Tutorial on Proof Theory

(with emphasis on proof mining)

Lecture 2: Proof Translations

Paulo Oliva

Queen Mary University of London

Days in Logic 2020

Lisbon, 30 Jan - 1 Feb 2020

Plan

Lecture 1: Formal Proofs

Lecture 2: **Proof Translations**

Lecture 3: Proof Interpretations

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

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

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**

$$\frac{\vdots}{\dfrac{A}{A \vee B}}$$

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

$$\frac{\vdots}{\dfrac{\bot}{A}}$$

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

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

Slash Translation

provability in **IL**

$$\Gamma \mid P \equiv \Gamma \vdash P$$

$$\Gamma \mid A \wedge B \equiv (\Gamma \mid A) \wedge (\Gamma \mid B)$$

$$\Gamma \mid A \vee B \equiv (\Gamma \mid A) \vee (\Gamma \mid B)$$

$$\Gamma \mid A \to B \equiv (\Gamma \mid A) \to (\Gamma \mid B)$$

$$\Gamma \mid \forall x A \equiv \forall t(\Gamma \mid A[t/x])$$

$$\Gamma \mid \exists x A \equiv \exists t(\Gamma \mid A[t/x])$$

closed terms of **IL**

Thm: Assume $\Gamma \mid \Gamma$

If $\Gamma \vdash A$ then $\Gamma \mid A$

Proof: Induction on the proof $\Gamma \vdash A$

Cor: Assume $\Gamma \mid A$

If $\Gamma \vdash A \vee B$ then either $\Gamma \mid A$ or $\Gamma \mid B$

Slash Translation

$$\Gamma\,|\,P \;\equiv\; \Gamma \vdash P$$

$$\Gamma\,|\,A \wedge B \;\equiv\; (\Gamma\,|\,A) \wedge (\Gamma\,|\,B)$$

$$\Gamma\,|\,A \vee B \;\equiv\; (\Gamma\,|\,A) \vee (\Gamma\,|\,B)$$

$$\Gamma\,|\,A \to B \;\equiv\; ((\Gamma\,|\,A) \to (\Gamma\,|\,B)) \wedge \Gamma \vdash A \to B$$

$$\Gamma\,|\,\forall x A \;\equiv\; \forall t(\Gamma\,|\,A[t/x]) \wedge \Gamma \vdash \forall x A$$

$$\Gamma\,|\,\exists x A \;\equiv\; \exists t(\Gamma\,|\,A[t/x])$$

Thm 1: Assume $\Gamma\,|\,\Gamma$. If $\Gamma \vdash A$ then $\Gamma\,|\,A$

Thm 2: $\Gamma\,|\,A$ implies $\Gamma \vdash A$

Cor: If $\vdash A \vee B$ then either $\vdash A$ or $\vdash B$

CL = ML + PBC

$$\frac{\begin{array}{c}\vdots\\ A\end{array}}{A \vee B} \qquad \frac{\begin{array}{c}\vdots\\ A(t)\end{array}}{\exists x\, A(x)} \qquad \frac{\begin{array}{c}[\neg A]_{\alpha}\\ \vdots\\ \bot\end{array}}{A}\ \text{PBC}, \alpha$$

Proposition (Disjunction property failure in CL).

