Tutorial on Proof Theory

(with emphasis on proof mining)

Lecture 1: Formal Proofs

Paulo Oliva
Queen Mary University of London

Days in Logic 2020

Lisbon, 30 Jan - 1 Feb 2020

Proof of A $\longrightarrow$ Truth of A

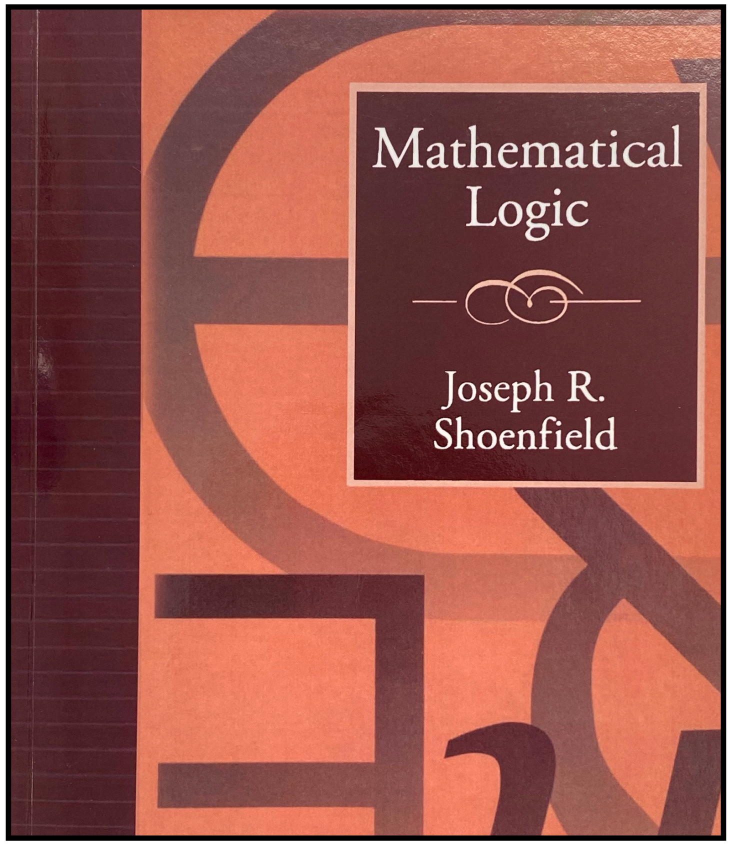
Construction for A $\longrightarrow$ Truth of A

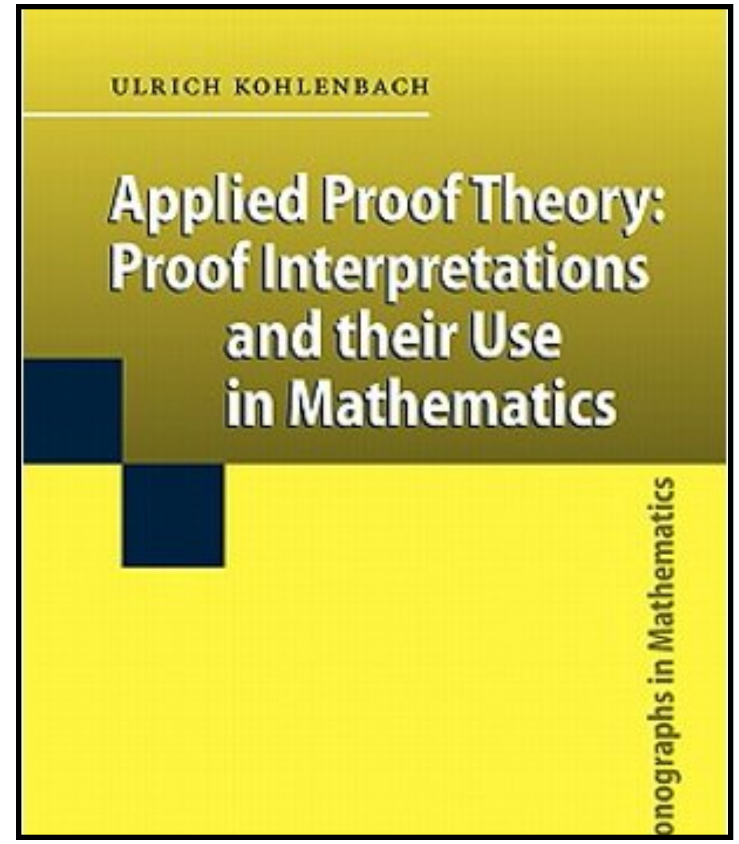
No proof of 0=1 $\longrightarrow$ Consistency

