

Logique – cours 7

DER d'informatique

ENS Paris-Saclay

2ème semestre, 2025-2026

13. Constructive logic

Dropping excluded middle and reductio ad absurdum

Recall: Gentzen calculi **LK** and **LJ**

- ▶ We defined Gentzen calculus **LK** with **22 rules**: 6 structural, 14 logical, axiom, and cut. (We don't consider equality.)
- ▶ The calculus **LJ** is the restriction of **LK** where the right side of a sequent is only allowed to contain **at most 1** formula.
- ▶ An alternative formulation of **LJ**, if we add \perp as a connective: **exactly** one formula on the right.
- ▶ We can then remove \neg as a basic connective, and regard it as an abbreviation:

$$\neg\varphi := \varphi \rightarrow \perp .$$

- ▶ In this formulation, **LJ** has 18 rules, and fits on one slide:

Sequent calculus LJ

$$\frac{\Gamma, \varphi, \psi, \Gamma' \vdash \delta}{\Gamma, \psi, \varphi, \Gamma' \vdash \delta} \mathcal{LX} \quad \frac{\Gamma \vdash \delta}{\Gamma, \varphi \vdash \delta} \mathcal{LW} \quad \frac{\Gamma \vdash \perp}{\Gamma \vdash \varphi} \mathcal{RW} \quad \frac{\Gamma, \varphi, \varphi \vdash \delta}{\Gamma, \varphi \vdash \delta} \mathcal{LC}$$

$$\frac{}{\varphi \vdash \varphi} \text{Ax} \quad \frac{\Gamma \vdash \varphi \quad \Gamma', \varphi \vdash \delta}{\Gamma, \Gamma' \vdash \delta} \text{Cut}$$

$$\frac{\Gamma, \varphi \vdash \delta}{\Gamma, \varphi \wedge \psi \vdash \delta} \mathcal{L1\wedge} \quad \frac{\Gamma, \psi \vdash \delta}{\Gamma, \varphi \wedge \psi \vdash \delta} \mathcal{L2\wedge} \quad \frac{\Gamma \vdash \varphi \quad \Gamma' \vdash \psi}{\Gamma, \Gamma' \vdash \varphi \wedge \psi} \mathcal{R\wedge}$$

$$\frac{\Gamma \vdash \varphi}{\Gamma \vdash \varphi \vee \psi} \mathcal{R1\vee} \quad \frac{\Gamma \vdash \psi}{\Gamma \vdash \varphi \vee \psi} \mathcal{R2\vee} \quad \frac{\Gamma, \varphi \vdash \delta \quad \Gamma', \psi \vdash \delta}{\Gamma, \Gamma', \varphi \vee \psi \vdash \delta} \mathcal{L\vee}$$

$$\frac{\Gamma \vdash \varphi \quad \Gamma', \psi \vdash \delta}{\Gamma, \Gamma', \varphi \rightarrow \psi \vdash \delta} \mathcal{L\rightarrow} \quad \frac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \rightarrow \psi} \mathcal{R\rightarrow}$$

$$\frac{\Gamma, \varphi[\frac{t}{x}] \vdash \delta}{\Gamma, \forall x. \varphi \vdash \delta} \mathcal{L\forall} \quad \frac{\Gamma \vdash \varphi}{\Gamma \vdash \forall x. \varphi} \mathcal{R\forall} \quad \frac{\Gamma, \varphi \vdash \delta}{\Gamma, \exists x. \varphi \vdash \delta} \mathcal{L\exists} \quad \frac{\Gamma \vdash \varphi[\frac{t}{x}]}{\Gamma \vdash \exists x. \varphi} \mathcal{R\exists}$$

in $\mathcal{R\forall}$ and $\mathcal{L\exists}$, the variable x must not be free in $\Gamma \cup \{\delta\}$.

Deciding intuitionistic logics

Recall, for a fixed signature, we defined:

- ▶ **IPC** is the set of propositional formulas φ such that $\vdash_{\mathbf{LJ}} \varphi$;
- ▶ **IQC** is the set of first-order formulas φ such that $\vdash_{\mathbf{LJ}} \varphi$.

