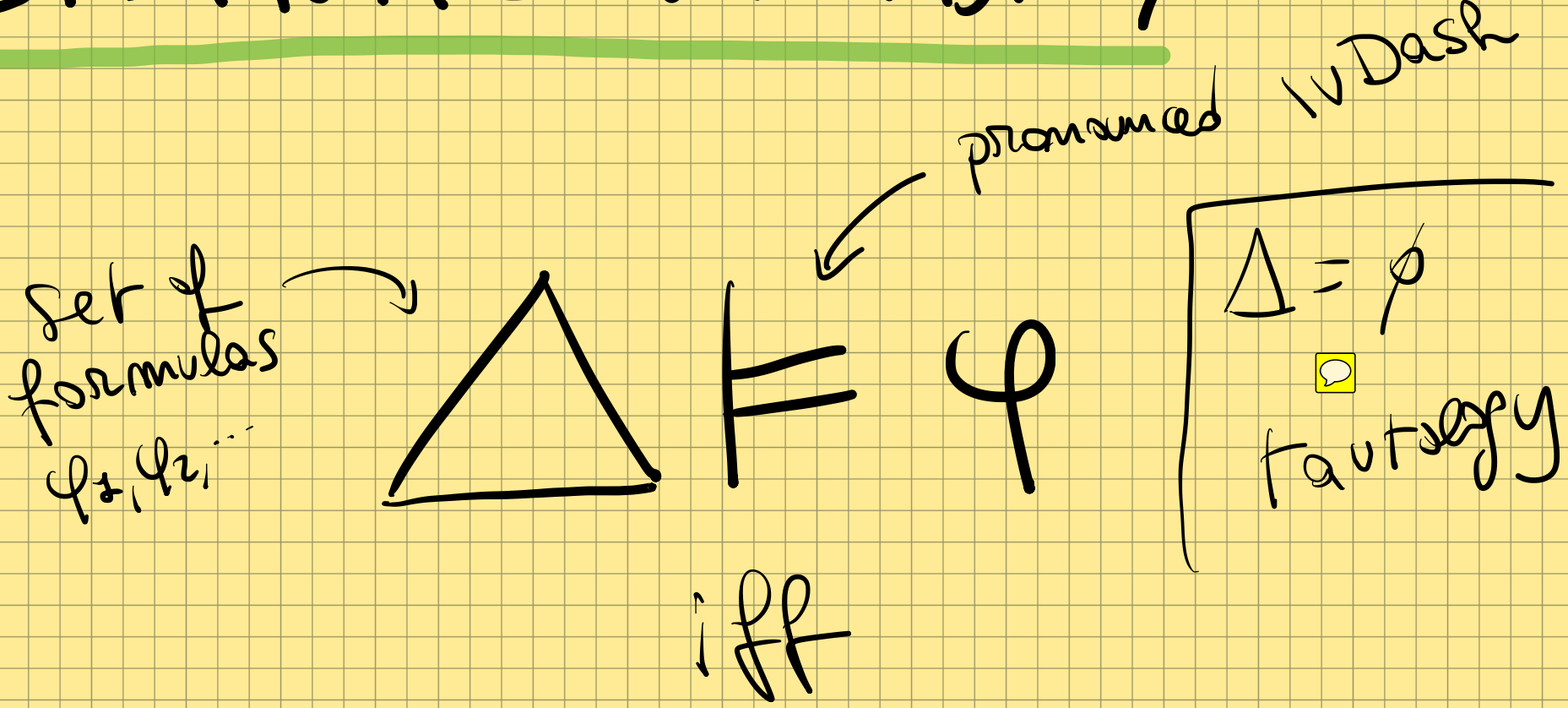
Logic for Computer Science

Summer Semester
2019-2020

LECTURE 2

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

SEMANTIC VALIDITY



for every truth valuation $\rho : \{\varphi_1, \varphi_2, \ldots\} \to \{0, 1\}$,

if $\left(\forall \varphi_i \in \Delta \cdot [\![\varphi_i]\!]\rho = 1\right)$, then $[\![\varphi]\!]\rho = 1$

