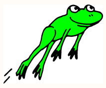
From Proof Nets to Combinatorial Proofs
—
A New Approach to Hilbert's 24th Problem

Willem Heijltjes and Lutz Straßburger

ESSLLI 2021 — Zoom — August 2-6, 2021



These are the slides an notes for the course *"From Proof Nets to Combinatorial Proofs — A New Approach to Hilbert's 24th Problem"* given at ESSLLI 2021. The summer school was planned to be held in Utrecht, but due the the Covid-19 crises it is being held online via Zoom.

Overview

1. The problem of proof identity
2. MLL: sequent proofs and proof nets
3. Cographs and handsome proof nets
4. Deep inference
5. ALL: sequent proofs, proof nets, and deep inference
6. Fibrations and skew fibrations
7. Classical propositional combinatorial proofs
8. First-order combinatorial proofs
9. Intuitionistic combinatorial proofs
10. Normalization

5 x 90 min $\Longrightarrow$ 10 x 45 min

MLL = multiplicative linear logic
ALL = additive linear logic

From Proof Nets to Combinatorial Proofs
—
A New Approach to Hilbert's 24th Problem

1. Lecture
The Problem of Proof Identity

Willem Heijltjes and Lutz Straßburger

What is Proof Theory?

- Group theory = theory of groups
  - well-established definition of group
  - two groups are the same if they are isomorphic
- Graph theory = theory of graphs
  - well-established definition of graph
  - two graphs are the same if they are isomorphic
- Proof theory = theory of (formal) proofs ???
  - no well-established definition of formal proof
  - no idea when two proofs are the same

What is Proof Theory?

At the current state of the art,
Proof theory is not the theory of proofs but
the theory of proof systems.

All important results in proof theory are about proof systems:

- soundness
- completeness
- cut elimination
- focusing
- p-equivalence

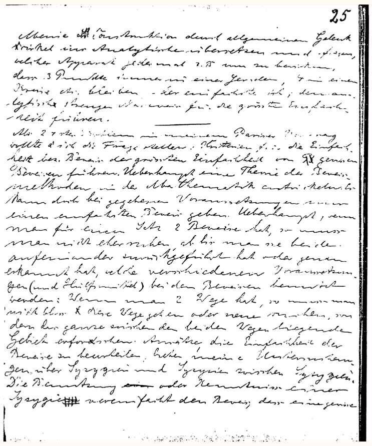
⋮

Can we make
proof theory a
theory of proofs?

Can we make proof theory a theory of proofs?

1. What is a proof?
   $\Rightarrow$ define proofs independently from the proof systems
2. When are two proofs the same?
   $\Rightarrow$ define a notion of proof identity

Hilbert's 24th problem



As 24th problem in my Paris lecture, I wanted to ask the question: Find criteria of simplicity or rather prove the greatest simplicity of given proofs. More generally develop a theory of proof methods in mathematics. Under given conditions there can be only one simplest proof. And if one has 2 proofs for a given theorem, then one must not rest before one has reduced one to the other or discovered which different premises (and auxiliary means) have been used in the proofs: When one has two routes then one must not just go these routes or find new routes, but the whole area lying between these two routes must be investigated…

Hilbert was thinking about adding the problem of proof identity as 24th problem to his famous lecture with the famous 23 problems that was held in 1900. But proof theory as a field was only established in 1928 with the appearance of the Book *"GrundzÃijge der theoretischen Logik"* by Hilbert and Ackermann. So, the problem of proof identity is older than proof theory itself.

Sources:

- picture of Hilbert: `https://de.wikisource.org/wiki/David_Hilbert?uselang=de#/media/Datei:Hilbert.jpg`
- Notebook of Hilbert: *David Hilbert, Mathematische Notizbücher, Niedersächsische Staats- und Universitätbibliothek, Cod. Ms. D. Hilbert 600:3, S.25* (Scan from a hardcopy made by Rüdiger Thiele)
- Translation: Lutz Straßburger

See also:

- *Rüdiger Thiele:* **"Hilbert's Twenty-Fourth Problem".** *American Mathematical Monthly 110, pp 1–24, 2003*

When are two proofs the same?

