Logic for Computer Science

Summer semester
2019-2020

LECTURE 4: INTUTIONISTIC PROPOSITIONAL LOGIC

Lectures: LORENZO CLEMENTE
Tutorials: DARIA WALUKIEWICZ, JACEK CHRZASZCZ, JĘDRZEJ KOŁODZIEJSKI
Labs: DARIA, JACEK + PIOTR HOFMAN

PLAN

- Motivating examples.
- Brouwer-Heyting-Kolmogorov interpretation of $\to, \wedge, \vee, \neg, \bot$.
- Gentzen's natural deduction.
- Curry-Howard correspondence.
- Intuitionistic Tautology is PSPACE-complete.
- Models of propositional intuitionistic logic
- Glivenko's double-negation translation
- Disjunction property
- Rieger-Nishimura lattice

no proofs

CLASSICAL MOTIVATING EXAMPLE

Statement: $\boxed{\text{There are irrational numbers } a, b \in \mathbb{R} \setminus \mathbb{Q} \text{ s.t. } a^b \in \mathbb{Q} \text{ is rational.}}$

Proof: Consider $x = \sqrt{2}^{\sqrt{2}} \in \mathbb{R}$. There are two cases:

1) $x \in \mathbb{Q}$. Then we are done since $a = b = \sqrt{2} \notin \mathbb{Q}$.

2) $x \notin \mathbb{Q}$. Then take $a = x$, $b = \sqrt{2}$. Thus, $a^b = 2 \in \mathbb{Q}$.

which a, b??

NONCONSTRUCTIVE ARGUMENT!

Law of excluded middle (LEM):

$$\underbrace{x \in \mathbb{Q}}_{P} \vee \underbrace{x \notin \mathbb{Q}}_{\neg P}$$

CLASSICAL LOGIC vs INTUITIONISTIC LOGIC

	Classical logic	Intuitionistic logic
Philosophy :	Platonic/Idealistic	Man-made
Focus :	Semantics (truth)	Constructive proof
Logical connectives :	Defined by truth tables	Operate on proofs

via

BROWER - HEYTING - KOLMOGOROV interpretation

BROWER - HEYTING - KOLMOGOROV interpretation

Write $p : \varphi$ if p is a proof of φ.

$p : \varphi \wedge \psi$ implies $p = (q, r)$, $q : \varphi$, $r : \psi$.

$p : \varphi \vee \psi$ implies $p = (b, q)$ where either
$b = 0$ and $q : \varphi$, or $b = 1$ and $q : \psi$.

$p : \varphi \to \psi$ implies p is a computable function
mapping every $q : \varphi$ to $p(q) : \psi$.

$p : \bot$ is impossible.

$$\boxed{\neg \varphi \equiv \varphi \to \bot}$$

NATURAL DEDUCTION for $\{\to\}$

A **sequent** is a pair $\Gamma \vdash \varphi$ derivable according to the rules below:

set of formulas

WARNING!

overloaded, nothing to do with the "provability relation" from Hilbert's proof system

Axiom:
$$\frac{}{\Gamma, \varphi \vdash \varphi}\ (Ax)$$

Introduction rule:
$$\frac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \to \psi}\ (\to I)$$

≈ deduction theorem

eliminated formula

Elimination rules:
$$\frac{\Gamma \vdash \varphi \qquad \Gamma \vdash \varphi \to \psi}{\Gamma \vdash \psi}\ (\to E)$$