FOUR EASY PIECES ON "⊨"

1) Semantic deduction theorem (P1.1.3):

$\Delta \cup \{\varphi\} \models \psi$ iff $\Delta \models \varphi \to \psi$

2) Monotonicity (P1.1.6):

$\Delta \models \varphi$ and $\Delta \subseteq \Gamma$ implies $\Gamma \models \varphi$

3) Strong soundness of Modus Ponens:

$\{\varphi, \varphi \to \psi\} \models \psi$

4) Soundness of substitution (P1.1.5):

$\models \varphi$ implies $\models \varphi[p \mapsto \psi]$. Strongly sound?

LESS EASY PIECE: COMPACTNESS

there is a valuation ρ s.t. $\forall \varphi \in \Delta \cdot [\![\varphi]\!]_\rho = 1$

Δ is satisfiable

iff

every finite $\Gamma \subseteq_{fin} \Delta$ is satisfiable

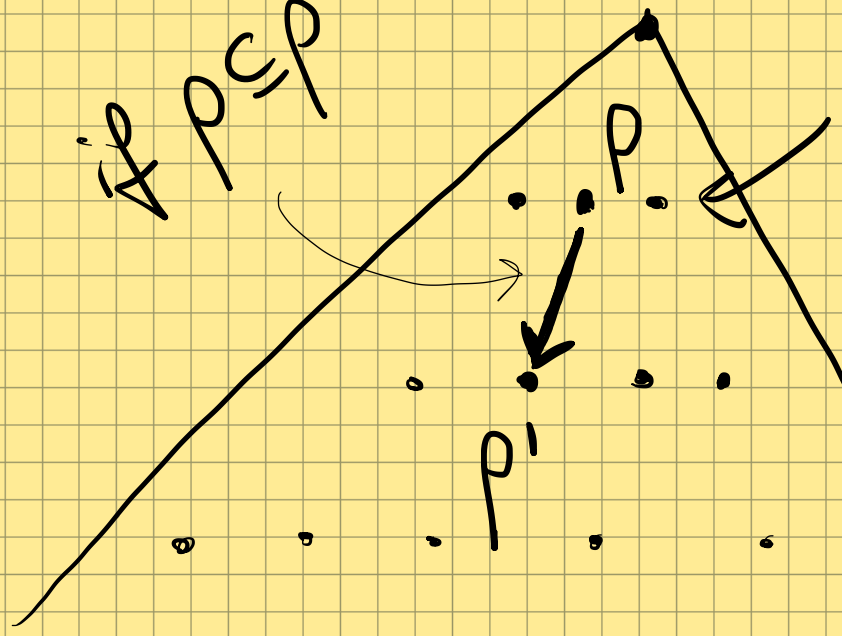
(Δ is finitely satisfiable)

KÖNIG'S LEMMA ⇒ COMPACTNESS

Assume $\Delta = \{\varphi_1, \varphi_2, \dots\}$ is finitely satisfiable.

Then also $\Gamma = \{\psi_0, \psi_1, \dots\}$ " " ".

where $\psi_n \equiv \varphi_1 \wedge \dots \wedge \varphi_n$ (thus $Var(\varphi_n) \subseteq Var(\varphi_{n+1})$)



at level n there are all $\rho : Var(\varphi_n) \to \{0,1\}$ s.t. $[\![\varphi_n]\!]\rho = 1$

1) The tree is infinite
2) is finitely branching

$\Rightarrow \rho_0 \rho_1 \dots$. Take $\rho_\omega = \bigcup_n \rho_n$

COMPACTNESS: TUTORIALS

P 1.5.1: König's lemma $\Rightarrow$ Compactness.

P 1.5.2: Compactness $\Rightarrow$ König's lemma.