Normalization?

Curry-Howard-Correspondence
- formulas = types
- proofs = programs
- normalization = computation

fondations of functional programming languages

Two proofs are the same iff they have the same normal form.

- propositional logic: exponential blow-up
- predicate logic: elementary blow-up
- Identify a proof on an A4-page with a proof of the size of the universe
- corresponds to removing lemmas from a proof. But lemmas are important in mathematical proofs.
- Example: Normalizing Fürstenberg's proof of the inifinity of primes yields Euklid's proof

When are two proofs (in normal form) the same?

Rule permutation?

$$\vee\dfrac{\wedge\dfrac{\vdash \Gamma, A, B, C \qquad \vdash D, \Delta}{\vdash \Gamma, A, B, C \wedge D, \Delta}}{\vdash \Gamma, A \vee B, C \wedge D, \Delta} \quad \stackrel{?}{=} \quad \wedge\dfrac{\vee\dfrac{\vdash \Gamma, A, B, C}{\vdash \Gamma, A \vee B, C} \qquad \vdash D, \Delta}{\vdash \Gamma, A \vee B, C \wedge D, \Delta} \tag{1}$$

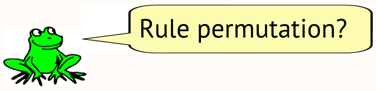
$$\mathsf{weak}\dfrac{\wedge\dfrac{\vdash \Gamma, C \qquad \vdash D, \Delta}{\vdash \Gamma, C \wedge D, \Delta}}{\vdash \Gamma, A, C \wedge D, \Delta} \quad \stackrel{?}{=} \quad \wedge\dfrac{\mathsf{weak}\dfrac{\vdash \Gamma, C}{\vdash \Gamma, A, C} \qquad \vdash D, \Delta}{\vdash \Gamma, A \vee B, C \wedge D, \Delta} \tag{2}$$

$$\vee\dfrac{\wedge\dfrac{\vdash \Gamma, A, B, C \qquad \vdash \Gamma, A, B, D}{\vdash \Gamma, A, B, C \wedge D}}{\vdash \Gamma, A \vee B, C \wedge D} \quad \stackrel{?}{=} \quad \wedge\dfrac{\vee\dfrac{\vdash \Gamma, A, B, C}{\vdash \Gamma, A \vee B, C} \qquad \vee\dfrac{\vdash \Gamma, A, B, D}{\vdash \Gamma, A \vee B, D}}{\vdash \Gamma, A \vee B, C \wedge D} \tag{3}$$

Two proofs are the same iff they can be transformed into each other via a sequence of rule permutation steps.

- works only for sequent calculus like formalisms
- PSPACE-hard if (2) is present
- exponential blow-up of the size of the proof if (3) is present

When are two proofs (in normal form) the same?