≈ modus ponens

EXAMPLES of proofs trees with natural deduction

$$\dfrac{\dfrac{\dfrac{}{\varphi, \psi \vdash \varphi}\,(Ax)}{\varphi \vdash \psi \to \varphi}\,(\to I)}{\vdash \underbrace{\varphi \to \psi \to \varphi}_{A1}}\,(\to I)$$

from Hilbert's proof system

EXAMPLES of proofs trees with natural deduction

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma \vdash \varphi \to \psi \to \theta}\,(Ax) \qquad \dfrac{}{\Gamma \vdash \varphi}\,(Ax)}{\Gamma \vdash \psi \to \theta}\,(\to E) \qquad \dfrac{\dfrac{}{\Gamma \vdash \varphi \to \psi}\,(Ax) \qquad \dfrac{}{\Gamma \vdash \varphi}\,(Ax)}{\Gamma \vdash \psi}\,(\to E)}{\Gamma := \{\varphi \to \psi \to \theta,\ \varphi \to \psi,\ \varphi\} \vdash \theta}\,(\to E)}{\varphi \to \psi \to \theta,\ \varphi \to \psi \vdash \varphi \to \theta}\,(\to I)}{\varphi \to \psi \to \theta \vdash (\varphi \to \psi) \to \varphi \to \theta}\,(\to I)}{\underbrace{\vdash (\varphi \to \psi \to \theta) \to (\varphi \to \psi) \to \varphi \to \theta}_{A2}}\,(\to I)}{}
$$

from Hilbert's proof system

This proof is **normal**: No $(\to I)$ followed by $(\to E)$ (introduced formulas are not removed later)