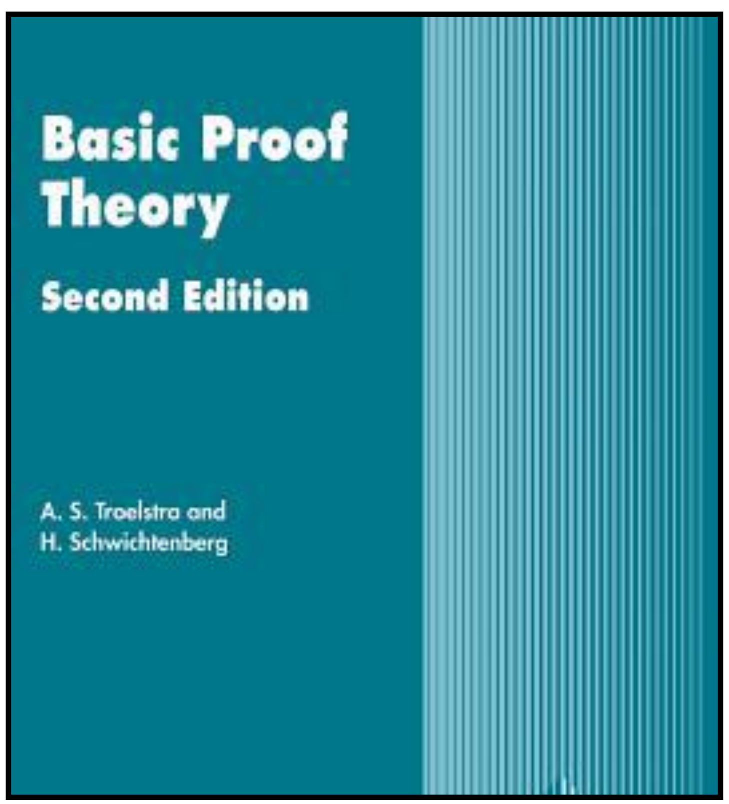
No short proof of A_n $\longrightarrow$ Separation of complexity classes

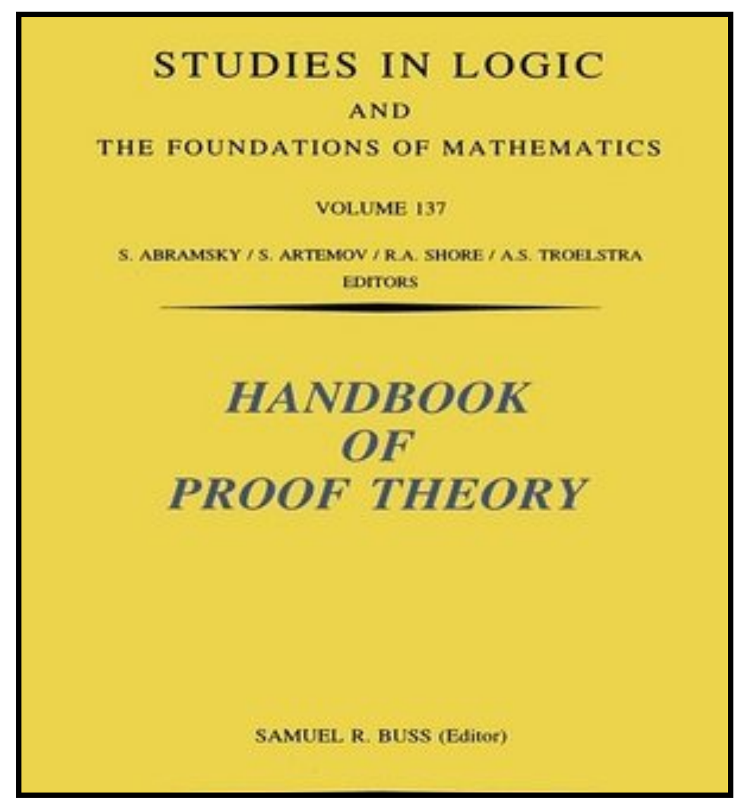
Proof of A $\longrightarrow$ Program of type A