Theorem (Statman, 1979)

IPC-membership is **PSPACE**-complete.

Proof.

By reduction to QBF-validity, see [the paper](#) (6 pages). ■

Theorem

IQC-membership is undecidable.

Proof.

Reduction from classical FO logic, by Gödel translation (TD). ■

Brouwer-Heyting-Kolmogorov interpretation

When is a formula φ intuitionistically provable?

The idea is that a proof should be a **construction**:

- ▶ a construction of $\varphi \wedge \psi$ is: a pair of constructions, one of φ , the other of ψ ;
- ▶ a construction of $\varphi \vee \psi$ is: a choice of either 'left', and a construction of φ , or 'right', and a construction of ψ ;
- ▶ a construction of $\varphi \rightarrow \psi$ is: a construction that takes as input a construction of φ and yields as output a construction of ψ ;
- ▶ a construction of $\forall x\varphi$ is: a construction that takes as input an instance a for x and produces a construction of $\varphi[a/x]$;
- ▶ a construction of $\exists x\varphi$ is: a pair of an instance a for x and a construction of $\varphi[a/x]$.

BHK, slightly more formally

Let us write $\pi : \varphi$ for ‘ π is a construction of φ ’. Then

- ▶ given $\pi_1 : \varphi_1$ and $\pi_2 : \varphi_2$, we get $\langle \pi_1, \pi_2 \rangle : \varphi_1 \wedge \varphi_2$,
- ▶ given $\pi_1 : \varphi_1$, we get $\iota_\ell(\pi_1) : \varphi_1 \vee \varphi_2$,
- ▶ given $\pi_2 : \varphi_2$, we get $\iota_r(\pi_2) : \varphi_1 \vee \varphi_2$,
- ▶ given, for any $x : \varphi_1$, a construction $\pi(x) : \varphi_2$, we get $\lambda x.f(x) : \varphi_1 \rightarrow \varphi_2$,
- ▶ given, for any a , a construction $\pi(a) : \varphi[a/x]$, we get $\lambda x.\pi(x) : \forall x.\varphi$,
- ▶ given a and $\pi : \varphi[a/x]$, we get $\langle a, \pi \rangle : \exists x.\varphi$.

The above may be viewed as **typing rules** in a language where first-order formulas are the types.

Dependently typed systems (used in proof assistants) exploit this.

Semantics

There are no **truth tables** for intuitionistic logic.

There do exist other **semantics** for intuitionistic logic.

(due to many people: Heyting, Beth, Henkin, Rasiowa, Kripke, ...)

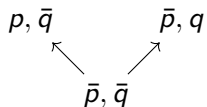
The key idea is that the truth of a formula may **change**:

- ▶ a property which is 'not yet' true may **become** true;
- ▶ a property which has become true **stays true** later;
- ▶ an implication is true now iff it is true classically **from now on**.

A first example of an intuitionistic model

Recall that $(p \rightarrow q) \vee (q \rightarrow p)$ is classically provable.

Consider the intuitionistic model



(where \bar{p} means: 'p is false'.)

At the root, $p \rightarrow q$ is **false**, because of the left child.

The formula $q \rightarrow p$ is also **false**, because of the right child.

Thus, $(p \rightarrow q) \vee (q \rightarrow p)$ is **falsified** by this (intuitionistic) model.

Definition of intuitionistic models, propositional case

Let P be a set of propositional variables.

An **IPC-model** over P is a tuple $\mathcal{M} = (W, \leq, V)$, where

- ▶ W is a set whose elements are called **nodes** or **worlds**;
- ▶ \leq is a partial order on W ;
- ▶ $V: W \rightarrow \mathcal{P}(P)$ is a function which is **persistent**, i.e.,

for any $w, w' \in W$, if $w \leq w'$, then $V(w) \subseteq V(w')$.

An **IPC-model** is **rooted** if it has a \leq -minimum world w_0 , and it is **finite** if W is finite.

Definition of intuitionistic semantics, propositional case

Let $\mathcal{M} = (W, \leq, V)$ be an **IPC**-model.

