# CSC_51051_EP: Natural deduction

Samuel Mimram

2025

École polytechnique

Part I

# Introduction

# Propositional logic

In propositional logic, we consider **formulas** which are built from

- variables: $X$, $Y$, $\ldots$
- connectives: $\wedge$, $\vee$, $\Rightarrow$, $\neg$, $\ldots$

For instance,

$$(X \Rightarrow Y) \Rightarrow (\neg X \vee Y)$$

# The boolean interpretation

Usually,

- we interpret variables as booleans (*valuations*),
- we have a standard interpretation for connectives

| $A \wedge B$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

| $A \vee B$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 1 |

| $A \Rightarrow B$ | 0 | 1 |
|---|---|---|
| 0 | 1 | 1 |
| 1 | 0 | 1 |

| $\neg A$ | |
|---|---|
| 0 | 1 |
| 1 | 0 |

A formula is **valid** when its interpretation is true for every value given to the variables.

$$\underbrace{(X \Rightarrow Y) \Rightarrow (\neg X \vee Y)}_{1}$$

with $X = 1$ and $Y = 0$.

# The set-theoretic interpretation

With this idea that propositions should correspond to types and consider

$$\mathbb{N} \Rightarrow \mathbb{N}$$

We should therefore interpret

- a type $A$ as a **set**,
- $A \Rightarrow B$ as the set of **functions** from $A$ to $B$,
- $A \wedge B$ as the product $A \times B$,
- $A \vee B$ as the disjoint union $A \sqcup B$.

We recover the previous interpretation by considering whether a set is empty or not:

| $A \wedge B$ | $\emptyset$ | $1$ |
|---|---|---|
| $\emptyset$ | $\emptyset$ | $\emptyset$ |
| $1$ | $\emptyset$ | $1$ |

| $A \vee B$ | $\emptyset$ | $1$ |
|---|---|---|
| $\emptyset$ | $\emptyset$ | $1$ |
| $1$ | $1$ | $1$ |

| $A \Rightarrow B$ | $\emptyset$ | $1$ |
|---|---|---|
| $\emptyset$ | $1$ | $1$ |
| $1$ | $\emptyset$ | $1$ |

| $\neg A$ | |
|---|---|
| $\emptyset$ | $1$ |
| $1$ | $\emptyset$ |

# The proof-theoretic interpretation

This is not entirely satisfactory since the way a function is implemented matters.

For instance,

$$\mathbb{N} \Rightarrow \mathbb{N}$$
$$n \mapsto 0$$

can be implemented as

- `let f n = 0`
- `let f n = n - n`
- `let rec f n = if n = 0 then n else f (n - 1)`

Note that the complexities are respectively $O(1)$, $O(\log_2(n))$ and $O(n)$.

# The three levels of interpretation

Girard advocates that there are three levels for interpreting proofs:

**0.** the *boolean level*: propositions are interpreted as booleans and we are interested in whether a proposition is provable or not,

**1.** the *extensional level*: propositions are interpreted as sets and we are interested in which functions can be implemented,

**2.** the *intentional level*: we are interested in the proofs (= programs) themselves, and how they evolve during reduction,

$\vdots$

$\infty$. the *homotopical level*: we take equality seriously in account.

# Intuitionism

Shifting from provability to proofs was initiated by Brouwer's **intuitionism** (around 1900):

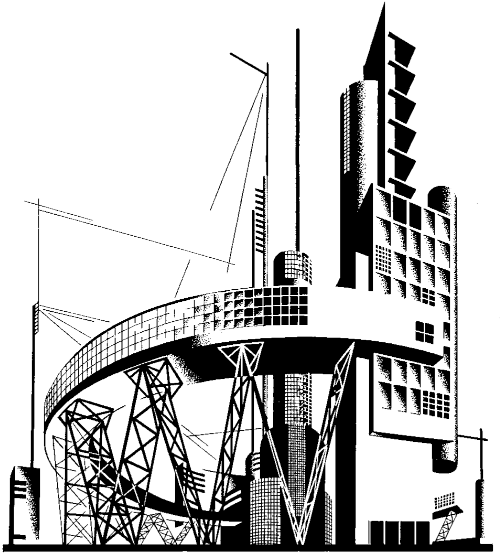
- mathematics is not about a preexisting reality,
  it is a subjective mental construction,
- this construction has an existence of its own.

In this point of view, we switch from provability to proofs:

- $A \wedge B$ means that I have both a proof of $A$ and a proof $B$
  (it is a product rather than an intersection)
- $A \Rightarrow B$ is a way of producing a proof of $B$ from a proof of $A$.

This has some important consequences that we will see.

# Constructivism



# Formalizing the notion proof

We want to give a precise definition of the notion of **proof**.

This means give a list of all the allowed (low-level!) steps in a proof.

For instance, we want to show that $x \mapsto 2 \times x$ is continuous in $0$:
we have to prove the formula

$$\forall \varepsilon.(\varepsilon > 0 \Rightarrow \exists \eta.(\eta > 0 \land \forall x.|x| < \eta \Rightarrow |2x| < \varepsilon))$$

# Formalizing the notion proof

Done!

$$|x| < \varepsilon/2$$

- Suppose given $\varepsilon$.
- Suppose $\varepsilon > 0$.
- Take $\eta = \varepsilon/2$.
-

- Since $2 > 0$.
- By usual identities.
- By hypothesis.
-

- Suppose given $x$.
- Suppose $|x| < \varepsilon/2$.
- By usual identities.
- By hypothesis

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\varepsilon > 0 \vdash \varepsilon > 0}}{\varepsilon > 0 \vdash (\varepsilon/2) \times 2 > 0 \times 2}}{\varepsilon > 0 \vdash \varepsilon/2 > 0} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\varepsilon > 0, |x| < \varepsilon/2 \vdash |x| < \varepsilon/2}}{\varepsilon > 0, |x| < \varepsilon/2 \vdash |2x|/2 < \varepsilon/2}}{\varepsilon > 0, |x| < \varepsilon/2 \vdash |2x| < \varepsilon}}{\varepsilon > 0 \vdash |x| < \varepsilon/2 \Rightarrow |2x| < \varepsilon}}{\varepsilon > 0 \vdash \forall x. |x| < \varepsilon/2 \Rightarrow |2x| < \varepsilon}}{\varepsilon > 0 \vdash \varepsilon/2 > 0 \land \forall x. |x| < \varepsilon/2 \Rightarrow |2x| < \varepsilon}}{\varepsilon > 0 \vdash \exists \eta. (\eta > 0 \land \forall x. |x| < \eta \Rightarrow |2x| < \varepsilon)}}{\vdash \varepsilon > 0 \Rightarrow \exists \eta. (\eta > 0 \land \forall x. |x| < \eta \Rightarrow |2x| < \varepsilon)}}{\vdash \forall \varepsilon. (\varepsilon > 0 \Rightarrow \exists \eta. (\eta > 0 \land \forall x. |x| < \eta \Rightarrow |2x| < \varepsilon))}$$

# Formalizing the notion of proof

This has several interesting consequences.

- We can show properties of the system: consistency, decidability, etc.
- We can reason on proofs.
- We can transform proofs.