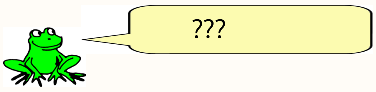


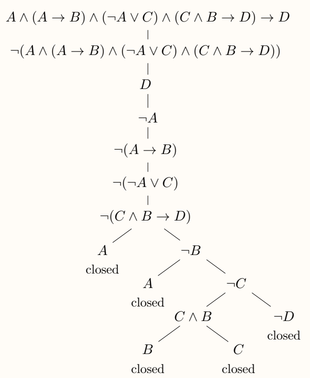
$$
{\scriptstyle\to_R}\dfrac{{\scriptstyle\wedge_L(3\times)}\dfrac{{\scriptstyle\to_L}\dfrac{{\scriptstyle\mathsf{con}}\dfrac{{\scriptstyle\wedge_R}\dfrac{{\scriptstyle\vee_L}\dfrac{{\scriptstyle\neg_L}\dfrac{{\scriptstyle\mathsf{axiom}}\dfrac{}{A\vdash A}}{A,\neg A\vdash}\quad {\scriptstyle\mathsf{axiom}}\dfrac{}{C\vdash C}}{A,\neg A\vee C\vdash C}\quad {\scriptstyle\to_L}\dfrac{{\scriptstyle\mathsf{axiom}}\dfrac{}{A\vdash A}\quad{\scriptstyle\mathsf{axiom}}\dfrac{}{B\vdash B}}{A,A\to B\vdash B}}{A,A,A\to B,\neg A\vee C\vdash C\wedge B}}{A,A\to B,\neg A\vee C\vdash C\wedge B}\quad {\scriptstyle\mathsf{axiom}}\dfrac{}{D\vdash D}}{A,A\to B,\neg A\vee C,C\wedge B\to D\vdash D}}{A\wedge(A\to B)\wedge(\neg A\vee C)\wedge(C\wedge B\to D)\vdash D}}{\vdash A\wedge(A\to B)\wedge(\neg A\vee C)\wedge(C\wedge B\to D)\to D}
$$

$$
{\scriptstyle\to_R}\dfrac{{\scriptstyle\wedge_L(3\times)}\dfrac{{\scriptstyle\mathsf{con}}\dfrac{{\scriptstyle\to_L}\dfrac{{\scriptstyle\mathsf{axiom}}\dfrac{}{A\vdash A}\quad {\scriptstyle\vee_L}\dfrac{{\scriptstyle\neg_L}\dfrac{{\scriptstyle\mathsf{axiom}}\dfrac{}{A\vdash A}}{A,\neg A\vdash}\quad {\scriptstyle\to_L}\dfrac{{\scriptstyle\wedge_R}\dfrac{{\scriptstyle\mathsf{axiom}}\dfrac{}{B\vdash B}\quad{\scriptstyle\mathsf{axiom}}\dfrac{}{C\vdash C}}{B,C\vdash C\wedge B}\quad {\scriptstyle\mathsf{axiom}}\dfrac{}{D\vdash D}}{B,C,C\wedge B\to D\vdash D}}{A,B,\neg A\vee C,C\wedge B\to D\vdash D}}{A,A,A\to B,\neg A\vee C,C\wedge B\to D\vdash D}}{A,A\to B,\neg A\vee C,C\wedge B\to D\vdash D}}{A\wedge(A\to B)\wedge(\neg A\vee C)\wedge(C\wedge B\to D)\vdash D}}{\vdash A\wedge(A\to B)\wedge(\neg A\vee C)\wedge(C\wedge B\to D)\to D}
$$

Example.
These two are equivalent modulo rule permutations.

When are two proofs (in normal form) the same?