The **semantic relation** \models between worlds $w \in W$ and propositional formulas φ is defined by induction on φ , as follows:

- ▶ for $p \in P$, $w \models p$ iff $p \in V(w)$;
- ▶ it is not the case that $w \models \perp$;
- ▶ $w \models \varphi \vee \psi$ iff $w \models \varphi$ or $w \models \psi$;
- ▶ $w \models \varphi \wedge \psi$ iff $w \models \varphi$ and $w \models \psi$;
- ▶ $w \models \varphi \rightarrow \psi$ iff **for all** $v \geq w$, if $v \models \varphi$ then $v \models \psi$;

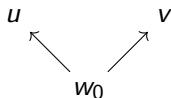
Note. Since $\neg\varphi := \varphi \rightarrow \perp$, we also have:

- ▶ $w \models \neg\varphi$ iff **for all** $v \geq w$, it is not the case that $v \models \varphi$.

If multiple models are in play, we sometimes write $\mathcal{M}, w \models \varphi$.

The example, more formally

Consider the **IPC**-model over $\{p, q\}$



where $V(w_0) = \emptyset$, $V(u) = \{p\}$, $V(v) = \{q\}$.

Then $u \geq w$, $u \models p$ and $u \not\models q$, so $w_0 \not\models p \rightarrow q$.

Similarly, $w_0 \not\models q \rightarrow p$.

So $w_0 \not\models (p \rightarrow q) \vee (q \rightarrow p)$.

Remark. We can add $(\varphi \rightarrow \psi) \vee (\psi \rightarrow \varphi)$ as an axiom to **IPC**; this is called *Gödel-Dummett logic*. It is complete with respect to **linear IPC**-models.

Definition of intuitionistic models, first-order case

Let L be a purely relational signature (for simplicity, and no $\dot{=}$).

An **IQC-model** is a tuple $\mathcal{M} = (W, \leq, I, \mathcal{D})$, where

- ▶ W is a set whose elements are called **nodes** or **worlds**;
- ▶ \leq is a partial order on W ;
- ▶ I is a set whose elements are called **individuals**;
- ▶ \mathcal{D} is a function which assigns to each $w \in W$ an L -structure $\mathcal{D}_w = (D_w, (R_w)_{R \in L})$, where $D_w \subseteq I$ and, for every R of arity n , $R_w \subseteq (D_w)^n$;
- ▶ \mathcal{D} is **persistent**, i.e., for any $w, w' \in W$ such that $w \leq w'$,
 - ▶ $D_w \subseteq D_{w'}$, and,
 - ▶ for any $R \in L$, $R_w \subseteq R_{w'}$.

Definition of intuitionistic semantics, first-order case

Let $\mathcal{M} = (W, \leq, I, \mathcal{D})$ be an **IQC**-model.

The **semantic relation** \models between worlds $w \in W$ and first-order formulas φ is defined by induction on φ , as follows:

- ▶ for $a_1, \dots, a_n \in I$, $w \models R(a_1, \dots, a_n)$ iff $(a_1, \dots, a_n) \in R_w$;
- ▶ $w \models \exists x\varphi$ iff there exists $a \in D_w$ such that $w \models \varphi[a/x]$;
- ▶ $w \models \forall x\varphi$ iff **for all** $v \geq w$ and $a \in D_v$, $v \models \varphi[a/x]$;
- ▶ all other inductive cases are as in the propositional case.

Persistence transfers to formulas

Lemma (Persistence)

Let w, v be nodes in an **IQC**-model such that $w \leq v$. Then, for any formula φ , if $w \models \varphi$, then $v \models \varphi$.

Proof.

Induction on φ . ■

Soundness

Theorem (Soundness)

Suppose $\Gamma \vdash_{\mathbf{LJ}} \varphi$. For any world w in any **IQC**-model, if $w \models \gamma$ for all $\gamma \in \Gamma$, then $w \models \varphi$.

Proof.

Induction on an **LJ**-derivation of $\Gamma \vdash \varphi$. ■

Showing non-provability in LJ

Models give an alternative way of establishing that formulas are *not* LJ-provable:

Example

$$\begin{array}{c} p \\ \uparrow \\ \bar{p} \end{array}$$

In this model, $\not\models p \vee \neg p$. By soundness, $\not\vdash_{\text{LJ}} p \vee \neg p$.