Part II

# Intuitionistic natural deduction

# Formulas

We consider **formulas** generated by the grammar

$$A, B ::= X \mid A \Rightarrow B \mid A \wedge B \mid \top \mid A \vee B \mid \bot \mid \neg A$$

where $X$ is a variable.

By convention:

- the binding priority is $\neg$, $\wedge$, $\vee$, $\Rightarrow$:

$$\neg A \vee B \wedge C \Rightarrow D \qquad \text{is} \qquad ((\neg A) \vee (B \wedge C)) \Rightarrow D$$

- the operations are bracketed on the *right*:

$$A_1 \wedge A_2 \wedge A_3 \Rightarrow B \Rightarrow C \qquad \text{is} \qquad (A_1 \wedge (A_2 \wedge A_3)) \Rightarrow (B \Rightarrow C)$$

# Sequents

A **context** $\Gamma$ is a list of formulas

$$A_1, \ldots, A_n$$

A **sequent**

$$\Gamma \vdash A$$

consists of a context $\Gamma$ together with a formula $A$.

An **inference rule**

$$\frac{\Gamma_1 \vdash A_1 \qquad \ldots \qquad \Gamma_n \vdash A_n}{\Gamma \vdash A}$$

specifies when we can deduce a sequent from others.

# Intuitionistic natural deduction (NJ)

$$\frac{}{\Gamma, A, \Gamma' \vdash A}\,(\text{ax})$$

$$\frac{\Gamma \vdash A \Rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B}\,(\Rightarrow_{\text{E}}) \qquad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}\,(\Rightarrow_{\text{I}})$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\,(\wedge^{\text{l}}_{\text{E}}) \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\,(\wedge^{\text{r}}_{\text{E}}) \qquad \frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\,(\wedge_{\text{I}})$$

$$\frac{\Gamma \vdash A \vee B \qquad \Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma \vdash C}\,(\vee_{\text{E}}) \qquad \frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\,(\vee^{\text{l}}_{\text{I}}) \quad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\,(\vee^{\text{r}}_{\text{I}})$$

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash A}\,(\bot_{\text{E}}) \qquad \frac{}{\Gamma \vdash \top}\,(\top_{\text{I}})$$

$$\frac{\Gamma \vdash \neg A \qquad \Gamma \vdash A}{\Gamma \vdash \bot}\,(\neg_{\text{E}}) \qquad \frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}\,(\neg_{\text{I}})$$

# Rules: remarks

Apart from the axiom, rules are either

- **elimination** rules: use a connective,
- **introduction** rules: show a connective.

The leaves are axiom (or $\top$ introduction) rules: all the other rules have premises.

The axiom is the only way to "use" a formula in the context.

There is no introduction of $\bot$ and elimination of $\top$.

The **principal** premise is the leftmost premise of an elimination rule.

Some rules have latin names:

- $(\Rightarrow_E)$: *modus ponens*
- $(\bot_E)$: *ex falso quot libet* or *explosion principle*

# Proofs

A **proof** is a tree formed with the derivation rules of NJ.

A sequent $\Gamma \vdash A$ is **provable** when it is the conclusion of some proof.

A formula $A$ is **provable** when the sequent $\vdash A$ is.

# A proof of $A \Rightarrow A$

$$\dfrac{\dfrac{}{A \vdash A}\,(\mathrm{ax})}{\vdash A \Rightarrow A}\,(\Rightarrow_{\mathrm{I}})$$

# A proof of $A \wedge B \Rightarrow A \vee B$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \wedge B \vdash A \wedge B}\ (\text{ax})}{A \wedge B \vdash A}\ (\wedge_E^l)}{A \wedge B \vdash A \vee B}\ (\vee_I^l)}{\vdash A \wedge B \Rightarrow A \vee B}\ (\Rightarrow_I)$$

# A proof of $(A \lor B) \Rightarrow (B \lor A)$

$$
\dfrac{
  \dfrac{}{A \lor B \vdash A \lor B}\,(\text{ax})
  \qquad
  \dfrac{\dfrac{}{A \lor B, A \vdash A}\,(\text{ax})}{A \lor B, A \vdash B \lor A}\,(\lor_{\text{I}}^{\text{r}})
  \qquad
  \dfrac{\dfrac{}{A \lor B, B \vdash B}\,(\text{ax})}{A \lor B, B \vdash B \lor A}\,(\lor_{\text{I}}^{\text{l}})
}{
  \dfrac{A \lor B \vdash B \lor A}{\vdash A \lor B \Rightarrow B \lor A}\,(\Rightarrow_{\text{I}})
}\,(\lor_{\text{E}})
$$

# A proof of $(A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)$

$$
\dfrac{\dfrac{}{A \Rightarrow B, \neg B, A \vdash \neg B}(\text{ax}) \quad \dfrac{\dfrac{}{A \Rightarrow B, \neg B, A \vdash A \Rightarrow B}(\text{ax}) \quad \dfrac{}{A \Rightarrow B, \neg B, A \vdash A}(\text{ax})}{A \Rightarrow B, \neg B, A \vdash B}(\Rightarrow_{\text{E}})}{\dfrac{A \Rightarrow B, \neg B, A \vdash \bot}{\dfrac{A \Rightarrow B, \neg B \vdash \neg A}{\dfrac{A \Rightarrow B \vdash \neg B \Rightarrow \neg A}{\vdash (A \Rightarrow B) \Rightarrow \neg B \Rightarrow \neg A}(\Rightarrow_{\text{I}})}(\Rightarrow_{\text{I}})}(\neg_{\text{I}})}(\neg_{\text{E}})
$$

# Definable connectives

We could have added some other connectives such as $\Leftrightarrow$, which can be implemented:

$$A \Leftrightarrow B \qquad = \qquad (A \Rightarrow B) \wedge (B \Rightarrow A)$$

Even some present connectives can be implemented from others:

$$\neg A \qquad = \qquad A \Rightarrow \bot$$

**Proof.**
Can be deduced (not trivial) from the fact that $\neg A \Leftrightarrow (A \Rightarrow \bot)$ is provable. □

Part III

# Properties of NJ

# Induction on proofs

Since proofs have become syntactic objects,
we can reason (= make proofs) on them!

# Induction on natural numbers

The set $\mathbb{N}$ of natural numbers is the smallest set containing $0$ and closed under successor.

$$\frac{}{0 : \mathbb{N}} \qquad\qquad \frac{n : \mathbb{N}}{S(n) : \mathbb{N}}$$

The **recurrence principle** states that, given a predicate $P(n)$ on natural numbers, if, for every rule,

- if $P$ holds for the premises then $P$ holds for the conclusion

then $P(n)$ holds for every $n \in \mathbb{N}$.