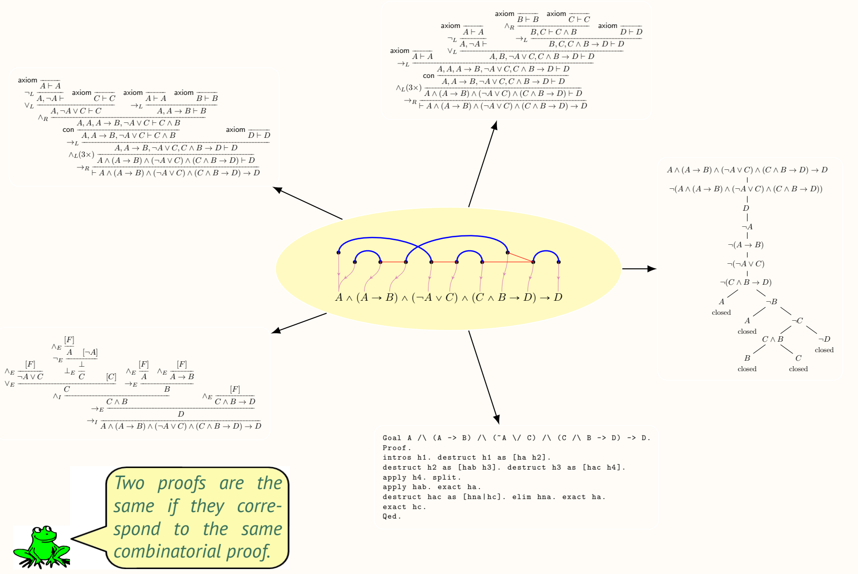
$$
{\scriptstyle\to_I}\dfrac{{\scriptstyle\to_E}\dfrac{{\scriptstyle\wedge_I}\dfrac{{\scriptstyle\vee_E}\dfrac{{\scriptstyle\wedge_E}\dfrac{[F]}{\neg A\vee C}\quad {\scriptstyle\bot_E}\dfrac{{\scriptstyle\neg_E}\dfrac{{\scriptstyle\wedge_E}\dfrac{[F]}{A}\quad[\neg A]}{\bot}}{C}\quad [C]}{C}\quad {\scriptstyle\to_E}\dfrac{{\scriptstyle\wedge_E}\dfrac{[F]}{A}\quad{\scriptstyle\wedge_E}\dfrac{[F]}{A\to B}}{B}}{C\wedge B}\quad {\scriptstyle\wedge_E}\dfrac{[F]}{C\wedge B\to D}}{D}}{A\wedge(A\to B)\wedge(\neg A\vee C)\wedge(C\wedge B\to D)\to D}
$$

```
Goal A /\ (A -> B) /\ (~A \/ C) /\ (C /\ B -> D) -> D.
Proof.
intros h1. destruct h1 as [ha h2].
destruct h2 as [hab h3]. destruct h3 as [hac h4].
apply h4. split.
apply hab. exact ha.
destruct hac as [hna|hc]. elim hna. exact ha.
exact hc.
Qed.
```


This is a semantic tableau, a natural deduction proof, and a Coq script, all proving the same formula.

Are these proofs "the same"?

Combinatorial Proof Identity



- The term "combinatorial proof identity" does not yet occur in the literature. We invented it for this course.
- This course is about the stuff that goes into the yellow blob in the middle.
- The technical details about "the yellow blob in the middle" depend on the logic. In every logic behaves differently when it comes to the strucure of its proofs. This means that the answer to the question of when two proofs are the same might be different for every logic. In this course we look into the following five logics:
  - classical propositional logic
  - classical first-order logic
  - intuitionistic propositional logic
  - multiplicative linear logic
  - additive linear logic

Classical Propositional Logic (CPL)

- *Formulas:* $A ::= a \mid \bar{a} \mid A \wedge B \mid A \vee B$
- *Negation:* $\bar{\bar{a}} = a \qquad \overline{A \wedge B} = \bar{A} \vee \bar{B} \qquad \overline{A \vee B} = \bar{A} \wedge \bar{B}$
- *Implication:* $A \supset B = \bar{A} \vee B$
- *Sequents:* $\Gamma ::= A_1, A_2, \ldots, A_k$
- *Inference rules (sequent calculus):*

$$\mathsf{ax}\,\frac{}{\vdash a, \bar{a}} \qquad \vee\,\frac{\vdash \Gamma, A, B}{\vdash \Gamma, A \vee B} \qquad \wedge\,\frac{\vdash \Gamma, A \quad \vdash \Delta, B}{\vdash \Gamma, \Delta, A \wedge B}$$

$$\mathsf{cont}\,\frac{\vdash \Gamma, A, A}{\vdash \Gamma, A} \qquad \mathsf{weak}\,\frac{\vdash \Gamma}{\vdash \Gamma, A}$$

- We are using formulas in *negation normal form* (NNF) because we need only half as many inference rules.
- We don't have the constants truth and falsum in the language to avoid unnecessary complications in later parts of the course. Note that in classical logic we can pick a fresh proposional variable a_0 and define truth as $a_0 \vee \bar{a}_0$ and falsum as $a_0 \wedge \bar{a}_0$.
- *Sequents* are multisets of formulas. The meaning is the disjunction of the formulas.
- In this course, we *always* consider the comma in the sequent notation to be associative and commutative.
- *Sequent derivations* are formally trees whose nodes are the instances of the inference rules, and whose edges are the sequents. *(Sequent) proofs* are derivations where all leaves are axioms.
- **Exercise 1.1:** Prove Pierce's law $((a \supset b) \supset a) \supset a$ in this sequent calculus.