Constant domains

Let φ be a formula not containing the variable x , and ψ any formula. Define

$$\mathbf{CD}_{\varphi,\psi} := \forall x(\varphi \vee \psi) \rightarrow (\varphi \vee \forall x\psi) .$$

Then $\vdash_{\mathbf{LK}} \mathbf{CD}_{\varphi,\psi}$ (exercise), but, in general, $\not\vdash_{\mathbf{LJ}} \mathbf{CD}_{\varphi,\psi}$.

Example

Let P, Q be unary relation symbols, $\varphi := \exists yP(y)$ and $\psi := Q(x)$. In the model below, $\forall x(\varphi \vee \psi)$ holds but $\varphi \vee \forall x\psi$ does not hold.

$$\begin{array}{cc} Q(a), P(b), \overline{Q(b)} & D = \{a, b\} \\ | & \\ Q(a) & D = \{a\} \end{array}$$

IQC + CD is complete with respect to **constant domain** models.

Completeness

Theorem

Suppose $\Gamma \vdash \varphi$ is a sequent such that, for any rooted intuitionistic model, if $w_0 \models \gamma$ for all $\gamma \in \Gamma$, then $w_0 \models \varphi$. Then $\Gamma \vdash_{\mathbf{LJ}} \varphi$.

Proof.

We outline some general ideas for the proof below, and the DM asks you to prove it for the propositional case. ■

Note. The theorem as we stated it does *not* hold if one works in an intuitionistic meta-theory. There are ways to modify the definition of ‘model’ to make it hold even with an intuitionistic meta-theory.

Semantic proof of the disjunction property

Proposition (Disjunction property)

For any formulas φ and ψ , if $\vdash \varphi \vee \psi$ is **LJ**-provable, then either $\vdash \varphi$ is **LJ**-provable or $\vdash \psi$ is **LJ**-provable.

Proof.

Suppose that neither $\vdash_{\mathbf{LJ}} \varphi$ nor $\vdash_{\mathbf{LJ}} \psi$.

By **completeness**, pick rooted intuitionistic models $(W_1, \leq_1, I_1, \mathcal{D}_1)$ and $(W_2, \leq_2, I_2, \mathcal{D}_2)$ with roots w_1 and w_2 , $w_1 \not\models \varphi$ and $w_2 \not\models \psi$.

Consider the model with worlds $\{w_0\} \sqcup W_1 \sqcup W_2$, $I := I_1 \sqcup I_2$, and \mathcal{D}_w defined as in \mathcal{D}_1 or \mathcal{D}_2 , except when $w = w_0$, where we put $\mathcal{D}_w := \emptyset$ and $R_w := \emptyset$ for every symbol R .

The resulting model is persistent (**check**) and thus $w_0 \not\models \varphi \vee \psi$.

By soundness, it is not the case that $\vdash_{\mathbf{LJ}} \varphi \vee \psi$. ■

14. Heyting algebras

An algebraic approach to completeness

Suprema and infima

Let (L, \leq) be a partially ordered set and let $S \subseteq L$.

A **supremum** of S is an element $s_0 \in L$ such that

- ▶ s_0 is an upper bound of S ;
- ▶ for any upper bound t of S , we have $s_0 \leq t$.

Note: s_0 can fail to be an element of S . If $s_0 \in S$, **maximum**.

Suprema are **unique**: if s_0 and s'_0 are suprema of S , then $s_0 = s'_0$.

The set S may **not have any** supremum.

We make the analogous definition and remarks for **infimum**.

We write $\bigvee S$ for the supremum of S and $\bigwedge S$ for the infimum.

If $S = \{s_1, s_2\}$, we write $s_1 \vee s_2$ for $\bigvee S$ and $s_1 \wedge s_2$ for $\bigwedge S$.

If $S = \emptyset$, we write \perp for $\bigvee \emptyset$ and \top for $\bigwedge \emptyset$.

Bounded lattices

A **bounded lattice** is a partially ordered set (L, \leq) such that, for any finite subset S of L , the supremum and infimum of S exist.