P 1.5.3: De Bruijn - Erdős' theorem
(an infinite graph is k-colourable
iff every finite subgraph thereof is so).

P 1.8.8: Weak completeness $\Rightarrow$ strong completeness.

... and other applications ...

HOW TO PROVE VALIDITY?

Let φ have propositional variables $p_1, \dots, p_k$.

$\models \varphi$ holds iff $\underbrace{\forall \rho}_{2^k \text{ valuations!}} . [\![\varphi]\!]\rho = 1$

Validity of propositional formulas is coNP-complete in general.

We need a method that can "get lucky".

HILBERT'S PROOF SYSTEM (propositional logic)

We consider the minimal set of connectives $\{\to, \bot\}$
(we saw in P1.2.3 that it is expressively complete)

A1: $\varphi \to \psi \to \varphi$

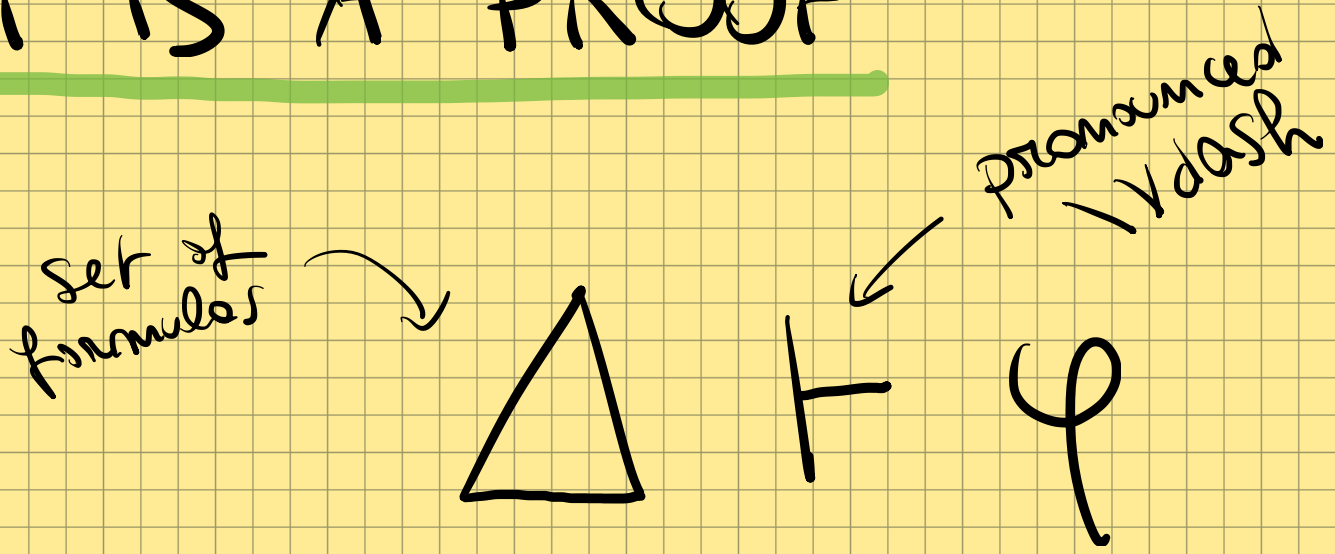
A2: $(\varphi \to \psi \to \theta) \to (\varphi \to \psi) \to \varphi \to \theta$

A3: $\neg\neg\varphi \to \varphi$ (where $\neg\varphi \equiv \varphi \to \bot$)

} axiom schemes

MP: $\dfrac{\varphi \to \psi \quad \varphi}{\psi}$ } inference rule MODUS PONENS

WHAT IS A PROOF



iff

$\exists\, \varphi_1, \ldots, \varphi_n \equiv \varphi$ omol

each φ_i : either φ_i is A_1, A_2, A_3,

or $\varphi_i \in \Delta$,

or $\dfrac{\varphi_k \quad \varphi_j}{\varphi_i}$ by MP $k, j < i$

PROOF EXAMPLE

$$\begin{cases} A1: \varphi \to \psi \to \varphi \\ A2: (\varphi \to \psi \to \theta) \to (\varphi \to \psi) \to \varphi \to \theta \\ A3: \neg\neg\varphi \to \varphi \end{cases}$$