# Induction on proofs

The set of proofs is the smallest set closed under the deduction rules:

**Theorem**
*Suppose given a predicate $P(\pi)$ on proofs $\pi$. Suppose that, for every rule,*

$$\pi \quad = \quad \cfrac{\cfrac{\pi_1}{\Gamma_1 \vdash A_1} \qquad \ldots \qquad \cfrac{\pi_n}{\Gamma_n \vdash A_n}}{\Gamma \vdash A}$$

*if $P(\pi_i)$ holds for every $i$ then $P(\pi)$ also holds. Then $P(\pi)$ holds for every proof $\pi$.*

# Admissible rules

A rule

$$\frac{\Gamma_1 \vdash A_1 \qquad \dots \qquad \Gamma_n \vdash A_n}{\Gamma \vdash A}$$

is **admissible** when, whenever all the premises are provable, the conclusion is also provable.

This means that, from a proof for each $\Gamma_i \vdash A_i$, we can construct a proof of $\Gamma \vdash A$ (but not necessarily that we can implement the above deduction with some rules).

# Weakening

We have this idea that if we can prove something with some hypothesis, then we can also prove it with more hypothesis.

For instance:

$$\dfrac{\dfrac{\overline{C, A \land B \vdash A \land B}\ (\text{ax})}{C, A \land B \vdash A}\ (\land_{\text{E}}^{\text{l}})}{C, A \land B \vdash A \lor B}\ (\lor_{\text{I}}^{\text{l}})$$

This can be formalized by showing that the following **weakening** rule is admissible.

# Weakening

We can always add more hypothesis in a context:

**Proposition**

*The **weakening rule** is admissible:* $\dfrac{\Gamma, \Gamma' \vdash B}{\Gamma, A, \Gamma' \vdash B}\ (\mathrm{wk})$ .

**Proof.**
By induction on the proof of $\Gamma, \Gamma' \vdash B$.

- Other cases are similar. □

# Weakening

Note that the axiom rule

$$\frac{}{\Gamma, A, \Gamma' \vdash A} \text{(ax)}$$

is the only one really using the context, the other rules do not change the context, e.g.

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

excepting

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B} (\Rightarrow_\mathrm{I})$$

which only adds one formula to the context.

This explains why most inductive cases go through without any difficulty,
axiom being the only "subtle" one.

## Contraction

In a context, the multiplicity of a formula does not really matter:

**Proposition**
*The **contraction rule** is admissible:*

$$\frac{\Gamma, A, A, \Gamma' \vdash B}{\Gamma, A, \Gamma' \vdash B}\ (\text{contr})$$

**Proof.**
By induction on the proof of $\Gamma, A, A, \Gamma' \vdash C$:

$$\frac{}{\Gamma, A, A, \Gamma' \vdash B}\ (\text{ax}) \qquad \text{becomes} \qquad \frac{}{\Gamma, A, \Gamma' \vdash B}\ (\text{ax})$$

(including when $B = A$), other cases are simple, e.g.

$$\frac{\dfrac{\vdots}{\Gamma, A, \Gamma' \vdash B} \qquad \dfrac{\vdots}{\Gamma, A, \Gamma' \vdash C}}{\Gamma, A, \Gamma' \vdash B \wedge C}\ (\wedge_{\text{I}}) \qquad \text{becomes} \qquad \frac{\dfrac{\vdots}{\Gamma, A, A, \Gamma' \vdash B} \qquad \dfrac{\vdots}{\Gamma, A, A, \Gamma' \vdash C}}{\Gamma, A, A, \Gamma' \vdash B \wedge C}\ (\wedge_{\text{I}})$$

# Exchange

In a context, the order of formulas does not really matter:

**Proposition**
*The* ***exchange rule***

$$\frac{\Gamma, A, B, \Gamma' \vdash C}{\Gamma, B, A, \Gamma' \vdash C}\ (\text{xch})$$

*is admissible.*

**Proof.**
By induction on the proof of $\Gamma, A, B, \Gamma' \vdash C$.

$$\frac{}{\Gamma, A, B, \Gamma' \vdash C}\ (\text{ax}) \qquad \text{becomes} \qquad \frac{}{\Gamma, B, A, \Gamma' \vdash C}\ (\text{ax})$$

other cases are immediate by induction. □

# Truth strengthening

In a context, the formula $\top$ does not bring any information:

**Proposition**
*The **truth strengthening rule***

$$\frac{\Gamma, \top, \Gamma' \vdash A}{\Gamma, \Gamma' \vdash A}$$

*is admissible.*

**Proof.**
By induction on the proof of $\Gamma, \top, \Gamma' \vdash A$:

$$\frac{}{\Gamma, \top, \Gamma' \vdash \top}\,(\text{ax}) \qquad \text{becomes} \qquad \frac{}{\Gamma, \Gamma \vdash \top}\,(\top_{\text{I}})$$

other cases are immediate by induction. □

# Contexts as sets

The **structural rules**

$$\frac{\Gamma, \Gamma' \vdash B}{\Gamma, A, \Gamma' \vdash B}\ (\text{wk}) \qquad \frac{\Gamma, A, A, \Gamma' \vdash B}{\Gamma, A, \Gamma' \vdash B}\ (\text{contr})$$

$$\frac{\Gamma, A, B, \Gamma' \vdash C}{\Gamma, B, A, \Gamma' \vdash C}\ (\text{xch}) \qquad \frac{\Gamma, \top, \Gamma' \vdash A}{\Gamma, \Gamma' \vdash A}$$

say that that contexts are commutative and idempotent.

Can we implement them as sets?

# Contexts as sets

Quizz: how many "pure" OCaml programs of type

```
'a -> 'a -> 'a
```

can you come up with?

Essentially two:

```
let f x y = x
let f x y = y
```

I say "essentially" because there are many other which are "equivalent":

```
let f'  x y = (fun z -> z) x
let f'' x y = (fun (z,t) -> z) (x, 5)
...
```

# Contexts as sets

Having contexts as sets is not a good idea: the two proofs

$$\dfrac{\dfrac{\dfrac{}{A, A \vdash A}\,(\mathrm{ax})}{A \vdash A \Rightarrow A}\,(\Rightarrow_{\mathrm{I}})}{\vdash A \Rightarrow A \Rightarrow A}\,(\Rightarrow_{\mathrm{I}}) \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{A, A \vdash A}\,(\mathrm{ax})}{A, A \vdash A}\,(\mathrm{xch})}{A \vdash A \Rightarrow A}\,(\Rightarrow_{\mathrm{I}})}{\vdash A \Rightarrow A \Rightarrow A}\,(\Rightarrow_{\mathrm{I}})$$

get identified into

$$\dfrac{\dfrac{\dfrac{}{A \vdash A}\,(\mathrm{ax})}{A \vdash A \Rightarrow A}\,(\Rightarrow_{\mathrm{I}})}{\vdash A \Rightarrow A \Rightarrow A}\,(\Rightarrow_{\mathrm{I}})$$

whereas we expect to have two projections!

# Substitution

A **substitution** $\sigma$ is a function which assigns a formula to every variable.

We write $A[\sigma]$ for the formula $A$ with variables replaced according to $\sigma$.