An equivalent, algebraic definition:

A **bounded lattice** is a tuple $(L, \vee, \perp, \wedge, \top)$ where \vee, \wedge are binary operations and \perp, \top are nullary operations, such that

- ▶ (L, \vee, \perp) and (L, \wedge, \top) are commutative, idempotent monoids;
- ▶ for all $a, b \in L$, $a \wedge (a \vee b) = a = a \vee (a \wedge b)$.

We then **define** $a \leq b$ iff $a \vee b = b$.

Proposition

For any bounded lattice $(L, \vee, \perp, \wedge, \top)$ in the algebraic sense,
 $a \vee b = \sup_{\leq} \{a, b\}$, $\perp = \sup_{\leq} \emptyset$, $a \wedge b = \inf_{\leq} \{a, b\}$, $\top = \inf_{\leq} \emptyset$.

Order-completeness

A lattice L is **complete** if, for any $S \subseteq L$, $\bigvee S$ and $\bigwedge S$ exist.

Note. If all suprema exist, then all infima exist, and vice versa.

Finite lattices are always complete, but infinite bounded lattices may not be.

Heyting algebras

A **Heyting algebra** is a tuple $(A, \vee, \perp, \wedge, \top, \rightarrow)$, where $(A, \vee, \perp, \wedge, \top)$ is a bounded lattice, and, for any $a, b, c \in A$,

$$c \wedge a \leq b \text{ if, and only if } c \leq a \rightarrow b .$$

In other words, $a \rightarrow b = \max\{c \in A \mid c \wedge a \leq b\}$.

The element $b \rightarrow c$ is the **relative pseudocomplement** of b in c .

We say that a partially ordered set (A, \leq) is a **Heyting algebra** if finite suprema and infima exist in A , and, for any $a, b \in A$, the set $\{c \in A \mid c \wedge a \leq b\}$ has a maximum.

Note. There is at most one Heyting algebra structure on a poset.

Two kinds of Heyting algebras

1. A complete lattice A is a Heyting algebra if, and only if, for any $a \in A$ and $S \subseteq A$,

$$a \wedge \bigvee S = \bigvee_{s \in S} (a \wedge s).$$

Proof.

$a \rightarrow b$ can be defined as $\bigvee \{c \mid c \wedge a \leq b\}$. ■

2. Any totally ordered set with endpoints is a Heyting algebra.

Proof.

$a \rightarrow b$ can be defined as \top if $a \leq b$ and as b otherwise. ■

Evaluating formulas in Heyting algebras

Fix a set P . A **propositional formula** (over P) is built with $\vee, \perp, \wedge, \rightarrow$, and propositional variables $p \in P$.

We write $\text{Form}(P)$ for the set of propositional formulas over P .

Let A be a Heyting algebra and $f: P \rightarrow A$ a function.

We inductively define $\bar{f}(\varphi) \in A$: for $p \in P$ and $\varphi, \psi \in \text{Form}(P)$,

- ▶ $\bar{f}(p) := f(p)$,
- ▶ $\bar{f}(\varphi \vee \psi) := \bar{f}(\varphi) \vee_A \bar{f}(\psi)$;
- ▶ $\bar{f}(\perp) := \perp_A$;
- ▶ $\bar{f}(\varphi \wedge \psi) := \bar{f}(\varphi) \wedge_A \bar{f}(\psi)$;
- ▶ $\bar{f}(\varphi \rightarrow \psi) := \bar{f}(\varphi) \rightarrow_A \bar{f}(\psi)$.

Provability and equality in Heyting algebras

IPC(P) is the set of $\varphi \in \text{Form}(P)$ such that $\vdash_{\mathbf{LJ}} \varphi$.

Theorem (Algebraic soundness and completeness for IPC)

For any $\varphi \in \text{Form}(P)$, the following are equivalent:

1. $\vdash_{\mathbf{LJ}} \varphi$;
2. for any Heyting algebra A and any $f: P \rightarrow A$, $\bar{f}(\varphi) = \top_A$.

Proof.

See DM. ■

World-based semantics as Heyting-valued semantics

If (W, \leq) is a partially ordered set, write $\mathcal{U}(W)$ for the collection of **upward closed subsets** of W , ordered by inclusion.