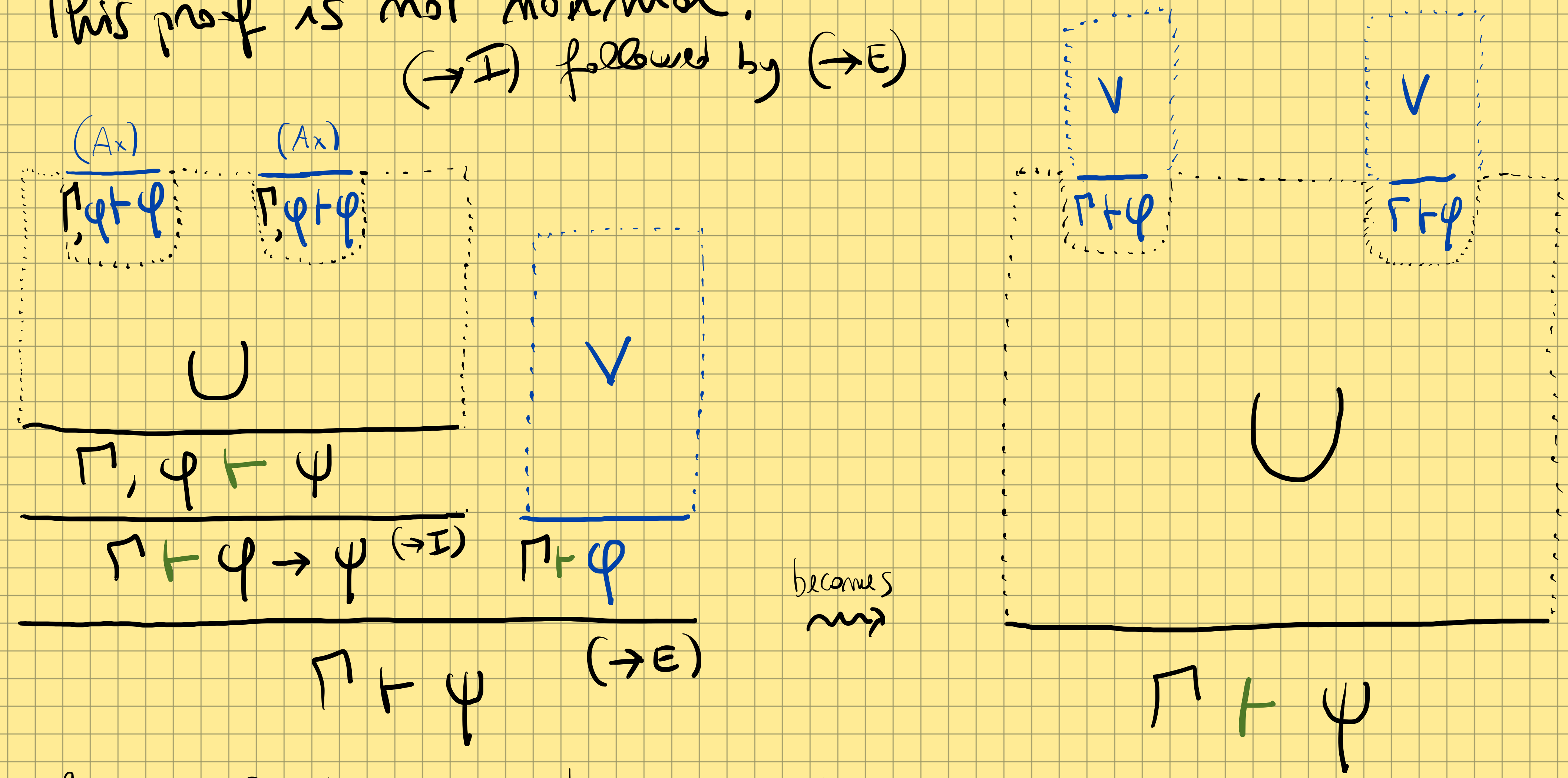
EXAMPLE of NON-NORMAL PROOF

$$
\dfrac{
  (\to I)\ \dfrac{(Ax)\ \dfrac{}{\Gamma, \varphi \vdash \varphi}}{\Gamma \vdash \varphi \to \varphi}
  \qquad
  \dfrac{\vdots}{\Gamma \vdash \varphi}
}{\Gamma \vdash \varphi}\ (\to E)
$$

not normal

NORMALIZATION of PROOFS

This proof is not normal: (→I) followed by (→E)



- The proof becomes bigger, but simpler
- This endows proofs with a computational aspect...

let's keep this in mind...

SIMPLY-TYPED λ-CALCULUS

Terms: variable | λ-abstraction | application

$$U, V ::= x \mid \lambda x . U \mid U\,V$$

Simple types: type variable | function type

$$\alpha, \beta ::= a \mid \alpha \to \beta$$

Typing rules:

Typing judgment

(at most one occurrence of $x:\alpha$ for every x)

$$\frac{}{\Gamma, x:\alpha \vdash x:\alpha}\ (Ax)$$

$$\frac{\Gamma, x:\alpha \vdash U:\beta}{\Gamma \vdash \lambda x . U : \alpha \to \beta}\ (\to I)$$

$$\frac{\Gamma \vdash U : \alpha \to \beta \qquad \Gamma \vdash V : \alpha}{\Gamma \vdash U\,V : \beta}\ (\to E)$$

$$\frac{\Gamma \vdash U : \bot}{\Gamma \vdash V : \alpha}\ (\bot E)$$

EXAMPLES of typing derivations

$$
\dfrac{\dfrac{\dfrac{}{x:\alpha,\ y:\beta \vdash x:\alpha}\ (Ax)}{x:\alpha \vdash \lambda y\cdot x : \beta \to \alpha}\ (\to I)}{\vdash \underbrace{\lambda x\cdot \lambda y\cdot x}_{\text{PROOF}} : \underbrace{\alpha \to \beta \to \alpha}_{\text{A1}}}\ (\to I)
$$

