A Gentle Introduction to Deep Inference

7. Lecture

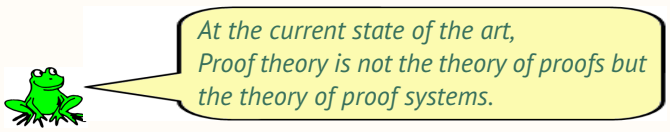
Combinatorial Proofs

Victoria Barrett and Lutz Straßburger

What is Proof Theory?

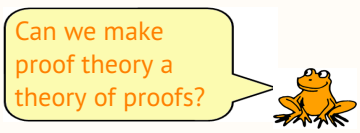
- Group theory = theory of groups
  - well-established definition of group
  - two groups are the same if they are isomorphic
- Graph theory = theory of graphs
  - well-established definition of graph
  - two graphs are the same if they are isomorphic
- Proof theory = theory of (formal) proofs ???
 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

What is Proof Theory?



All important results in proof theory are about proof systems:

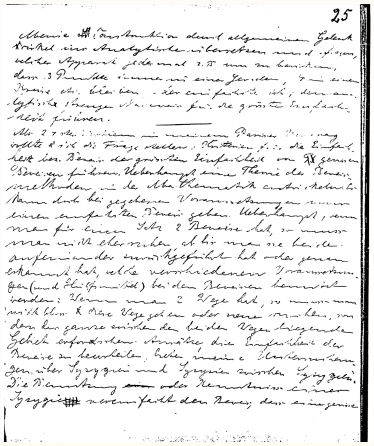
- soundness
- completeness
- cut elimination
- focusing
- p-equivalence
- ⋮



Can we make proof theory a theory of proofs?

1. What is a proof?
   ⇒ define proofs independently from the proof systems
2. When are two proofs the same?
   ⇒ 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 *"Grundzüge 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?

Curry-Howard-Correspondence

- formulas = types
- proofs = programs
- normalization = computation

fondations of functional programming languages

If we assume to proofs to be the same iff they have the same normal form, then proof identity is very expensive:

- for propositional logic: exponential blow-up
- for predicate logic: elementary blow-up
- We would identify a proof on an A4-page with a proof of the size of the universe
- It would correspond 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. See also:
  - Matthias Baaz, Stefan Hetzl, Alexander Leitsch, Clemens Richter, Hendrik Spohr: **"CERES: An analysis of Fürstenberg's proof of the infinity of primes".** *Theoretical Computer Science 403(2–3), pp.160–175, 2008*

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

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

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

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

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

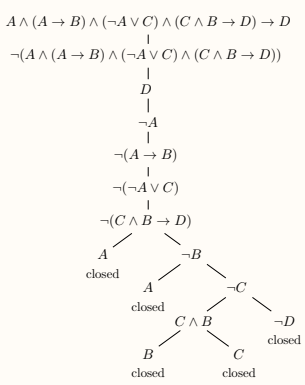
When are two proofs (in normal form) the same?

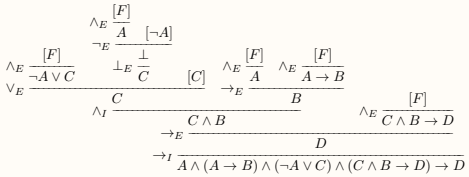
$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash A}\,\mathrm{axiom}}{A, \neg A \vdash}\,\neg_L \quad \dfrac{}{C \vdash C}\,\mathrm{axiom}}{A, \neg A \vee C \vdash C}\,\vee_L \quad \dfrac{\dfrac{}{A \vdash A}\,\mathrm{axiom} \quad \dfrac{}{B \vdash B}\,\mathrm{axiom}}{A, A \to B \vdash B}\,\to_L}{A,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

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

Example.
These two are equivalent modulo rule permutations.