$\vdash \varphi \to \varphi$:

1. $\varphi \to \varphi \to \varphi$ (A1)
2. $\varphi \to (\varphi \to \varphi) \to \varphi$ (A1)
3. $(\varphi \to (\varphi \to \varphi) \to \varphi) \to (\varphi \to \varphi \to \varphi) \to \varphi \to \varphi$
4. $(\varphi \to \varphi \to \varphi) \to \varphi \to \varphi$ (MP 2,3) (A2)
5. $\varphi \to \varphi$ (MP 1,4)

DEDUCTION THEOREM (for propositional logic)

$$\Delta \vdash \varphi \to \psi \quad \text{iff} \quad \Delta \cup \{\varphi\} \vdash \psi$$

($\Leftarrow$) we have a proof $\psi_1, \psi_2, \dots, \psi_n \equiv \psi$.
one can prove $\Delta \vdash \varphi \to \psi_i$ (by ind. on i).

($\Rightarrow$) straightforward (by (MP) at the end).

PROOF EXAMPLE (Alternative argument using the Deduction Theorem)

$\vdash \varphi \to \varphi$

We have $\varphi \vdash \varphi$ (by definition of "$\vdash$")

Apply the Deduction theorem.

SOUNDNESS of HILBERT'S SYSTEM

$\Delta \vdash \varphi$ implies $\Delta \models \varphi$

[Meta] Proof (by induction on the length of proofs)

Base $n = 1$: $\pi = \varphi_1$. Then φ_1 is an axiom (truth tables)

Inductive step $n \geq 2$: $\pi = \varphi_1, \dots, \varphi_{n-1}, \varphi_n$

Cases: 1) φ_n is an axiom ✓ 2) $\varphi_n \in \Delta$ ✓

3) MP $\dfrac{\varphi_i \quad \varphi_j}{\varphi_n}$ $(i, j < n)$. By IH, $\Delta \models \{\varphi_i, \varphi_j\}$.

By Strong soundness of MP, $\Delta \models \varphi_n$.

COMPLETENESS of HILBERT'S SYSTEM

$\Delta \models \varphi$ implies $\Delta \vdash \varphi$

- Conceptually much harder!
  It requires us to understand what a proof is.
- Weak completeness: $\Delta = \emptyset$.

(Tutorials: weak completeness $\Rightarrow$ completeness)

TOWARDS COMPLETENESS

We will use the following facts.

(B1) $\vdash \varphi \to \varphi$ (already proved)

(B2) $\vdash \varphi \to \neg\neg\varphi$ $\qquad \neg\varphi \equiv \varphi \to \bot$

(B3) $\vdash \neg\varphi \to (\varphi \to \psi)$

(B4) $\vdash (\varphi \to \psi) \to ((\neg\varphi \to \psi) \to \psi)$

(B5) $\vdash \varphi \to (\neg\psi \to \neg(\varphi \to \psi))$

$$\varphi^\rho \equiv \begin{cases} \varphi & \text{if } [\![\varphi]\!]_\rho = 1, \\ \neg\varphi & \text{otherwise.} \end{cases} \qquad \text{and} \qquad \mathrm{Var}(\varphi) = \{q_1, \dots, q_m\}$$

CORE LEMMA : $\{q_1^\rho, \dots, q_m^\rho\} \vdash \varphi^\rho$

Proof by structural induction on φ.

Base case $\varphi \equiv q_i$. There are two subcases:

1) $\rho(q_i) = 1$: $\varphi^\rho \equiv \varphi \equiv q_i$, $q_i^\rho \equiv q_i$.

By (B1), $\vdash q_i \to q_i$.