PROOF of A1

EXAMPLES of typing derivations

$$
\dfrac{
  \dfrac{
    \dfrac{
      \dfrac{
        \dfrac{
          \dfrac{}{\Gamma \vdash x : \alpha \to \beta \to \gamma}
          \quad
          \dfrac{}{\Gamma \vdash z : \alpha}
        }{\Gamma \vdash xz : \beta \to \gamma}
        \qquad
        \dfrac{
          \dfrac{}{\Gamma \vdash y : \alpha \to \beta}
          \quad
          \dfrac{}{\Gamma \vdash z : \alpha}
        }{\Gamma \vdash yz : \beta}\,(\to E)
      }{\Gamma := \{x : \alpha \to \beta \to \gamma,\ y : \alpha \to \beta,\ z : \alpha\} \vdash xz(yz) : \gamma}\,(\to E)
    }{x : \alpha \to \beta \to \gamma,\ y : \alpha \to \beta \vdash \lambda z \cdot xz(yz) : \alpha \to \gamma}\,(\to I)
  }{x : \alpha \to \beta \to \gamma \vdash \lambda y \lambda z \cdot xz(yz) : (\alpha \to \beta) \to \alpha \to \gamma}\,(\to I)
}{\vdash \underbrace{\lambda x \lambda y \lambda z \cdot xz(yz)}_{\text{PROOF}} \underset{\text{of}}{:} \underbrace{(\alpha \to \beta \to \gamma) \to (\alpha \to \beta) \to \alpha \to \gamma}_{\text{A2}}}\,(\to I)
$$

NORMALIZATION of λ-terms (dynamics)

EVALUATION

β-reduction

$$(\lambda x . u)\ v \longrightarrow_\beta u[x \mapsto v]$$

all free occurrences of x in u are replaced by v (*)

Example: $(\lambda x . x)(\lambda y . y) \longrightarrow_\beta \lambda y . y$

* Conditions apply: Variable renaming may be necessary to prevent free variables of v from becoming bound in $u[x \mapsto v]$

HASKELL WILLIAM A.

CURRY-HOWARD CORRESPONDENCE *

LOGIC		PROGRAMS
Formula φ	$\longleftrightarrow$	Type α
Proof of φ	$\longleftrightarrow$	Program (λ-term) $\quad U : \alpha$
Proof normalization	$\longleftrightarrow$	Evaluation
Validity problem	$\longleftrightarrow$	Type inhabitation
Proof checking	$\longleftrightarrow$	Type reconstruction

* Not an exact correspondence in this presentation:

set

$$\dfrac{\dfrac{\{p\} \vdash p}{\{p\} \vdash p \to p}}{\vdash p \to p \to p}$$

Two possible terms for this proof:

$\lambda x . \lambda y . x$,

$\lambda x . \lambda y . y$

NATURAL DEDUCTION for $\{\to, \bot, \wedge, \vee, \neg\}$

Introduction rules

$$\frac{}{\Gamma, \varphi \vdash \varphi}\,(Ax) \qquad \frac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \to \psi}\,(\to I)$$

$$\frac{\Gamma \vdash \varphi \quad \Gamma \vdash \psi}{\Gamma \vdash \varphi \wedge \psi}\,(\wedge I)$$

$$\frac{\Gamma \vdash \varphi}{\Gamma \vdash \varphi \vee \psi}\,(\vee I_L) \qquad \frac{\Gamma \vdash \psi}{\Gamma \vdash \varphi \vee \psi}\,(\vee I_R)$$

Elimination rules

$$\frac{\Gamma \vdash \varphi \quad \Gamma \vdash \varphi \to \psi}{\Gamma \vdash \psi}\,(\to E)$$

$$\frac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \varphi}\,(\wedge E_L) \qquad \frac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \psi}\,(\wedge E_R)$$

$$\frac{\Gamma \vdash \varphi \vee \psi \quad \Gamma, \varphi \vdash \theta \quad \Gamma, \psi \vdash \theta}{\Gamma \vdash \theta}\,(\vee E)$$

proof by cases

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash \varphi}\,(\bot E)$$

miracle rule!

ex falso sequitur quodlibet

EXTENDED SIMPLY-TYPED λ-CALCULUS

$\alpha, \beta ::= a \mid \alpha \to \beta \mid \alpha \overset{\wedge}{\times} \beta$ (product) $\mid \alpha \overset{\vee}{+} \beta$ (Tagged union) $\mid \perp$