**Proposition**
*For every substitution $\sigma$, if the sequent*

$$A_1, \ldots, A_n \vdash A$$

*is provable, then the sequent*

$$A_1[\sigma], \ldots, A_n[\sigma] \vdash A[\sigma]$$

*is also provable.*

**Proof.**
By induction on the proof of $A_1, \ldots, A_n \vdash A$. □

## Proof substitution

Another more subtle operation is **proof substitution**:

**Proposition**
*Given provable sequents*

$$\frac{\pi}{\Gamma, A, \Gamma' \vdash B} \qquad \textit{and} \qquad \frac{\pi'}{\Gamma, \Gamma' \vdash A}$$

*we can construct a proof*

$$\frac{\pi[\pi'/A]}{\Gamma, \Gamma' \vdash B}$$

# Proof substitution

For instance, given the proofs

$$\pi = \dfrac{\dfrac{\dfrac{}{\Gamma, A, B \vdash A}\,(\text{ax}) \qquad \dfrac{}{\Gamma, A, B \vdash A}\,(\text{ax})}{\Gamma, A, B \vdash A \wedge A}\,(\wedge_{\text{I}})}{\Gamma, A \vdash B \Rightarrow A \wedge A}\,(\Rightarrow_{\text{I}}) \qquad \text{and} \qquad \pi' = \dfrac{\vdots}{\Gamma \vdash A}$$

we can construct the following proof $\pi[\pi'/A]$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\pi'}{\Gamma \vdash A}}{\Gamma, B \vdash A}\,(\text{wk}) \qquad \dfrac{\dfrac{\pi'}{\Gamma \vdash A}}{\Gamma, B \vdash A}\,(\text{wk})}{\Gamma, B \vdash A \wedge A}\,(\wedge_{\text{I}})}{\Gamma \vdash B \Rightarrow A \wedge A}\,(\Rightarrow_{\text{I}})$$

# Proof substitution

**Proposition**

*Given provable sequents* $\dfrac{\pi}{\Gamma, A, \Gamma' \vdash B}$ *and* $\dfrac{\pi'}{\Gamma, \Gamma' \vdash A}$,

*we can construct a proof* $\dfrac{\pi[\pi'/A]}{\Gamma, \Gamma' \vdash B}$.

**Proof.**
By induction on $\pi$:

- we replace axioms $\dfrac{}{\Gamma, A, \Gamma', \Gamma'' \vdash A}\,(\mathrm{ax})$ by $\dfrac{w(\pi')}{\Gamma, \Gamma', \Gamma'' \vdash A}$,
- $\dfrac{\dfrac{\pi_1}{\Gamma, A, \Gamma' \vdash B} \qquad \dfrac{\pi_2}{\Gamma, A, \Gamma' \vdash C}}{\Gamma, A, \Gamma' \vdash B \wedge C}$ becomes $\dfrac{\dfrac{\pi_1[\pi'/A]}{\Gamma, \Gamma' \vdash B} \qquad \dfrac{\pi_2[\pi'/A]}{\Gamma, \Gamma' \vdash C}}{\Gamma, \Gamma' \vdash B \wedge C}$, etc. □

Part IV

# Cut elimination

# Cut elimination

In mathematics, one often uses lemmas to show results.

**Theorem**
$\exists x. x + x = 4$.

**Proof.**
Take $x = 2$. □

The proof of the lemma must certainly contain a way to compute the value for $x$.

This process of extraction is called **cut elimination**.

# Cut elimination

Of course, this largely depends on the way we formalized things.

We define even natural numbers as the smallest set $\mathsf{Even} \subseteq \mathbb{N}$ such that

- $0 \in \mathsf{Even}$,
- if $n \in \mathsf{Even}$ then $n + 2 \in \mathsf{Even}$.

We can also show that $4$ is even:

- $0$ is even,
- thus $2$ is even,
- thus $4$ is even.

And therefore $4$ admits a half.

# Cut elimination

From our proof, we can compute the half of 4:

- 4 is even, because 2 is even, because 0 is even,
- $\mathsf{half}(4) = \mathsf{half}(2) + 1 = (\mathsf{half}(0) + 1) + 1 = 0 + 1 + 1 = 2$

Cut elimination "reverse engineers" the proof in order to extract this witness.

# Cuts

A **cut** is an elimination rule whose principal premise is proved by an introduction rule.

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma \vdash A} \qquad \dfrac{\pi'}{\Gamma \vdash B}}{\Gamma \vdash A \wedge B}\,(\wedge_I)}{\Gamma \vdash A}\,(\wedge_E^l) \qquad\qquad \dfrac{\dfrac{\dfrac{\pi}{\Gamma, A \vdash B}}{\Gamma \vdash A \Rightarrow B}\,(\Rightarrow_I) \qquad \dfrac{\pi'}{\Gamma \vdash A}}{\Gamma \vdash B}\,(\Rightarrow_E)$$

A **cut-free** proof is a proof without cuts.

# Cuts

An example of a proof with a cut is

$$\dfrac{\dfrac{\dfrac{}{A \vdash A}\,(\text{ax})}{A \vdash A \vee A}\,(\vee^{\text{l}}_{\text{I}}) \qquad \dfrac{}{A, A \vdash A}\,(\text{ax}) \qquad \dfrac{}{A, A \vdash A}\,(\text{ax})}{A \vdash A}\,(\vee_{\text{E}})$$

We can remove the cut and reduce it to

$$\dfrac{}{A \vdash A}\,(\text{ax})$$

# Cut elimination

**Theorem**
*If a sequent is provable then it has a cut-free proof.*

**Proof.**
The idea is to iteratively transform the proof of the original sequent in order to remove all cuts. □

# Cut elimination: conjunctions

We can eliminate cuts on $\land$:

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma \vdash A} \qquad \dfrac{\pi'}{\Gamma \vdash B}}{\Gamma \vdash A \land B}(\land_\mathsf{I})}{\Gamma \vdash A}(\land_\mathsf{E}^\mathsf{l}) \quad \rightsquigarrow \quad \dfrac{\pi}{\Gamma \vdash A}$$

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma \vdash A} \qquad \dfrac{\pi'}{\Gamma \vdash B}}{\Gamma \vdash A \land B}(\land_\mathsf{I})}{\Gamma \vdash B}(\land_\mathsf{E}^\mathsf{r}) \quad \rightsquigarrow \quad \dfrac{\pi'}{\Gamma \vdash B}$$

# Cut elimination: implications

We can eliminate cuts on $\Rightarrow$:

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma, A \vdash B}}{\Gamma \vdash A \Rightarrow B}\,(\Rightarrow_{\mathrm{I}}) \qquad \dfrac{\pi'}{\Gamma \vdash A}}{\Gamma \vdash B}\,(\Rightarrow_{\mathrm{E}}) \qquad \rightsquigarrow \qquad \dfrac{\pi[\pi'/A]}{\Gamma \vdash B}$$

where $\pi[\pi'/A]$ is $\pi$ where we have replaced all axioms on $A$

$$\dfrac{}{\Gamma, A, \Gamma' \vdash A}\,(\mathrm{ax}) \qquad \text{by} \qquad \dfrac{w(\pi')}{\Gamma, A, \Gamma' \vdash A}$$

where $w(\pi')$ is an appropriate weakening of $\pi$.