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

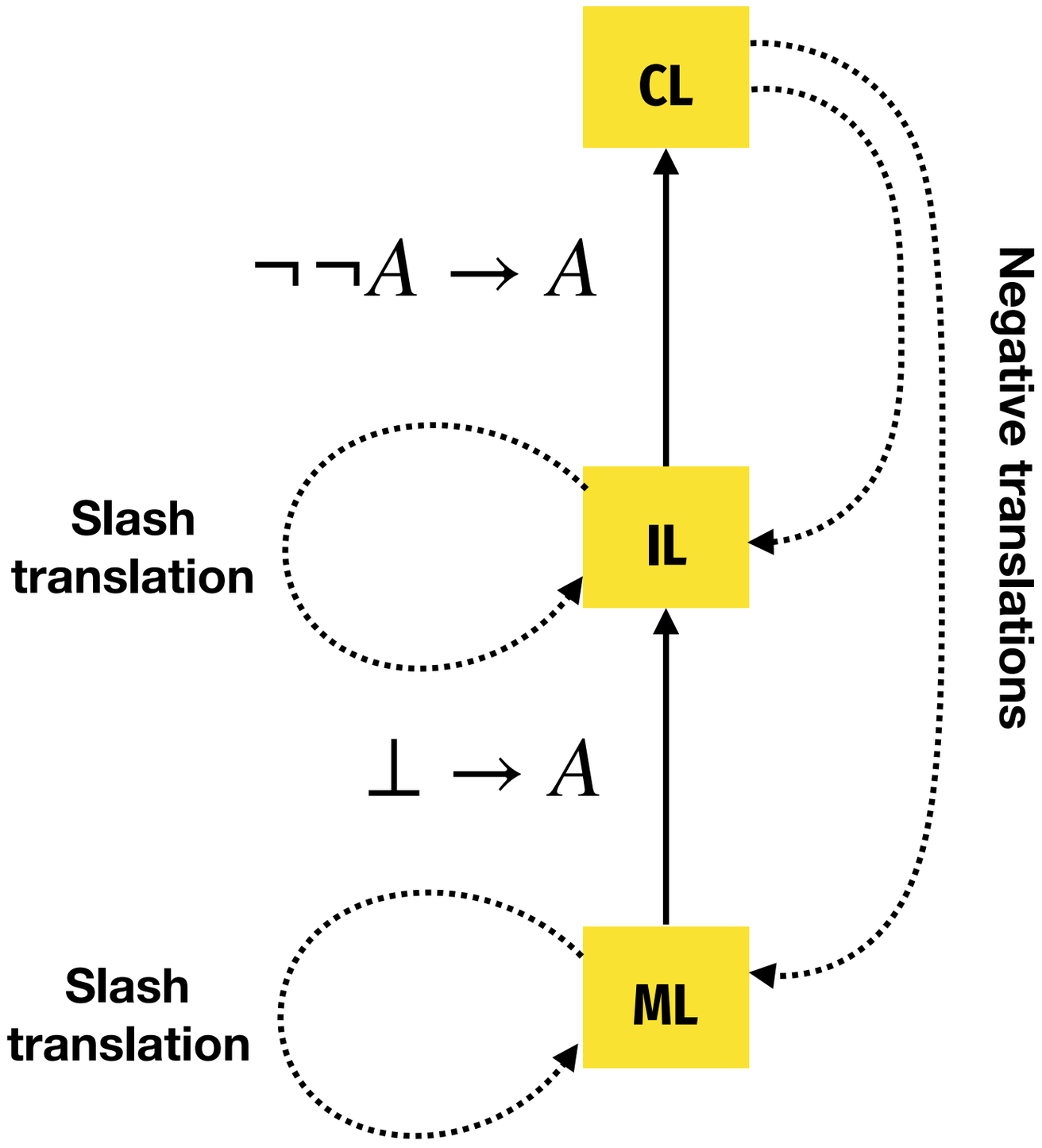
Proposition (Existence property failure in CL, Drinker paradox).

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

Herbrand Theorem

Theorem: If $\exists x A_{\mathrm{qf}}(x)$ is provable in classical predicate logic then for some terms $t_1, \ldots, t_n$ the disjunction $A_{\mathrm{qf}}(t_1) \vee \ldots \vee A_{\mathrm{qf}}(t_n)$ is provable in propositional logic

Proofs: Cut-elimination, epsilon-calculus, functional interpretation…


CL
$\neg\neg A \to A$
IL
Slash
translation
Negative translations
$\bot \to A$
ML
Slash
translation

Negative (Double Negation) Translations

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

Proof in Classical Logic

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

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

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

$$\dfrac{\dfrac{\bot}{\neg\neg(A \vee \neg A)}\,{\to}\mathrm{I},\,\gamma}{\bot}$$