$U, V ::= x \mid \lambda x . U \mid U\,V \mid (U, V) \mid \pi_1 U \mid \pi_2 V \mid \text{case } U \text{ of } V_1[x_1] \text{ or } V_2[x_2] \mid in_1\, U \mid in_2\, U \mid \mathcal{E}(U)$

pairing projections conditional injections miracle

$$\frac{}{\Gamma, x:\alpha \vdash x:\alpha}\,(Ax) \qquad \frac{\Gamma, x:\alpha \vdash U:\beta}{\Gamma \vdash \lambda x . U : \alpha \to \beta}\,(\to I) \qquad \frac{\Gamma \vdash U:\alpha \to \beta \quad \Gamma \vdash V:\alpha}{\Gamma \vdash U\,V : \beta}\,(\to E) \qquad \frac{\Gamma \vdash U:\perp}{\Gamma \vdash \mathcal{E}(U):\alpha}\,(\perp E)$$

$$\frac{\Gamma \vdash U:\alpha \quad \Gamma \vdash V:\beta}{\Gamma \vdash (U, V):\alpha \times \beta}\,(\times I) \qquad \frac{\Gamma \vdash U:\alpha \times \beta}{\Gamma \vdash \pi_1 U : \alpha}\,(\times E_L) \qquad \frac{\Gamma \vdash U:\alpha \times \beta}{\Gamma \vdash \pi_2 U : \beta}\,(\times E_R)$$

$$\frac{\Gamma \vdash U:\alpha}{\Gamma \vdash in_1(U) : \alpha + \beta}\,(+I_1)$$

$$\frac{\Gamma \vdash U:\beta}{\Gamma \vdash in_2(U) : \alpha + \beta}\,(+I_2)$$

$$\frac{\Gamma \vdash U:\alpha+\beta \quad \Gamma, x_1:\alpha \vdash V_1:\gamma \quad \Gamma, x_2:\beta \vdash V_2:\gamma}{\Gamma \vdash \text{case } U \text{ of } V_1[x_1] \text{ or } V_2[x_2]}\,(+E)$$

NORMALIZATION of EXTENDED λ-terms

$$(\lambda x. u)\, v \twoheadrightarrow_\beta u[x \mapsto v]$$

$$\pi_1(u, v) \twoheadrightarrow_\beta u$$

$$\pi_2(u, v) \twoheadrightarrow_\beta v$$

$$\text{case } in_1(u) \text{ of } v_1[x_1] \text{ or } v_2[x_2] \twoheadrightarrow_\beta v_1[x_1 \mapsto u]$$

$$\text{case } in_2(u) \text{ of } v_1[x_1] \text{ or } v_2[x_2] \twoheadrightarrow_\beta v_2[x_2 \mapsto u]$$

DISJUNCTION PROPERTY for IPL

$$\boxed{\text{Theorem: } \Gamma \vdash_{ND} \varphi \vee \psi \text{ implies } \Gamma \vdash_{ND} \varphi \text{ or } \Gamma \vdash_{ND} \psi}$$

Proof omitted (follows from the existence of normal proofs).

Clearly fails for classical logic:

$\vdash_H p \vee \neg p$ but neither $\vdash_H p$ nor $\vdash \neg p$.

TAUTOLOGY for IPL is PSPACE-complete

intuitionistic propositional logic

c.f. coNP-completeness for classical logic.

PSPACE-hardness : Reduction from QBF ∈ PSPACE-hard [Statman '79].

(in fact, PSPACE-complete)

$$\underbrace{\forall p \underbrace{\exists q \cdot \underbrace{\varphi}_{x_0}}_{x_1}}_{x_2} \quad \overset{\text{becomes}}{\rightsquigarrow} \quad (x_0 \leftrightarrow \underbrace{\neg\neg\varphi}_{\varphi}) \to (x_1 \leftrightarrow \underbrace{((q \to x_0) \vee (\neg q \to x_0))}_{\exists q}) \to (x_2 \leftrightarrow (\underbrace{(p \vee \neg p)}_{\forall p} \to x_1)) \to x_2$$

PSPACE-membership (Ben Yelles - Wajsberg algorithm): $\Gamma \vdash_{ND} \varphi$?