First-Order Classical Logic (FOL) — Formulas

$$\begin{array}{rrcl}
\textit{Terms:} & t & ::= & x \mid f(t_1, \ldots, t_n) \\
\textit{Atoms:} & a & ::= & p(t_1, \ldots, t_m) \mid \bar{p}(t_1, \ldots, t_m) \\
\textit{Formulas:} & A & ::= & a \mid A \wedge A \mid A \vee A \mid \exists x.A \mid \forall x.A \\
\textit{Sequents:} & \Gamma & ::= & A_1, A_2, \ldots, A_k
\end{array}$$

Negation:

$$\begin{array}{rclrcl}
\bar{\bar{a}} & = & a & \overline{p(t_1, \ldots, t_m)} & = & \bar{p}(t_1, \ldots, t_m) \\
& & & \overline{\bar{p}(t_1, \ldots, t_m)} & = & p(t_1, \ldots, t_m) \\
\overline{A \wedge B} & = & \bar{A} \vee \bar{B} & \overline{\exists x.A} & = & \forall x.\bar{A} \\
\overline{A \vee B} & = & \bar{A} \wedge \bar{B} & \overline{\forall x.A} & = & \exists x.\bar{A}
\end{array}$$

- As in the propositional case, we consider formulas in NNF.
- We do not discuss semantics in this course.

First-Order Classical Logic (FOL) — Sequent Calculus

$$\mathsf{ax}\,\frac{}{\vdash a, \bar{a}} \qquad \vee\,\frac{\vdash \Gamma, A, B}{\vdash \Gamma, A \vee B} \qquad \wedge\,\frac{\vdash \Gamma, A \quad \vdash B, \Delta}{\vdash \Gamma, A \wedge B, \Delta}$$

$$\exists\,\frac{\vdash \Gamma, A[x/t]}{\vdash \Gamma, \exists x.A} \qquad \forall\,\frac{\vdash \Gamma, A}{\vdash \Gamma, \forall x.A}\ (x \text{ not free in } \Gamma)$$

$$\mathsf{cont}\,\frac{\vdash \Gamma, A, A}{\vdash \Gamma, A} \qquad \mathsf{weak}\,\frac{\vdash \Gamma}{\vdash \Gamma, A}$$

- We only need to add the rules for the quantifiers to the propositional system.
- We also do not discuss the cut rule

$$\mathsf{cut}\,\frac{\vdash \Gamma, A \quad \vdash \Delta, \bar{A}}{\vdash \Gamma, \Delta}$$

All sequent systems we discuss in this course admit cut elimination.

- **Exercise 1.2:** Prove the drinker's formula $\exists x.(px \supset \forall y.py)$ in the sequent calculus. '

Additive vs. Multiplicative

	multiplicative	additive
disjunction	$\vee\ \dfrac{\vdash \Gamma, A, B}{\vdash \Gamma, A \vee B}$	$\vee\ \dfrac{\vdash \Gamma, A}{\vdash \Gamma, A \vee B} \quad \vee\ \dfrac{\vdash \Gamma, B}{\vdash \Gamma, A \vee B}$
	$\downarrow$	$\downarrow$
	$\parr\ \dfrac{\vdash \Gamma, A, B}{\vdash \Gamma, A \parr B}$	$\oplus\ \dfrac{\vdash \Gamma, A}{\vdash \Gamma, A \oplus B} \quad \oplus\ \dfrac{\vdash \Gamma, B}{\vdash \Gamma, A \oplus B}$
conjunction	$\wedge\ \dfrac{\vdash \Gamma, A \qquad \vdash \Delta, B}{\vdash \Gamma, \Delta, A \wedge B}$	$\wedge\ \dfrac{\vdash \Gamma, A \qquad \vdash \Gamma, B}{\vdash \Gamma, A \wedge B}$
	$\downarrow$	$\downarrow$
	$\otimes\ \dfrac{\vdash \Gamma, A \qquad \vdash \Delta, B}{\vdash \Gamma, \Delta, A \otimes B}$	$\&\ \dfrac{\vdash \Gamma, A \qquad \vdash \Gamma, B}{\vdash \Gamma, A \,\&\, B}$