By the Deduction Theorem, $\underbrace{q_i}_{q_i^\rho} \vdash \underbrace{q_i}_{\varphi^\rho}$.

$$\varphi^\rho \equiv \begin{cases} \varphi & \text{if } [\![\varphi]\!]_\rho = 1, \\ \neg\varphi & \text{otherwise.} \end{cases} \qquad \text{and} \qquad Var(\varphi) = \{q_1, \dots, q_n\}$$

CORE LEMMA : $\{q_1^\rho, \dots, q_n^\rho\} \vdash \varphi^\rho$

Proof by structural induction on φ.

Base case $\varphi \equiv q_i$. There are two subcases:

2) $\rho(q_i) = 0 : \varphi^\rho \equiv \neg\varphi \equiv \neg q_i \equiv q_i^\rho$.

$\neg q_i \vdash \neg q_i$ as in the previous case.

$$\varphi^\rho \equiv \begin{cases} \varphi & \text{if } [\![\varphi]\!]_\rho = 1, \\ \neg\varphi & \text{otherwise.} \end{cases} \qquad \text{and} \qquad Var(\varphi) = \{q_1, \dots, q_n\}$$

CORE LEMMA : $\{q_1^\rho, \dots, q_n^\rho\} \vdash \varphi^\rho$

Proof by structural induction on φ.

Inductive step $\varphi \equiv \neg\psi$. Two subcases:

1) $\rho(\psi) = 1$. $\varphi^\rho \equiv \neg\varphi \equiv \neg\neg\psi$, $\psi^\rho = \psi$.

By the inductive assumption, $\{q_1^\rho, \dots, q_n^\rho\} \vdash \psi$

By (B2), $\vdash \psi \to \neg\neg\psi$. By (MP), $\{q_1^\rho, \dots, q_n^\rho\} \vdash \neg\neg\psi$.

$$\varphi^\rho \equiv \begin{cases} \varphi & \text{if } [\![\varphi]\!]_\rho = 1, \\ \neg\varphi & \text{otherwise.} \end{cases} \qquad \text{and} \qquad Var(\varphi) = \{q_1, \dots, q_m\}$$

CORE LEMMA : $\{q_1^\rho, \dots, q_m^\rho\} \vdash \varphi^\rho$

Proof by structural induction on φ.

Inductive step $\varphi \equiv \neg\psi$. Two subcases:

2) $\rho(\psi) = 0$. $\varphi^\rho \equiv \varphi \equiv \neg\psi \equiv \psi^\rho$.

By the inductive assumption, $\{q_1^\rho, \dots, q_m^\rho\} \vdash \neg\psi$.

$$\varphi^\rho \equiv \begin{cases} \varphi & \text{if } [\![\varphi]\!]_\rho = 1, \\ \neg\varphi & \text{otherwise.} \end{cases} \qquad \text{and} \qquad Var(\varphi) = \{q_1, \dots, q_n\}$$

CORE LEMMA : $\{q_1^\rho, \dots, q_n^\rho\} \vdash \varphi^\rho$

Proof by structural induction on φ.

Inductive step $\varphi \equiv \psi \to \theta$. Three subcases:

1) $\rho(\theta) = 1$. $\varphi^\rho \equiv \varphi$, $\theta^\rho \equiv \theta$.

By inductive assumption on θ, $\{q_1^\rho, \dots, q_n^\rho\} \vdash \theta$.

By monotonicity + DT, $\{q_1^\rho, \dots, q_n^\rho\} \vdash \psi \to \theta$.

$$\varphi^\rho \equiv \begin{cases} \varphi & \text{if } [\![\varphi]\!]_\rho = 1, \\ \neg\varphi & \text{otherwise.} \end{cases} \quad \text{and} \quad Var(\varphi) = \{q_1, \dots, q_n\}$$

CORE LEMMA : $\{q_1^\rho, \dots, q_n^\rho\} \vdash \varphi^\rho$

Proof by structural induction on φ.