$\varphi \in \{p, \bot\}$: Choose $\varphi_1 \to \cdots \to \varphi_n \to \varphi \in \Gamma$, check $\Gamma \vdash \varphi_1$ and ... $\Gamma \vdash \varphi_n$.

$\varphi \equiv \psi \wedge \theta$: check $\Gamma \vdash \psi$ and $\Gamma \vdash \theta$.

$\varphi \equiv \psi \vee \theta$: check $\Gamma \vdash \psi$ or $\Gamma \vdash \theta$ (by the disjunction property)

$\varphi \equiv \psi \to \theta$: check $\Gamma, \psi \vdash \theta$.

Alternating PTIME = PSPACE algorithm :
- existential choice.
- universal choice.
- quadratic recursion depth.

NATURAL DEDUCTION for CLASSICAL LOGIC

Additional rule: $$\frac{\Gamma, \neg\varphi \vdash \bot}{\Gamma \vdash \varphi} \ (\text{⚡})$$ (proof by contradiction)

THEOREM. $\underbrace{\Gamma \vdash_H \varphi}_{\text{provable in Hilbert's proof system}}$ iff $\underbrace{\Gamma \vdash_{ND} \varphi}_{\text{provable in natural deduction}}$

double negation $\neg\neg\varphi \to \varphi$

Proof of "$\Rightarrow$": We showed A1, A2 are derivable in ND.
MP is $(\to E)$. It remains to derive A3 (next slide).

Proof of "$\Leftarrow$": It suffices to show that ND rules are sound (they preserve the semantics):

$\Gamma \vdash_{ND} \varphi$ implies $\Gamma \models \varphi$.

Conclude by completeness of $\vdash_H$ wrt $\models$.

PROOF of A3

in natural deduction

$$\dfrac{}{\Gamma_2, \neg\neg\varphi \vdash \varphi}\ (\mathrm{Ax})$$

$$\dfrac{\Gamma_2, \neg\neg\varphi \vdash \varphi}{\Gamma_2 \vdash \neg\neg\varphi \to \varphi}\ (\to I)$$

$$\dfrac{\dfrac{}{\Gamma_2 \vdash (\neg\neg\varphi \to \varphi) \to \bot}\ (\mathrm{Ax}) \qquad \Gamma_2 \vdash \neg\neg\varphi \to \varphi}{\Gamma_2 := \Gamma_1, \varphi \vdash \bot}\ (\to E)$$

$$\dfrac{\Gamma_2 := \Gamma_1, \varphi \vdash \bot}{\Gamma_1 \vdash \neg\varphi}\ (\to I)$$

$$\dfrac{\dfrac{}{\Gamma_1 \vdash \neg\varphi \to \bot}\ (\mathrm{Ax}) \qquad \Gamma_1 \vdash \neg\varphi}{\Gamma_1 \vdash \bot}\ (\to E)$$

$$\dfrac{\Gamma_1 \vdash \bot}{\Gamma_1 := \Gamma_0, \neg\neg\varphi \vdash \varphi}\ (\bot E)$$

$$\dfrac{\Gamma_1 := \Gamma_0, \neg\neg\varphi \vdash \varphi}{\Gamma_0 \vdash \neg\neg\varphi \to \varphi}\ (\to I)$$

$$\dfrac{\dfrac{}{\Gamma_0 \vdash (\neg\neg\varphi \to \varphi) \to \bot}\ (\mathrm{Ax}) \qquad \Gamma_0 \vdash \neg\neg\varphi \to \varphi}{\Gamma_0 := \neg(\neg\neg\varphi \to \varphi) \vdash \bot}\ (\to E)$$

This proof is intuitionistically valid

$$\dfrac{\Gamma_0 := \neg(\neg\neg\varphi \to \varphi) \vdash \bot}{\vdash \neg\neg\varphi \to \varphi}\ (↯)$$