Proof of A $\longrightarrow$ More than truth of A


Mathematical Logic
Joseph R. Shoenfield


ULRICH KOHLENBACH
Applied Proof Theory: Proof Interpretations and their Use in Mathematics
onographs in Mathematics


Basic Proof Theory
Second Edition
A. S. Troelstra and
H. Schwichtenberg


STUDIES IN LOGIC
AND
THE FOUNDATIONS OF MATHEMATICS
VOLUME 137
S. ABRAMSKY / S. ARTEMOV / R.A. SHORE / A.S. TROELSTRA
EDITORS
HANDBOOK OF PROOF THEORY
SAMUEL R. BUSS (Editor)

Plan

Lecture 1: **Formal Proofs**

Lecture 2: Proof Translations

Lecture 3: Proof Interpretations

Today

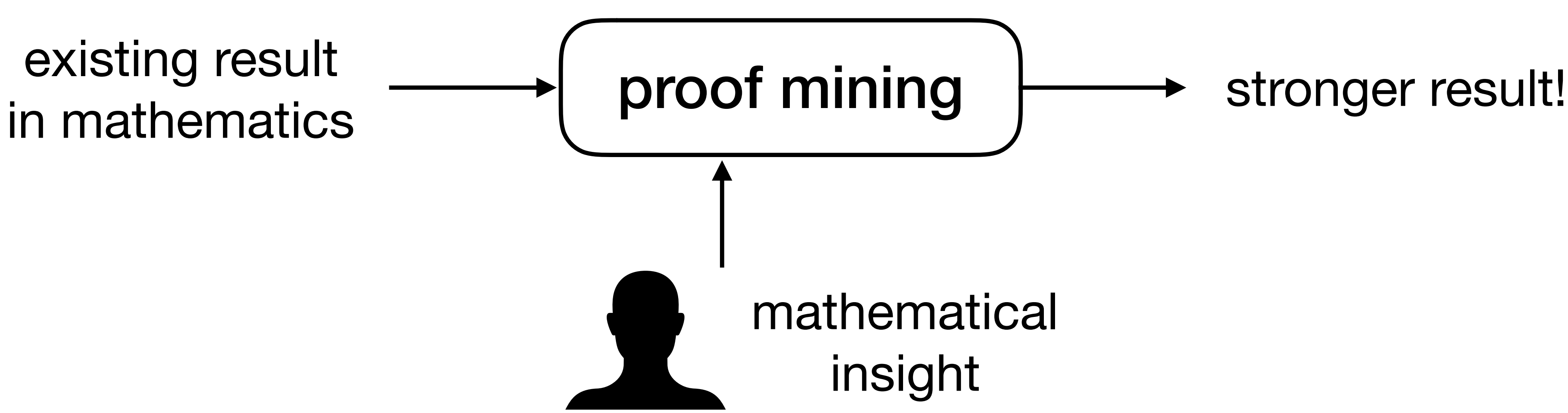
- Applied proof theory: Proof mining
- Formal language
- Formal proofs
- Some examples!