Inductive step $\varphi \equiv \psi \to \theta$. Three subcases:

2) $\rho(\psi) = 0$. $\varphi^\rho \equiv \varphi$, $\psi^\rho \equiv \neg\psi$.

By inductive assumption on ψ, $\{q_1^\rho, \dots, q_n^\rho\} \vdash \neg\psi$.

By (B3), $\vdash \neg\psi \to \psi \to \theta$. By (MP), $\{q_1^\rho, \dots, q_n^\rho\} \vdash \psi \to \theta$.

$$\varphi^\rho \equiv \begin{cases} \varphi & \text{if } [\![\varphi]\!]_\rho = 1, \\ \neg\varphi & \text{otherwise.} \end{cases} \qquad \text{and} \qquad \mathrm{Var}(\varphi) = \{q_1, \dots, q_m\}$$

CORE LEMMA : $\{q_1^\rho, \dots, q_m^\rho\} \vdash \varphi^\rho$

Proof by structural induction on φ.

Inductive step $\varphi \equiv \psi \to \theta$. Three subcases:

3) $\rho(\psi) = 1$, $\rho(\theta) = 0$. $\varphi^\rho \equiv \neg\varphi$, $\psi^\rho \equiv \psi$, $\theta^\rho \equiv \neg\theta$

By inductive assumption on ψ, θ, $\{q_1^\rho, \dots, q_m^\rho\} \vdash \{\psi, \neg\theta\}$.

By (B5), $\vdash \psi \to \neg\theta \to \neg(\psi \to \theta)$. We conclude by (MP)x2.

PROOF of the WEAK COMPLETENESS THEOREM

$(\models \varphi$ implies $\vdash \varphi)$

Let $Var(\varphi) = \{q_0, \dots, q_{n-1}\}$. We show $\forall\, 0 \leq m \leq n$:

$\forall$ valuation $\rho : \{q_m, \dots, q_{n-1}\} \to \{0,1\}$,

$\{q_m^\rho, \dots, q_{n-1}^\rho\} \vdash \varphi$.

By induction on m.

Base case $m = 0$: It is the core lemma!

PROOF of the WEAK COMPLETENESS THEOREM

$$(\models \varphi \text{ implies } \vdash \varphi)$$

Let $Var(\varphi) = \{q_0, \dots, q_{n-1}\}$. We show $\forall 0 \leq m \leq n$:

$\forall$ valuation $\rho : \{q_m, \dots, q_{n-1}\} \to \{0,1\}$,

$$\{q_m^\rho, \dots, q_{n-1}^\rho\} \vdash \varphi.$$

By induction on m. Induction step $m > 0$.

Let $\rho_0 = \rho[q_{m-1} \mapsto 0]$ and $\rho_1 = \rho[q_{m-1} \mapsto 1]$.

By induction, $\{q_{m-1}^{\rho_0}, \dots, q_{n-1}^{\rho_0}\} \vdash \varphi$ and $\{q_{m-1}^{\rho_1}, \dots, q_{n-1}^{\rho_1}\} \vdash \varphi$.

By the DT, $\{q_m^\rho, \dots, q_{n-1}^\rho\} \vdash \neg q_{m-1} \to \varphi$ and $\{q_m^\rho, \dots, q_{n-1}^\rho\} \vdash q_{m-1} \to \varphi$.

By (B4)+(MP)x2 we are done.

APPLICATIONS & COMPLETENESS

- Weak Completeness implies Strong Completeness
  ($\Vdash \varphi$ implies $\vdash \varphi$) P1.8.8
- Compactness ($\Delta \Vdash \varphi$ implies $\exists \Gamma \subseteq_{fin} \Delta . \Gamma \Vdash \varphi$)

How?

By Completeness $\Delta \vdash \varphi$,
$\exists \Gamma \subseteq_{fin} \Delta . \Gamma \vdash \varphi$, by soundness

VALIDITY PROBLEM

There is a PTIME algorithm for propositional logic iff $P = NP$

Can we hope for a proof system with polynomially long proofs?