A3

the only non-intuitionistic step

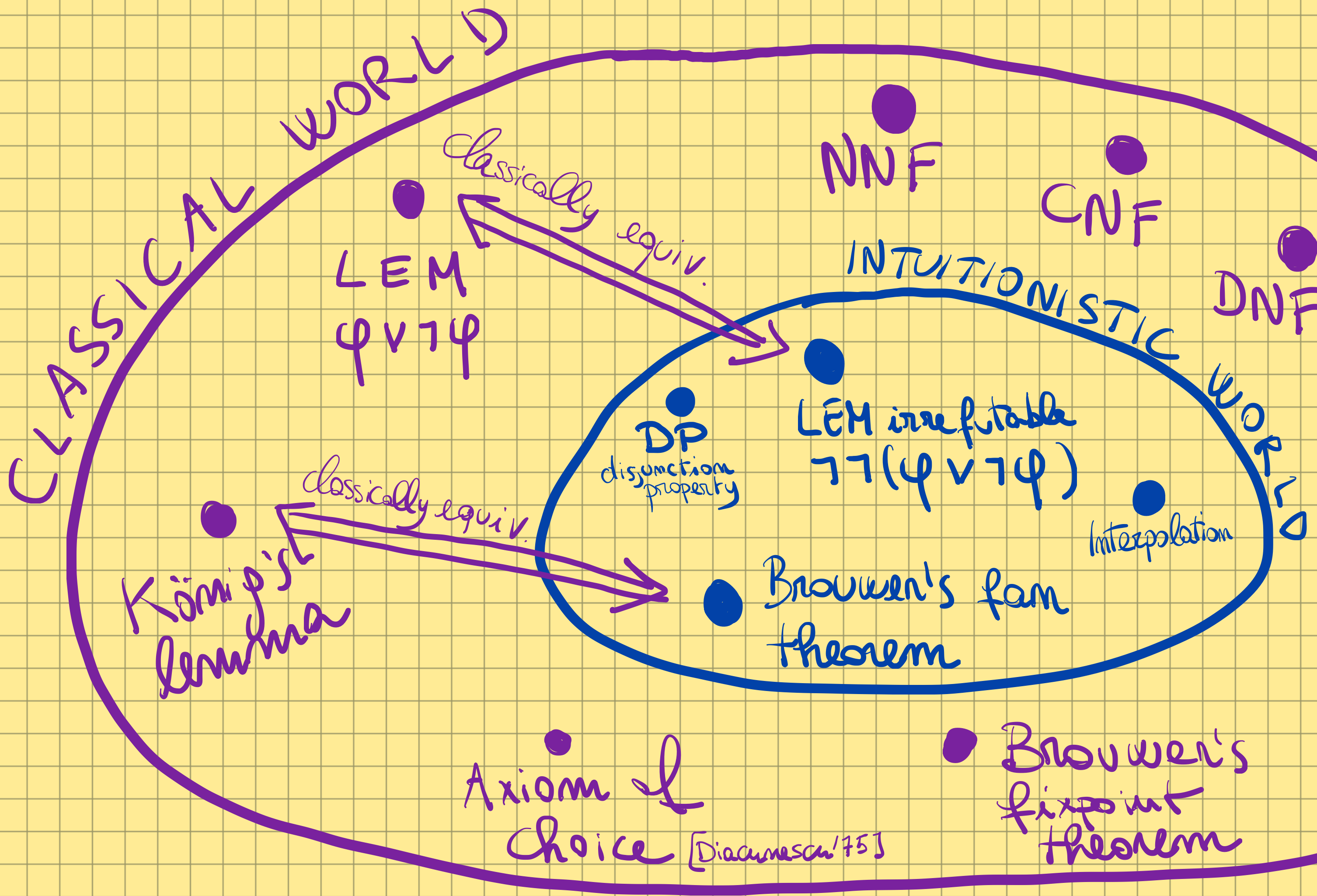
GLIVENKO'S THEOREM 1929 for propositional logic

Double-negation encoding of classical propositional logic into intuitionistic propositional logic:

φ is a classical propositional tautology iff $\neg\neg\varphi$ is an intuitionistic propositional tautology

CLASSICAL vs INTUITIONISTIC logic

- Intuitionistic logic is a conservative extension of classical logic: $\Gamma \vdash_{ND} \varphi$ implies $\Gamma \vdash_{H} \varphi$.