- When contraction and weakening are in the system, additive and multiplicative formulations of the and-rule (resp. or-rule) are equivalent. But when contraction and weakening are absent, they define different connectives.
- **Exercise 1.3:** Show that with contraction and weakening $A \parr B$ and $A \oplus B$ imply each other, and similarly for $A \otimes B$ and $A \,\&\, B$. Which implications hold when only weakening is present, and which when only contraction is present?
- The terminology "additive/multiplicative" is due to Girard. Same for the choice of symbols.
  - *Jean-Yves Girard:* **"Linear logic".** *Theoret. Comput. Sci. 50 (1), pp.1–102, 1987*

Multiplicative Linear Logic (MLL)

- *Formulas:* $A ::= a \mid a^\perp \mid A \otimes B \mid A \parr B$
- *Negation:* $a^{\perp\perp} = a,\ (A \otimes B)^\perp = A^\perp \parr B^\perp,\ (A \parr B)^\perp = A^\perp \otimes B^\perp$
- *Implication:* $A \multimap B = A^\perp \parr B$
- *Sequents:* $\Gamma ::= A_1, A_2, \ldots, A_k$
- *Inference rules (sequent calculus):*

$$\mathsf{ax}\ \frac{}{\vdash a, a^\perp} \qquad \parr\ \frac{\vdash \Gamma, A, B}{\vdash \Gamma, A \parr B} \qquad \otimes\ \frac{\vdash \Gamma, A \qquad \vdash \Delta, B}{\vdash \Gamma, \Delta, A \otimes B}$$

- **Exercise 1.4:** Find a formula that is provable in classical logic but not in MLL. What about the other way around?

Multiplicative Additive Linear Logic (MALL)

- *Formulas:* $A ::= a \mid a^\perp \mid A \otimes B \mid A \parr B \mid A \,\&\, B \mid A \oplus B$
- *Negation:* $a^{\perp\perp} = a,\quad (A \otimes B)^\perp = A^\perp \parr B^\perp,\ (A \parr B)^\perp = A^\perp \otimes B^\perp$
  $(A \,\&\, B)^\perp = A^\perp \oplus B^\perp,\ (A \oplus B)^\perp = A^\perp \,\&\, B^\perp$
- *Implication:* $A \multimap B = A^\perp \parr B$
- *Sequents:* $\Gamma ::= A_1, A_2, \ldots, A_k$
- *Inference rules (sequent calculus):*

$$\mathsf{ax}\ \frac{}{\vdash a, a^\perp} \qquad \parr\ \frac{\vdash \Gamma, A, B}{\vdash \Gamma, A \parr B} \qquad \otimes\ \frac{\vdash \Gamma, A \qquad \vdash \Delta, B}{\vdash \Gamma, \Delta, A \otimes B}$$

$$\&\ \frac{\vdash \Gamma, A \qquad \vdash \Gamma, B}{\vdash \Gamma, A \,\&\, B} \qquad \oplus\ \frac{\vdash \Gamma, A}{\vdash \Gamma, A \oplus B} \qquad \oplus\ \frac{\vdash \Gamma, B}{\vdash \Gamma, A \oplus B}$$

Additive Linear Logic (ALL)