# Cut elimination: disjunctions

We can eliminate cuts on $\lor$:

$$
\cfrac{\cfrac{\cfrac{\pi}{\Gamma \vdash A}}{\Gamma \vdash A \lor B}\,(\lor_\mathrm{I}^\mathrm{l}) \qquad \cfrac{\pi'}{\Gamma, A \vdash C} \qquad \cfrac{\pi''}{\Gamma, B \vdash C}}{\Gamma \vdash C}\,(\lor_\mathrm{E}) \quad \rightsquigarrow \quad \cfrac{\pi'[\pi/A]}{\Gamma \vdash C}
$$

$$
\cfrac{\cfrac{\cfrac{\pi}{\Gamma \vdash B}}{\Gamma \vdash A \lor B}\,(\lor_\mathrm{I}^\mathrm{r}) \qquad \cfrac{\pi'}{\Gamma, A \vdash C} \qquad \cfrac{\pi''}{\Gamma, B \vdash C}}{\Gamma \vdash C}\,(\lor_\mathrm{E}) \quad \rightsquigarrow \quad \cfrac{\pi''[\pi/B]}{\Gamma \vdash C}
$$

# Cut elimination: termination

For instance,

$$
\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma, A \vdash A}\,(\mathrm{ax}) \qquad \dfrac{}{\Gamma, A \vdash A}\,(\mathrm{ax})}{\Gamma, A \vdash A \wedge A}\,(\wedge_\mathrm{I})}{\Gamma \vdash A \Rightarrow A \wedge A}\,(\Rightarrow_\mathrm{I}) \qquad \dfrac{\pi}{\Gamma \vdash A}}{\Gamma \vdash A \wedge A}\,(\Rightarrow_\mathrm{E})
$$

is transformed into

$$
\dfrac{\dfrac{\pi}{\Gamma \vdash A} \qquad \dfrac{\pi}{\Gamma \vdash A}}{\Gamma \vdash A \wedge A}\,(\wedge_\mathrm{I})
$$

Note that if $\pi$ contained $n$ cuts then we now have $2n$ cuts...

# Cut elimination: termination

It is true that every order we chose to remove the cuts, we will end up on a cut-free proof after a finite number of steps, but it is quite difficult to show.

However, here, we only need to show that *a particular way* of eliminating cuts will terminates and this is not too hard (more on this if we have time).

# Cut elimination

This cut elimination procedure is due to Gentzen (1930s).

We will see that it corresponds to “executing” a proof.

Or, as Girard put it:

> *A logic without cut elimination is like a car without an engine.*

Note that

- the cut-free proof is “simpler”,
- but it can be much bigger.

Think of a program computing the factorial of 1000.

# Cut elimination: an important consequence

**Proposition**
*A cut-free proof of* $\vdash A$ *necessarily ends with an introduction rule.*

Note that a cut-free proof of $\Gamma \vdash A$ does not necessarily end with an introduction rule (with $\Gamma$ non-empty): what should be the introduction rule for

$$A \vee B \vdash A \vee B$$

# Consistency

An easy way to implement a proof checker:

```
let is_valid_proof p = true
```

A logical system with easy proofs:

$$\frac{}{\Gamma \vdash A}\ (\text{trustme})$$

A logical system is **consistent** if there is at least one sequent which is not provable.

# Consistency

A logical system is **consistent** if there is at least one sequent which is not provable.

**Proposition**
*A logical system is consistent if and only if the formula $\bot$ is not provable.*

**Proof.**
If $\bot$ is not provable then the system is consistent.

If the system is consistent there is a non-provable sequent $\Gamma \vdash A$. If $\bot$ was provable we could deduce $A$:

$$\dfrac{\dfrac{\dfrac{\vdots}{\vdash \bot}}{\Gamma \vdash \bot}\,(\text{wk})}{\Gamma \vdash A}\,(\bot_E)$$

Contradiction. □

# Consistency

**Theorem**
*The logical system NJ is consistent.*

**Proof.**
Suppose that $\bot$ is provable.

By the cut elimination theorem, we would have a cut-free proof.

By previous theorem, it would end with an introduction rule.

But there is no introduction rule for $\bot$.

Contradiction. $\square$

**Remark**
Another way to formulate consistency:

there is no formula $A$ such that both $A$ and $\neg A$ are provable.

# Consistency

At the beginning of the 20th century, Hilbert wanted to construct a collection of axioms which one could use as foundations of mathematics.

Since we are at day one, there is no semantics yet (= pre-existing mathematical world), everything is purely syntactic.

Consistency is thus one of the only possible correctness criterion for such an axiomatics.

But we cannot use "meta-mathematics" to prove consistency: we should therefore look for a system proving its own consistency.

*Gödel's second incompleteness theorem*: this is impossible for a non-trivial system.

# Commutative cuts

Cut elimination does not simplify all the proofs: we would like

$$\dfrac{\dfrac{\dfrac{}{\bot \vdash \bot}\,(\mathrm{ax})}{\bot \vdash A \vee A}\,(\bot_{\mathrm{E}}) \qquad \dfrac{}{\bot, A \vdash A}\,(\mathrm{ax}) \qquad \dfrac{}{\bot, A \vdash A}\,(\mathrm{ax})}{\bot \vdash A}\,(\vee_{\mathrm{E}})$$

to simplify into

$$\dfrac{\dfrac{}{\bot \vdash \bot}\,(\mathrm{ax})}{\bot \vdash A}\,(\bot_{\mathrm{E}})$$

# Commutative cuts

A typical cut is

$$\cfrac{\cfrac{\cfrac{}{A \vdash A}\,(\text{ax}) \qquad \cfrac{}{A \vdash A}\,(\text{ax})}{A \vdash A \wedge A}\,(\wedge_{\text{I}})}{A \vdash A}\,(\wedge_{\text{E}}^{\text{l}})$$

Some “cuts” are “too far apart” to be eliminated:

$$\cfrac{\cfrac{\cfrac{}{\ldots \vdash B \vee C}\,(\text{ax}) \qquad \cfrac{\cfrac{}{\ldots \vdash A}\,(\text{ax}) \quad \cfrac{}{\ldots \vdash A}\,(\text{ax})}{A, B \vee C, B \vdash A \wedge A}\,(\wedge_{\text{I}}) \qquad \cfrac{\cfrac{}{\ldots \vdash A}\,(\text{ax}) \quad \cfrac{}{\ldots \vdash A}\,(\text{ax})}{A, B \vee C, C \vdash A \wedge A}\,(\wedge_{\text{I}})}{A, B \vee C \vdash A \wedge A}\,(\vee_{\text{E}})}{A, B \vee C \vdash A}\,(\wedge_{\text{E}}^{\text{l}})$$

This is due to the form of the rule

$$\cfrac{\Gamma \vdash A \vee B \qquad \Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma \vdash C}\,(\vee_{\text{E}})$$

where the $C$ comes out of nowhere.