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

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

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 $\dfrac{p}{q} = \sqrt{2}$

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

Then $\dfrac{p^2}{q^2} = 2$, 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. $\square$

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 $(x^2 - y^2) = (x + y)(x - y)$. $\square$

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

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

Formal Language

Atomic formulas

$\perp$ (contradiction)

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

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

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

$\neg A \equiv A \to \perp$

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

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

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

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 $x \in \mathbb{R}$

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

First-order Logic

(natural deduction system)

Introduction Rules

$$\frac{\dfrac{\vdots}{A} \qquad \dfrac{\vdots}{B}}{A \wedge B}\ \wedge\mathrm{I}$$

$$\frac{\dfrac{\vdots}{A}}{A \vee B}\ \vee\mathrm{I} \qquad \frac{\dfrac{\vdots}{B}}{A \vee B}\ \vee\mathrm{I}$$

$$\frac{\dfrac{\dfrac{[A]_\alpha}{\vdots}}{B}}{A \to B}\ \to\mathrm{I},\alpha$$

Elimination Rules

$$\frac{\dfrac{\vdots}{A \wedge B}}{A}\ \wedge\mathrm{E} \qquad \frac{\dfrac{\vdots}{A \wedge B}}{B}\ \wedge\mathrm{E}$$

$$\frac{\dfrac{\vdots}{A \vee B} \qquad \dfrac{\dfrac{[A]_\alpha}{\vdots}}{C} \qquad \dfrac{\dfrac{[B]_\beta}{\vdots}}{C}}{C}\ \vee\mathrm{E},\alpha,\beta$$

$$\frac{\dfrac{\vdots}{A} \qquad \dfrac{\vdots}{A \to B}}{B}\ \to\mathrm{E}$$

Introduction Rules

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

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

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

$$\dfrac{\begin{matrix}\vdots \\ \hline \bot\end{matrix}}{A}\ \mathrm{EFQ}$$

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

Proof by contradiction

$$\dfrac{\begin{matrix}\dfrac{[\neg A]_\alpha}{\vdots} \\ \hline \bot\end{matrix}}{A}\ \mathrm{PBC},\ \alpha$$

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

Tree Style

Sequent Style

$$\dfrac{\dfrac{\vdots}{A} \qquad \dfrac{\vdots}{B}}{A \wedge B}\,\wedge\mathrm{I} \quad \longrightarrow \quad \dfrac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\,\wedge\mathrm{I}$$

$$\dfrac{\dfrac{\vdots}{A \vee B} \qquad \dfrac{\dfrac{[A]_\alpha}{\vdots}}{C} \qquad \dfrac{\dfrac{[B]_\beta}{\vdots}}{C}}{C}\,\vee\mathrm{E}, \alpha, \beta \quad \longrightarrow \quad \dfrac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C}\,\vee\mathrm{E}$$

$$\dfrac{\dfrac{\dfrac{[A]_\alpha}{\vdots}}{B}}{A \to B}\,\to\mathrm{I}, \alpha \quad \longrightarrow \quad \dfrac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}\,\to\mathrm{I}$$

Aside: Linear Logic

$$\dfrac{\dfrac{\overline{[A]_\alpha}}{\vdots}}{\dfrac{\overline{\quad B \quad}}{A \to B}} \to \mathrm{I}, \alpha$$

In classical/ intuitionistic/minimal logic one doesn't "count" the number of times A appears as an assumption

First-order logic

assumes contraction

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge\mathrm{I}$$

same assumption used multiple times

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash A \rightarrow B}{\Gamma \vdash B} \rightarrow\mathrm{E}$$

Linear Logic

multiplicative conjunction

$$\frac{\Gamma \vdash A \qquad \Delta \vdash B}{\Gamma, \Delta \vdash A \otimes B} \otimes\mathrm{I}$$

additive conjunction

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \,\&\, B} \&\mathrm{I}$$

linear implication

$$\frac{\Gamma \vdash A \qquad \Delta \vdash A \multimap B}{\Gamma, \Delta \vdash B} \multimap\mathrm{E}$$

Formal Proofs

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

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

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

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

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

Proof.

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

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

Then $\dfrac{p^2}{q^2} = 2$, 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. $\square$

assumption used twice (contraction)

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

Tomorrow…

- Complete vs incomplete statements
- Intuitionistic vs classical proofs
- Double negation translations