- *Formulas:* $A ::= a \mid a^\perp \mid A \,\&\, B \mid A \oplus B$
- *Negation:* $a^{\perp\perp} = a \quad (A \,\&\, B)^\perp = A^\perp \oplus B^\perp,\ (A \oplus B)^\perp = A^\perp \,\&\, B^\perp$
- *Sequents:* $\Gamma ::= A_1, A_2, \ldots, A_k$
- *Inference rules (sequent calculus):*

$$\text{ax}\ \frac{}{\vdash a, a^\perp}$$

$$\&\ \frac{\vdash \Gamma, A \qquad \vdash \Gamma, B}{\vdash \Gamma, A \,\&\, B} \qquad \oplus\ \frac{\vdash \Gamma, A}{\vdash \Gamma, A \oplus B} \qquad \oplus\ \frac{\vdash \Gamma, B}{\vdash \Gamma, A \oplus B}$$

- Observe that every provable sequent in ALL has exactly two formulas.
- **Exercise 1.5:** Find a two-formula sequent that is provable in classical logic but not in ALL. What about the other way around?
- **Exercise 1.6:** Find a two-formula sequent that is provable in MLL but not in ALL. What about the other way around?

Intuitionistic Propositional Logic (IPL)

- *Formulas:* $A ::= a \mid A \wedge B \mid A \supset B$
- *Sequents:* $A_1, A_2, \ldots, A_k \vdash B$
- *Inference rules (sequent calculus):*

$$\text{ax}\ \frac{}{a \vdash a} \qquad \text{cont}\ \frac{\Gamma, A, A \vdash B}{\Gamma, A \vdash B} \qquad \text{weak}\ \frac{\Gamma \vdash B}{\Gamma, A \vdash B}$$

$$\wedge_L\ \frac{\Gamma, A, B \vdash C}{\Gamma, A \wedge B \vdash C} \qquad \wedge_R\ \frac{\Gamma \vdash A \qquad \Delta \vdash B}{\Gamma, \Delta \vdash A \wedge B}$$

$$\supset_L\ \frac{\Gamma \vdash A \qquad B, \Delta \vdash C}{\Gamma, A \supset B, \Delta \vdash C} \qquad \supset_R\ \frac{\Gamma, A \vdash B}{\Gamma \vdash A \supset B}$$

- In this course we only consider the disjunction-free fragment of intuitionistic logic ($\vee$ and $\perp$ are absent).
- Note that implication is now a primitive.
- Negation can be recovered by fixing a fresh propositional variable a_0 and define $\neg A = A \supset a_0$.
- We need two-sided sequents, and there is exactly one formula on the right.
- Each logical connective has a left-rule and a right-rule.
- **Exercise 1.7:** Can you prove Pierce's law $((a \supset b) \supset a) \supset a$ in intuitionistic logic?

Intuitionistic Multiplicative Linear Logic (IMLL)

- *Formulas:* $A ::= a \mid A \otimes B \mid A \multimap B$
- *Sequents:* $A_1, A_2, \ldots, A_k \vdash B$
- *Inference rules (sequent calculus):*

$$\text{ax}\ \frac{}{a \vdash a}$$

$$\otimes_L\ \frac{\Gamma, A, B \vdash C}{\Gamma, A \otimes B \vdash C} \qquad \otimes_R\ \frac{\Gamma \vdash A \qquad \Delta \vdash B}{\Gamma, \Delta \vdash A \otimes B}$$

$$\multimap_L\ \frac{\Gamma \vdash A \qquad B, \Delta \vdash C}{\Gamma, A \multimap B, \Delta \vdash C} \qquad \multimap_R\ \frac{\Gamma, A \vdash B}{\Gamma \vdash A \multimap B}$$

- Recall that in classical logic we can encode $A \supset B$ as $\bar{A} \vee B$. So, every formula in IPL can be seen as a formula in CPL.
- In the same way we have in linear logic that $A \multimap B$ is the same as $A^\perp \parr B$. Hence, every formula of IMLL is also a formula of MLL.
- **Exercise 1.8:** Find an IPL formula that is provable in CPL but not in IPL (or prove that such a formula does not exist).
- **Exercise 1.9:** Find an IMLL formula that is provable in MLL but not in IMLL (or prove that such a formula does not exist).