# Commutative cuts

Those can be handled by adding the following elimination rules for **commutative cuts**:

$$\dfrac{\dfrac{\Gamma \vdash \bot}{\Gamma \vdash A}\,(\bot_{\mathrm{E}}) \qquad \dots}{\Gamma \vdash B}\,(?_{\mathrm{E}}) \quad \rightsquigarrow \quad \dfrac{\Gamma \vdash \bot}{\Gamma \vdash B}\,(\bot_{\mathrm{E}})$$

Part V

# Intuitionism

# Proving disjunctions

The following is in accordance to the intuitionistic point of view:

**Proposition**
*If $A \lor B$ is provable then either $A$ or $B$ is provable.*

**Proof.**
There is a cut-free proof, which begins by an introduction rule:

$$\dfrac{\dfrac{\pi}{\vdash A}}{\vdash A \lor B}\ (\lor^{\mathsf{l}}_{\mathsf{I}}) \qquad \text{or} \qquad \dfrac{\dfrac{\pi}{\vdash B}}{\vdash A \lor B}\ (\lor^{\mathsf{r}}_{\mathsf{I}})$$

and therefore we have a proof of $A$ or a proof of $B$. □

# Excluded middle

An interesting consequence is that

**Proposition**
*The law of **excluded middle** $X \vee \neg X$ is not provable.*

**Proof.**
If it was the case we would have either

- A proof of $\neg X$, which should begin with the introduction rule $\dfrac{\dfrac{\pi}{X \vdash \bot}}{\vdash \neg X}\ (\neg_{\mathrm{I}})$

  By substitution, $\pi$ should induce a proof $\dfrac{\vdots}{\top \vdash \bot}$

  By $\top$-strengthening, we thus have a proof $\dfrac{\vdots}{\vdash \bot}$

  But there is no introduction rule for $\bot$, contradiction. □

# Excluded middle

**Proposition**
*The law of **excluded middle** $X \vee \neg X$ is not provable.*

Of course this does not say that, for a given value of $X$, we cannot decide:

- for $X = \top$, $X$ is provable,
- for $X = \bot$, $\neg X$ is provable,
- for $X = Y \Rightarrow Y$, $X$ provable,
- etc.

but we cannot do it in a generic way.

# Excluded middle

Since $X \vee \neg X$ is not provable, maybe is it false? No.

**Proposition**
*The formula* $\neg(X \vee \neg X)$ *cannot be proved.*

**Proof.**
We can prove $\neg\neg(X \vee \neg X)$, see next slide.

If $\neg(X \vee \neg X)$ was also provable, we would have

$$\dfrac{\dfrac{\vdots}{\vdash \neg\neg(X \vee \neg X)} \qquad \dfrac{\vdots}{\vdash \neg(X \vee \neg X)}}{\vdash \bot}\;(\neg_E)$$

which is excluded since our logic is consistent. □

# Excluded middle

$$\neg(\neg X \vee X), X \vdash X \quad (\text{ax})$$

$$\neg(\neg X \vee X), X \vdash \neg(\neg X \vee X) \quad (\text{ax}) \qquad \neg(\neg X \vee X), X \vdash \neg X \vee X \quad (\vee_{\text{I}}^{\text{r}})$$

$$\neg(\neg X \vee X), X \vdash \bot \quad (\neg_{\text{E}})$$

$$\neg(\neg X \vee X) \vdash \neg X \quad (\neg_{\text{I}})$$

$$\vdash \neg(\neg X \vee X) \quad (\text{ax}) \qquad \neg(\neg X \vee X) \vdash \neg X \vee X \quad (\vee_{\text{I}}^{\text{l}})$$

$$\neg(\neg X \vee X) \vdash \bot \quad (\neg_{\text{E}})$$

$$\vdash \neg\neg(\neg X \vee X) \quad (\neg_{\text{I}})$$

# Intuitionistic vs classical logic

We have two logics:

- **intuitionistic logic**: formulas provable in NJ,
- **classical logic**: formulas valid in boolean models.

**Proposition**
*A formula which is intuitionistically provable is classically valid.*

But the converse is not true: $X \vee \neg X$ is classically valid but not provable.

# Classical logic: NK

We call NK the system obtained from NJ by adding the axiom

$$\frac{}{\Gamma \vdash A \lor \neg A}\ (\text{lem})$$

**Theorem**
*A formula is valid in boolean models if and only if it can be proved in NK.*

Another possible axiom is

$$\frac{}{\Gamma \vdash \neg\neg A \Rightarrow A}$$

**Exercise**
Show this.

# Classical logic

A typical classical reasoning:

**Proposition**
*There exist two irrational numbers $a$ and $b$ such that $a^b$ is rational.*

**Proof.**

We know that $\sqrt{2}$ is irrational (if $\sqrt{2} = p/q$ then $p^2 = 2q^2$, prime factors).

The number $\sqrt{2}^{\sqrt{2}}$ is either rational or irrational.

- If it is rational, we are done.
- Otherwise, take $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$, we have $a^b = 2$. □

Classical logic is not **constructive**: we don't know which one.

# Classical logic

Another typical reasoning:

**Proposition**
*For every program $p$, either it stops after a finite number of steps or it does not.*

However, no program can solve the **halting problem**.

As a variant, do we really want to accept the following?

$$\forall x \in \mathbb{R}. x = 0 \lor x \neq 0$$

# Classical logic

Intuitionism does not validate either

$$\neg\neg X \Rightarrow X$$

I don't have lost my key. Where is it?

# Classical logic

**Proposition**
*Either* $(\pi + e)$ *or* $(\pi - e)$ *is irrational.*

**Proof.**
Suppose that both $(\pi + e)$ and $(\pi - e)$ are irrational. Therefore

$$2\pi = (\pi + e) + (\pi - e)$$

is irrational. Contradiction (we know that $\pi$ is irrational). □

Whether $(\pi + e)$ is irrational is currently open, and similarly for $(\pi - e)$.

Logically, we have shown $\neg A \Rightarrow \bot$ and deduced $A$, i.e. used $\neg\neg A \Rightarrow A$.

# Classical logic: semantical intuition

As before, we interpret formulas:

- $[\![A]\!]$ is a set (of "proofs" of $A$)
- $[\![A \Rightarrow B]\!] = [\![A]\!] \to [\![B]\!]$ is the set of functions
- $[\![\bot]\!] = \emptyset$

In particular, $[\![\neg A]\!] = [\![A \Rightarrow \bot]\!] = [\![A]\!] \to \emptyset$. Thus,

- if $[\![A]\!] \neq \emptyset$ then $[\![\neg A]\!] = \emptyset$,
- if $[\![A]\!] = \emptyset$ then $[\![\neg A]\!] = \emptyset \to \emptyset = \{\text{one element}\}$.

Thus,

- if $[\![A]\!] = \emptyset$ then $[\![\neg\neg A]\!] = \emptyset$,
- if $[\![A]\!] \neq \emptyset$ then $[\![\neg\neg A]\!] = \{\text{one element}\}$.

# Classical logic: double negation translation

Can we really prove more in classical logic?

**Theorem (Glivenko 1929)**
*A sequent $\Gamma \vdash A$ is classically provable if and only if $\neg\neg\Gamma \vdash \neg\neg A$ is intuitionistically provable.*

where $\neg\neg\Gamma$ means double negating every formula in $\Gamma$.