MODELS for Intuitionistic Propositional Logic

- The primary focus in intuitionistic logic is proof.
- Models exist, but come as an afterthought.
- Examples:
  - Heyting algebras
  - Kripke structures
  - Topological models
  - Cartesian-closed categories

One can prove a corresponding completeness result, i.e.,

$$\Gamma \models_{\text{Heyting}} \varphi \implies \Gamma \vdash_{ND} \varphi,$$

but only classical proofs are known*!

* The are more complex models for which an intuitionistic proof of completeness is known [Veldman'76]

RIEGER-NISHIMURA lattice for 1-IPL

VARIABLE

Fix a simple propositional variable p.

$\varphi_0 \equiv p \wedge \neg p$ (equivalent to $\bot$)

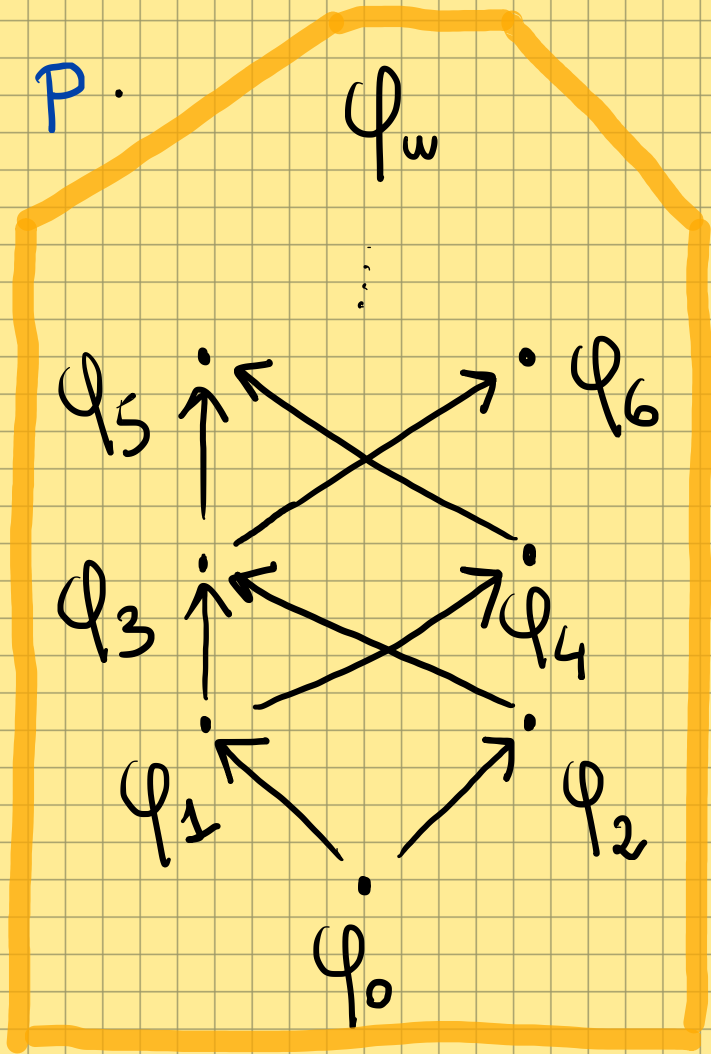
$\varphi_1 \equiv p$

$\varphi_2 \equiv \neg p$

$\varphi_{2n+3} \equiv \varphi_{2n+1} \vee \varphi_{2n+2}$

$\varphi_{2n+4} \equiv \varphi_{2n+3} \to \varphi_{2n+1}$

$\varphi_\omega \equiv p \to p$



1) Infinitely many inequivalent formulas over p.

2) Every φ over p is equivalent to some φ_n.