Proof in Intuitionistic Logic

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

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

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

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

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 $a^b \in \mathbb{Q}$

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

$$\downarrow$$

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

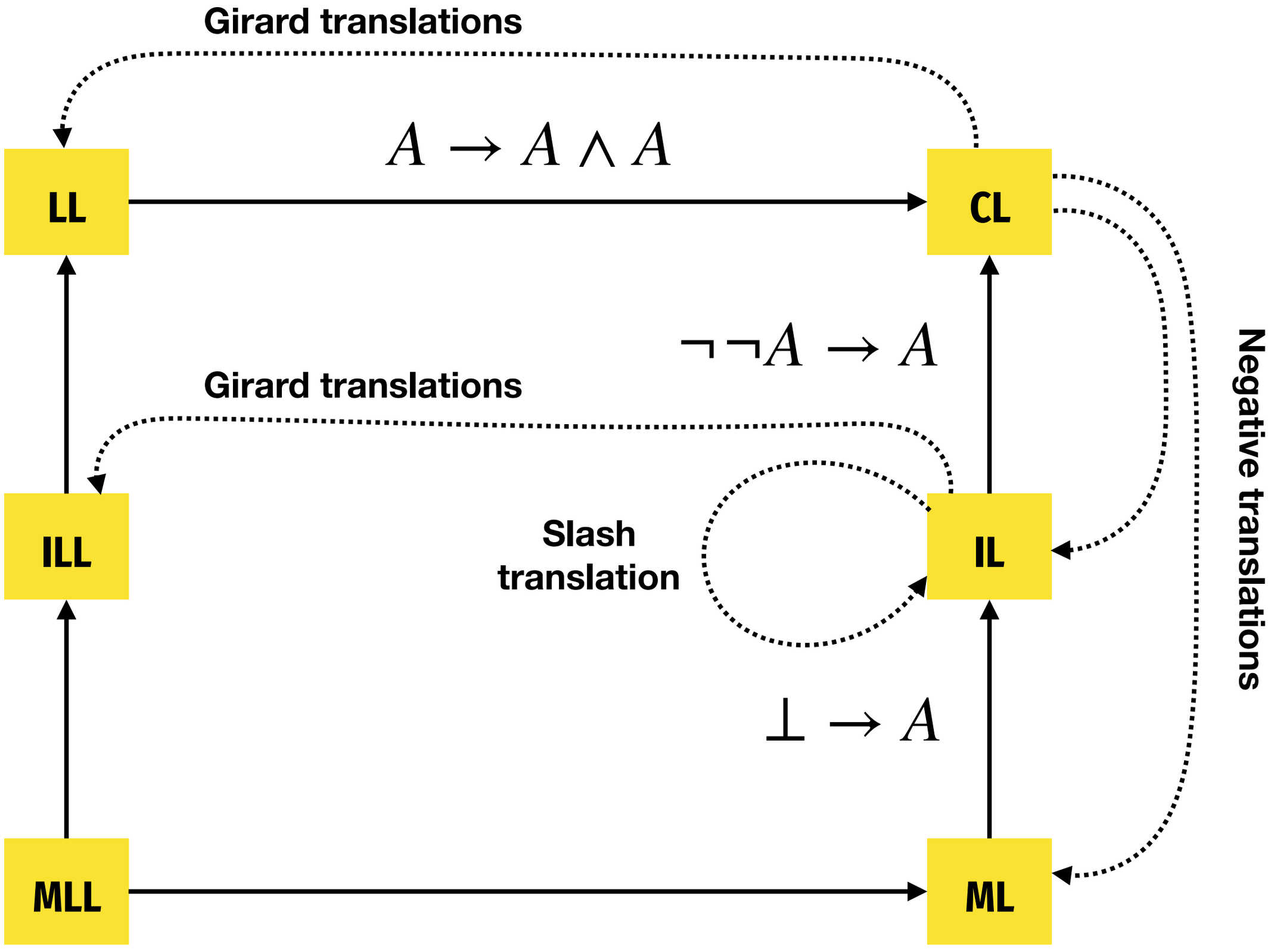
equivalently

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

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

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

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


Girard translations
$A \to A \wedge A$
LL
CL
$\neg\neg A \to A$
Girard translations
Slash
translation
Negative translations
ILL
IL
$\bot \to A$
MLL
ML

Girard Translations

Linear Logic

A refinement of classical and intuitionistic logic

$$A \to B \quad \Rightarrow \quad !A \multimap B$$

$$A \wedge B \quad \Rightarrow \quad A \,\&\, B \quad \text{or} \quad A \otimes B$$

call-by-name translation

$$
\begin{array}{lcl}
(A \wedge B)^{*} & \equiv & A^{*} \,\&\, B^{*} \\
(A \vee B)^{*} & \equiv & !A^{*} \oplus !B^{*} \\
(A \to B)^{*} & \equiv & !A^{*} \multimap B^{*} \\
(\forall z\, A)^{*} & \equiv & \forall z\, A^{*} \\
(\exists z\, A)^{*} & \equiv & \exists z !A^{*}
\end{array}
$$

call-by-value translation

$$
\begin{array}{lcl}
(A \wedge B)^{\circ} & \equiv & A^{\circ} \otimes B^{\circ} \\
(A \vee B)^{\circ} & \equiv & A^{\circ} \oplus B^{\circ} \\
(A \to B)^{\circ} & \equiv & !(A^{\circ} \multimap B^{\circ}) \\
(\forall z\, A)^{\circ} & \equiv & !\forall z\, A^{\circ} \\
(\exists z\, A)^{\circ} & \equiv & \exists z\, A^{\circ}
\end{array}
$$

$$
\mathrm{IL} \vdash A \quad \Rightarrow \quad \mathrm{LL} \vdash A^{\circ} \quad \mathrm{LL} \vdash A^{*}
$$

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

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

Tomorrow…

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