**Theorem**
*Intuitionistic logic is consistent iff classical logic is consistent.*

**Proof.**
If classical logic is inconsistent, we have a classical proof of $\bot$ and thus an intuitionistic proof of $\neg\neg\bot$. However, the implication $\neg\neg\bot \Rightarrow \bot$ holds intuitionistically: We thus have an intuitionistic proof of $\bot$:

$$\dfrac{\dfrac{\vdots}{\vdash \neg\neg\bot \Rightarrow \bot} \qquad \dfrac{\pi}{\vdash \neg\neg\bot}}{\vdash \bot}\ (\Rightarrow_{\mathsf{E}})$$

□

# Classical logic: double negation translation

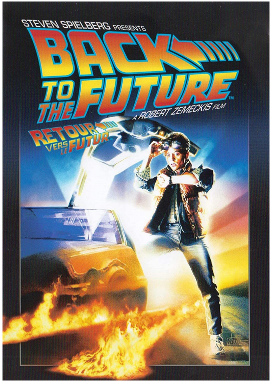
What about adding even more negations?

**Lemma**
*For $n > 0$, we have $\neg^{n+2} A \Leftrightarrow \neg^n A$.*

**Proof.**
The implications $A \Rightarrow \neg\neg A$ and $\neg\neg\neg A \Rightarrow A$ are intuitionistically provable. □

# Classical logic: operational intuition

Classical logic allows to “go back in time” and change our decisions based on current knowledge.




Use this to show $A \vee (A \Rightarrow \bot)$.

# Classical logic: formal operational intuition

Let us formalize this intuition by showing that the rule

$$\frac{\Gamma \vdash \neg\neg A}{\Gamma \vdash A}\ (\neg\neg_{\mathsf{E}})$$

allows us to derive

$$\neg A \vee A$$

# Excluded middle from double negation elimination

$$\dfrac{}{\neg(\neg A \vee A), A \vdash A}\ (\mathrm{ax})$$

$$\dfrac{}{\neg(\neg A \vee A), A \vdash \neg(\neg A \vee A)}\ (\mathrm{ax}) \qquad \dfrac{\neg(\neg A \vee A), A \vdash A}{\neg(\neg A \vee A), A \vdash \neg A \vee A}\ (\vee_{\mathrm{I}}^{\mathrm{r}})$$

$$\dfrac{\neg(\neg A \vee A), A \vdash \neg(\neg A \vee A) \qquad \neg(\neg A \vee A), A \vdash \neg A \vee A}{\neg(\neg A \vee A), A \vdash \bot}\ (\neg_{\mathrm{E}})$$

$$\dfrac{\neg(\neg A \vee A), A \vdash \bot}{\neg(\neg A \vee A) \vdash \neg A}\ (\neg_{\mathrm{I}})$$

$$\dfrac{}{\neg A \vee A)}\ (\mathrm{ax}) \qquad \dfrac{\neg(\neg A \vee A) \vdash \neg A}{\neg(\neg A \vee A) \vdash \neg A \vee A}\ (\vee_{\mathrm{I}}^{\mathrm{l}})$$

$$\dfrac{\qquad \neg(\neg A \vee A) \vdash \neg A \vee A}{\neg(\neg A \vee A) \vdash \bot}\ (\neg_{\mathrm{E}})$$

$$\dfrac{\neg(\neg A \vee A) \vdash \bot}{\vdash \neg\neg(\neg A \vee A)}\ (\neg_{\mathrm{I}})$$

$$\dfrac{\vdash \neg\neg(\neg A \vee A)}{\vdash \neg A \vee A}\ (\neg\neg_{\mathrm{E}})$$

More generally, we have proofs of the form

$$
\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma, \neg A \vdash \neg A}\,(\mathsf{ax}) \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma, \neg A, \Delta \vdash \neg A}\,(\mathsf{ax}) \qquad \dfrac{\vdots}{\Gamma, \neg A, \Delta \vdash A}}{\Gamma, \neg A, \Delta \vdash \bot}\,(\neg_{\mathsf{E}})}{\Gamma, \neg A, \Delta \vdash B}\,(\bot_{\mathsf{E}})}{\vdots}}{\Gamma, \neg A \vdash A}}{\Gamma, \neg A \vdash \bot}}{\Gamma \vdash \neg\neg A}\,(\neg_{\mathsf{I}})}{\Gamma \vdash A}\,(\neg\neg_{\mathsf{E}})
$$

# Intermediate logics

Are there intermediate principles between intuitionistic and classical?

Yes: for instance,

$$\neg\neg A \vee \neg A$$

or

$$(A \Rightarrow B) \vee (B \Rightarrow A)$$

Part VI

# Termination of cut elimination

# Termination of cut elimination

Remember that cut elimination was obtained by performing some transformations on proofs:

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma \vdash A} \qquad \dfrac{\pi'}{\Gamma \vdash B}}{\Gamma \vdash A \wedge B}\,(\wedge_\mathrm{I})}{\Gamma \vdash A}\,(\wedge_\mathrm{E}^\mathrm{l}) \quad \rightsquigarrow \quad \dfrac{\pi}{\Gamma \vdash A}$$

What we still have to show is that this process terminates at some point.

Intuitively, this can be achieved by associating a *size* (e.g. in $\mathbb{N}$) to each proof so that each reduction step is strictly decreasing:

$$\begin{array}{ccccccc} \pi_0 & \rightsquigarrow & \pi_1 & \rightsquigarrow & \pi_2 & \rightsquigarrow & \ldots \\ n_0 & > & n_1 & > & n_2 & > & \ldots \end{array}$$

# First try

Based on the previous rule, we could say that the size of a proof is the number of rules we use:

$$
\dfrac{\dfrac{\dfrac{}{\Gamma, A \vdash A}\,(\mathsf{ax}) \qquad \dfrac{}{\Gamma, A \vdash A}\,(\mathsf{ax})}{\Gamma, A \vdash A \wedge A}\,(\wedge_{\mathsf{I}})}{\Gamma \vdash A \Rightarrow A \wedge A}\,(\Rightarrow_{\mathsf{I}}) \qquad \dfrac{\pi}{\Gamma \vdash A}}{\Gamma \vdash A \wedge A}\,(\Rightarrow_{\mathsf{E}}) \quad \rightsquigarrow \quad \dfrac{\dfrac{\pi}{\Gamma \vdash A} \qquad \dfrac{\pi}{\Gamma \vdash A}}{\Gamma \vdash A \wedge A}\,(\wedge_{\mathsf{I}})
$$

$$
n_\pi + 5 \qquad > \qquad 2n_\pi + 1
$$

This does not work (and neither does the number of cuts).

We have more cuts, but they are smaller!

We have to come up with a much more subtle notion of size.

# Size of formulas

The **size** $|A|$ of a formula $A$ is its number of connectives:

$$
\begin{aligned}
|X| &= 1 \\
|\top| &= 1 \\
|\bot| &= 1 \\
|A \Rightarrow B| &= 1 + |A| + |B| \\
|A \land B| &= 1 + |A| + |B| \\
|A \lor B| &= 1 + |A| + |B|
\end{aligned}
$$

# Degree of a cut

The **degree** of a cut is the size of the cut formula.

