{\sqrt{2}}\in\mathbb{Q})}}{(\sqrt{2})^{\sqrt{2}}\notin\mathbb{Q}}
\qquad
\dfrac{\dfrac{[\forall a,b\in\mathbb{R}\neg(a,b\notin\mathbb{Q}\wedge a^{b}\in\mathbb{Q})]_{\alpha}}{\neg((\sqrt{2})^{\sqrt{2}}\notin\mathbb{Q}\wedge\sqrt{2}\notin\mathbb{Q}\wedge 2\in\mathbb{Q})}}{\neg((\sqrt{2})^{\sqrt{2}}\notin\mathbb{Q})}}{\dfrac{\bot}{\neg\forall a,b\in\mathbb{R}\neg(a,b\notin\mathbb{Q}\wedge a^{b}\in\mathbb{Q})}\ \boxed{\to\mathrm{I},\alpha}}
$$

Peano Arithmetic

Peano Axioms

$$0 \in \mathbb{N}$$

$$\forall n^{\mathbb{N}} (\mathrm{Succ}(n) \in \mathbb{N})$$

$$\forall n^{\mathbb{N}} (0 \neq \mathrm{Succ}(n))$$

$$\forall n^{\mathbb{N}}, m^{\mathbb{N}} (\mathrm{Succ}(n) = \mathrm{Succ}(m) \to n = m)$$

Induction Rule

$$\frac{\Gamma \vdash A(0) \qquad \Gamma \vdash \forall n^{\mathbb{N}} (A(n) \to A(n+1))}{\Gamma \vdash \forall n^{\mathbb{N}} A(n)}$$

Analysis

Comprehension

$$\exists f^{\mathbb{N}\to\mathbb{B}}\forall n^{\mathbb{N}}(fn \leftrightarrow A(n))$$

Axiom of Choice

$$\forall x^{\tau}\exists y^{\rho}A(x,y) \to \exists f^{\tau\to\rho}\forall x^{\tau}A(x,fx)$$

Axiom of Countable Choice

$$\forall n^{\mathbb{N}}\exists x^{\rho}A(n,x) \to \exists f^{\mathbb{N}\to\rho}\forall n^{\mathbb{N}}A(n,fn)$$

König's Lemma

$$\mathrm{Tree}(A)\wedge\forall n^{\mathbb{N}}\exists s^{\rho^*}(|s|\geq n\wedge A(n,s)) \to \exists f^{\mathbb{N}\to\rho}\forall n^{\mathbb{N}}A(n,\overline{f}(n))$$

Comprehension

$$\exists f^{\mathbb{N}\to\mathbb{B}}\forall n^{\mathbb{N}}(fn \leftrightarrow A(n))$$

Let $T(n,n,u)$ be the statement that Turing machine with code n on input n will halt with computation u

The Halting problem (known to be undecidable) is

$$A(n) \equiv \exists u T(n,n,u)$$

So clearly, the following (true) statement cannot be witnessed by a computable function f

$$\exists f^{\mathbb{N}\to\mathbb{B}}\forall n^{\mathbb{N}}(fn \leftrightarrow \exists u T(n,n,u))$$

Next time…

- Lambda calculus, system T
- Functional interpretation
- Interpreting induction
- Interpreting choice and comprehension