Then $\mathcal{U}(W)$ is a (complete) Heyting algebra. For $U, V \in \mathcal{U}(W)$,

$$U \rightarrow V = \{w \in W \mid \text{for all } v \geq w, \text{ if } v \in U, \text{ then } v \in V\} .$$

An intuitionistic propositional model is the same thing as a poset (W, \leq) together with a function $f: P \rightarrow \mathcal{U}(W)$.

Proposition

For any $w \in W$ and $\varphi \in \text{Form}(P)$,

$$w \models \varphi \text{ if, and only if, } w \in \bar{f}(\varphi) .$$

By induction on φ .

Representation of Heyting algebras via up-sets

Let A be a Heyting algebra.

An up-set F in A is a **filter** if $\top \in F$ and, for any $a, b \in A$, if $a \in F$ and $b \in F$, then $a \wedge b \in F$.

A filter F is **prime** if $\perp \notin F$, and, for any $a, b \in A$, if $a \vee b \in F$, then $a \in F$ or $b \in F$.

Let A_* be the poset of prime filters of A , ordered by inclusion.

Define the function $\eta: A \rightarrow \mathcal{U}(A_*)$ by, for $a \in A$,

$$\eta(a) := \{F \in A_* \mid a \in F\} .$$

Theorem (M. H. Stone, 1937)

The function η is an injective Heyting algebra homomorphism.

Proof.

See below.



Completeness of world-based semantics for IPC

Theorem

For any $\varphi \in \text{Form}(P)$, the following are equivalent:

1. for any Heyting algebra A and $f: P \rightarrow A$, $\bar{f}(\varphi) = \top_A$;
2. for any poset (W, \leq) and $f: P \rightarrow \mathcal{U}(W)$, $\bar{f}(\varphi) = W$.

Proof.

(1) \Rightarrow (2). Clear, since $\mathcal{U}(W)$ is a Heyting algebra.

(2) \Rightarrow (1). Let $f: P \rightarrow A$ be arbitrary.

Consider $g := \eta \circ f$, where $\eta: A \rightarrow \mathcal{U}(A_*)$ is as defined above.

By (2), $\bar{g}(\varphi) = W$.

Since η is a homomorphism, $\bar{g} = \eta \circ \bar{f}$.

Thus, $\eta(\bar{f}(\varphi)) = W = \eta(\top_A)$.

Since η is injective, $\bar{f}(\varphi) = \top_A$. ■

Proof of the Stone representation theorem

Lemma (Prime filter lemma)

Let A be a Heyting algebra. If F is a filter in A and $a \in A \setminus F$, then there exists a prime filter G such that $F \subseteq G$ and $a \notin G$.

Proof of one case of Stone's Theorem.

The difficult case is

$$\eta(a) \rightarrow \eta(b) \subseteq \eta(a \rightarrow b) .$$

Let $F \in A_*$ and suppose $a \rightarrow b \notin F$.

Let F' be the filter generated by $F \cup \{a\}$. Then $b \notin F'$ ([exercise](#)).

By the Prime filter lemma, pick $G \in A_*$ with $F' \subseteq G$, $b \notin G$.

Then $F \subseteq G$ and $a \in G$, but $b \notin G$. So $F \not\subseteq \eta(a) \rightarrow \eta(b)$. ■

Extending the proof to **IQC**

We will not treat the entire completeness proof for **IQC**.

It is a combination of:

- ▶ Henkin's (classical) construction, locally at each world;
- ▶ An extension lemma, which can be proved using the prime filter lemma, but taking care also of quantifiers.

Finite model property of **IPC**

Proposition

Let φ be a formula of **IPC**. If $\not\vdash_{\mathbf{LJ}} \varphi$, then there exists a **finite** rooted model in which $w_0 \not\models \varphi$.

Proof.

See DM. ■

The Rieger-Nishimura lattice and universal model

There exist infinitely many non-equivalent formulas in **IPC** on one propositional variable.

A Heyting algebra consisting of all equivalence classes of such formulas is called the **Rieger-Nishimura lattice**, or **Lindenbaum algebra on one variable**, or **free Heyting algebra on one generator**.

In the DM, you will see a construction of this lattice, via a 'universal model'.