For instance, the degree of

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma \vdash A} \qquad \dfrac{\pi'}{\Gamma \vdash B}}{\Gamma \vdash A \wedge B}\,(\wedge_{\mathsf{I}})}{\Gamma \vdash A}\,(\wedge_{\mathsf{E}}^{\mathsf{l}})$$

is

$$|A \wedge B| = 1 + |A| + |B|$$

# Degree of a proof

The **degree** of a proof is the multiset of the degrees of its cuts.

A **multiset** $M$ is a like a set but elements are counted with multiplicities:

$$\{a, b, a\} = \{a, a, b\} \neq \{a, b\}$$

We write $M \sqcup N$ for the (disjoint) union of multisets:

$$\{a, b, b\} \sqcup \{a, c\} = \{a, a, b, b, c\}$$

i.e.

$$(M \sqcup N)(x) = M(x) + N(x)$$

# Ordering multisets

We order multisets of natural numbers by $M > M'$ whenever $M'$ can be obtained from $M$ by iteratively replacing an element by (multiple) strictly smaller elements:

$$\{4, 4, 3\} > \{4, 3, 3, 3, 1\} > \{4, 3, 3, 3\} > \{4, 3, 3, 2, 2\} > \dots$$

**Theorem (Dershowitz-Manna)**
*There is no infinite strictly decreasing sequence of finite multisets.*

# Termination of cut elimination

Cut elimination makes the degree strictly decrease:

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma, A \vdash B}}{\Gamma \vdash A \Rightarrow B}\,(\Rightarrow_{\mathsf{I}}) \qquad \dfrac{\pi'}{\Gamma \vdash A}}{\Gamma \vdash B}\,(\Rightarrow_{\mathsf{E}}) \qquad \rightsquigarrow \qquad \dfrac{\pi[\pi'/A]}{\Gamma \vdash B}$$

$$M_\pi \sqcup \{|A \Rightarrow B|\} \sqcup M_{\pi'} \qquad > \qquad M_\pi \sqcup \{|A|, |A|, \ldots\} \sqcup (n \times M_{\pi'})$$

and we fail!

# Termination of cut elimination

For instance, we replace one cut on $A \Rightarrow A \wedge A$ by two on $A$:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma, A \vdash A}\,(\mathrm{ax}) \qquad \dfrac{}{\Gamma, A \vdash A}\,(\mathrm{ax})}{\Gamma, A \vdash A \wedge A}\,(\wedge_\mathrm{I})}{\Gamma \vdash A \Rightarrow A \wedge A}\,(\Rightarrow_\mathrm{I}) \qquad \dfrac{\pi}{\Gamma \vdash A}}{\Gamma \vdash A \wedge A}\,(\Rightarrow_\mathrm{E}) \quad \rightsquigarrow \quad \dfrac{\dfrac{\pi}{\Gamma \vdash A} \qquad \dfrac{\pi}{\Gamma \vdash A}}{\Gamma \vdash A \wedge A}\,(\wedge_\mathrm{I})$$

$$M_\pi \sqcup \{|A \Rightarrow A \wedge A|\} \qquad > \qquad M_\pi \sqcup \{|A|, |A|\}$$

Part VII

# Kripke semantics

# The completeness theorem

We have recalled the **completeness theorem** for classical logic:

**Theorem**
*A formula is classically provable if and only if it is valid, i.e. its interpretation is true for every valuation.*

Can we have a semantics with the same properties for intuitionistic logic?

# Kripke structures

A **Kripke structure** $(W, \leqslant, \rho)$ consists of

- a set $W$ of *worlds*,
- a partial order $\leqslant$,
- a function $\rho : W \to \mathcal{X} \to \{0, 1\}$

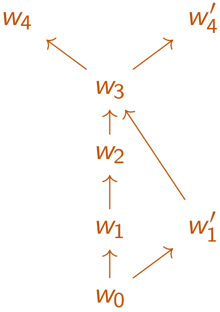
such that for every $w, w' \in W$

$$w \leqslant w' \text{ and } \rho(w, x) = 1 \qquad \text{implies} \qquad \rho(w', x) = 1$$

## Kripke structures

To every world $w$, the function $\rho$ associates a valuation $\rho w : \mathcal{X} \to \{0, 1\}$.

We can think of $w \leqslant w'$ as $w'$ being a **future** of $w$:




and the condition says:

what is true now will always be true in the future.

# Satisfaction

Given a Kripke structure $W$, a formula $A$ is **satisfied** in a world $w$, written

$$w \vDash_W A$$

when

$$\begin{array}{ll} w \vDash X & \text{iff } \rho(w, X) \\ w \vDash \top & \text{holds} \\ w \vDash \bot & \text{does not hold} \\ w \vDash A \wedge B & \text{iff } w \vDash A \text{ and } w \vDash B \\ w \vDash A \vee B & \text{iff } w \vDash A \text{ or } w \vDash B \\ w \vDash A \Rightarrow B & \text{iff, for every } w' \geqslant w,\ w' \vDash A \text{ implies } w' \vDash B \end{array}$$

What is $w \vDash \neg A = A \Rightarrow \bot$?

$$w \vDash \neg A \text{ iff, for every } w' \geqslant w,\ w' \vDash A \text{ does not hold}$$

# Validity

Given a context $\Gamma = A_i$, a formula $A$ and a Kripke structure $A$, we write

$$\Gamma \vDash_W A$$

when for every $w \in W$, if $w \vDash_W A_i$ for each $i$, then $w \vDash_W A$.

We write $\Gamma \vDash A$ when $\Gamma \vDash_W A$ for every Kripke structure $W$ and say that $A$ is **valid** in the context $\Gamma$.

# Soundness

**Theorem**
*If $\Gamma \vdash A$ is derivable intuitionistically then $\Gamma \vDash A$.*

**Proof.**
By induction. □

By contraposition:

- if $\Gamma \nvDash A$
- if, for some structure $W$, $\Gamma \nvDash_W A$
- if, for some structure $W$ and some $w$, $w \vDash A_i$ for all $i$ and $w \nvDash_W A$

then $\Gamma \vdash A$ is not derivable.

# An unprovable formula

Let's show that $\neg X \vee X$ is not provable.

Consider


with $w_0 \nvDash X$ and $w_1 \vDash X$.

We have $w_0 \nvDash \neg X$.

Therefore $w_0 \nvDash \neg X \vee X$.

# An unprovable formula

Let's show that $\neg\neg A \Rightarrow A$ is not provable.

Consider


with $w_0 \not\models X$ and $w_1 \models X$.

We have $w_0 \not\models \neg X$ and $w_1 \neg \models \neg X$, thus $w_0 \models \neg\neg X$.

But $w_0 \not\models X$, thus $w_0 \not\models \neg\neg X \Rightarrow X$.

## An unprovable formula

Suppose that $X$ means "I have my key".

Then $\neg X$ means "I have lost my key": I will never find it again in the future.

Then $\neg\neg X \Rightarrow X$ does not hold: it is not true that if I have not lost my key, I have my key (e.g. it could be somewhere in my apartment!).

# Completeness

The converse property also holds:

**Theorem**
$\Gamma \vdash A$ *is derivable intuitionistically iff* $\Gamma \vDash A$.