There is a polynomial proof system for propositional logic iff $NP = coNP$

INTERPOLATION (for propositional logic)

If $\vdash \varphi \to \psi$, then there is θ s.t. $\vdash \varphi \to \theta$, $\vdash \theta \to \psi$, and $Var(\theta) \subseteq Var(\varphi) \cap Var(\psi)$.

Example: $\vdash p \wedge q \to q \vee r$ interpolant $\theta = q$:

$\vdash p \wedge q \to q$, $\vdash q \to q \vee r$.

Proof: Take $p \in Var(\varphi) \setminus Var(\psi)$.

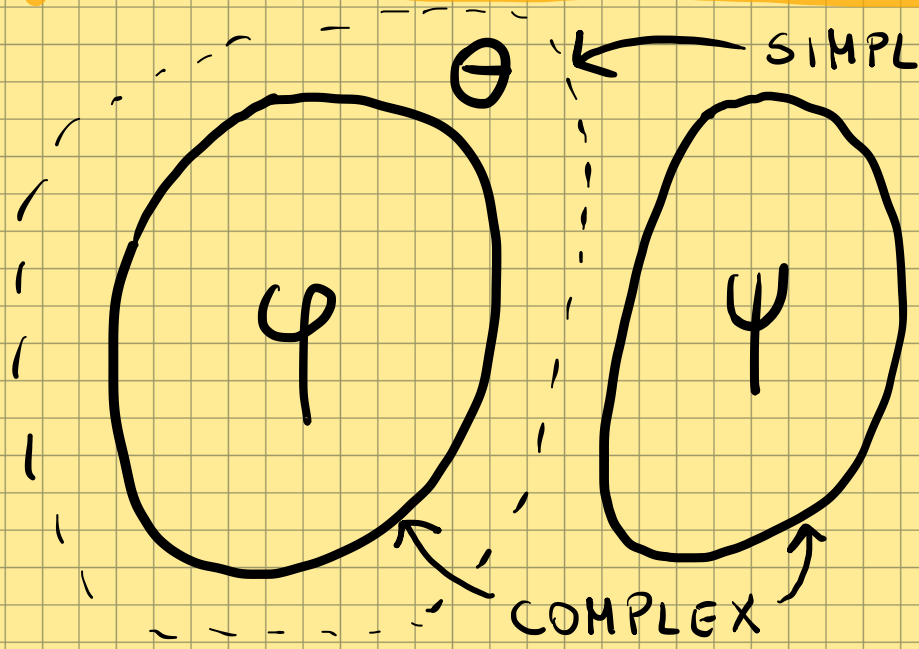
1) $\vdash \varphi \to \varphi[p \mapsto \bot] \vee \varphi[p \mapsto \top]$

2) $\vdash \varphi[p \mapsto \bot] \vee \varphi[p \mapsto \top] \to \psi$.

INTERPOLATION (for propositional logic)

If $\models \varphi \to \psi$, then there is θ s.t. $\models \varphi \to \theta$, $\models \theta \to \psi$, and $Var(\theta) \subseteq Var(\varphi) \cap Var(\psi)$.

If $\varphi \wedge \psi$ unsat. then $\exists \theta . \models \varphi \to \theta$ and $\theta \wedge \psi$ unsat.



SEPARABILITY:

- Co-r.e. vs. recursive.
- Analytic vs. Borel.
- Projective vs. elementary.
- Büchi vs. weak (infinite trees).
- Well-structured vs. regular...

APPLICATIONS of INTERPOLATION

Theory:

- Beth's definability theorem (P1.7.3).
- Circuit complexity (P1.7.5).
- Resolution provides interpolants (= explanation) of size polynomial in the refutation proof. (P1.7.6)

Practice:

- Inductive invariants in model-checking.
- Combination of theories (Nelson-Oppen).