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



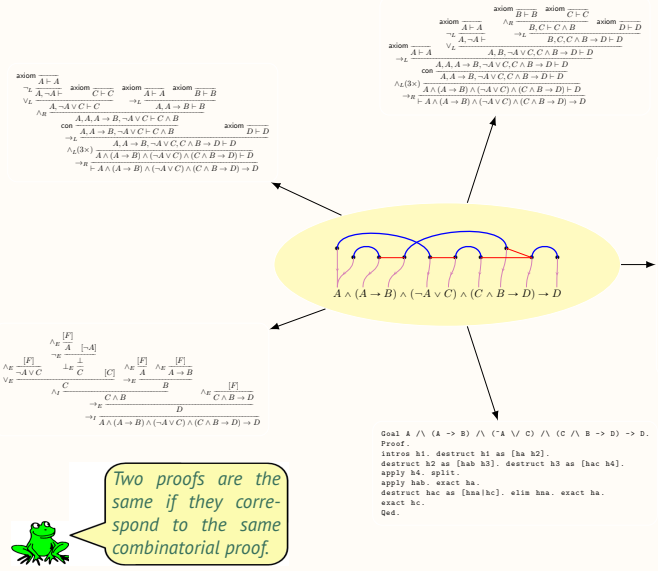


```
Goal A /\ (A -> B) /\ (~A \/ C) /\ (C /\ B -> D) -> D.
Proof.
intros h1. destruct h1 as [ha h2].
destruct h2 as [hab h3]. destruct h3 as [hac h4].
apply h4. split.
apply hab. exact ha.
destruct hac as [hna|hc]. elim hna. exact ha.
exact hc.
Qed.
```


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

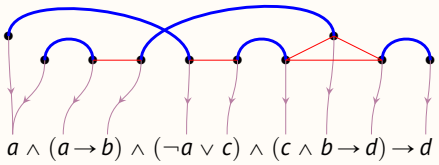
Are these proofs “the same”?

Combinatorial Proof Identity




```
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.
```


Example of a combinatorial proof



MLL axiom linking

cograph

skew fibration

conclusion

Overview

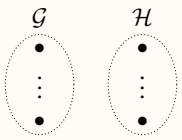
- formulas without syntax
- linear proofs without syntax
- contraction-weakening derivations without syntax
- decomposition theorems without syntax
- cut elimination without syntax

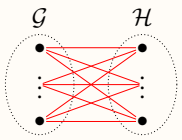
- Check out the notes for the ESSLLI 2021 course:
  - Willem Heijltjes and Lutz Straßburger: **"From Proof Nets to Combinatorial Proofs — A New Approach to Hilbert's 24th Problem".** `https://inria.hal.science/hal-03316571`

  The term "combinatorial proof identity" does not yet occur in the literature. It has been invented it for that course, which 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

From formulas to graphs

- *operations on graphs:*

$\mathcal{G} \vee \mathcal{H}$: 

$\mathcal{G} \wedge \mathcal{H}$: 

- *formulas:* $A, B ::= a \mid \bar{a} \mid A \wedge B \mid A \vee B$
- *equivalence of formulas:*

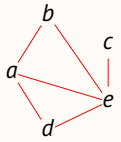
$$A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C \qquad A \wedge B \equiv B \wedge A$$
$$A \vee (B \vee C) \equiv (A \vee B) \vee C \qquad A \vee B \equiv B \vee A$$

- *from formulas to graphs:*

$[\![a]\!] = \bullet_a \qquad [\![\bar{a}]\!] = \bullet_{\bar{a}} \qquad [\![A \vee B]\!] = [\![A]\!] \vee [\![B]\!] \qquad [\![A \wedge B]\!] = [\![A]\!] \wedge [\![B]\!]$

From formulas to graphs

Example:

$((a \wedge (b \vee d)) \vee c) \wedge e \quad \longleftrightarrow$ 

Definition:
A *cograph* is an undirected P_4-free graph.
This mean that this configuration is forbidden:

Theorem:
An undirected graph is a cograph iff it is the graph of a formula.

Theorem:
$[\![A]\!] = [\![B]\!] \iff A \equiv B.$

- cographs have already been studied in the 1960s

Overview

- formulas without syntax ⇒ cographs
- linear proofs without syntax ⇒ cographs
- contraction-weakening derivations without syntax ⇒ cographs
- decomposition theorems without syntax ⇒ cographs
- cut elimination without syntax ⇒ cographs

From MLL to RB-cographs

- *MLL sequent calculus (unit-free):*

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

- *System MLS (unit-free):*

$$\text{ai}{\downarrow}\ \frac{B}{B \wedge (a \vee \bar{a})} \qquad \text{s}\ \frac{A \wedge (B \vee C)}{(A \wedge B) \vee C} \qquad \equiv \frac{A}{B}$$

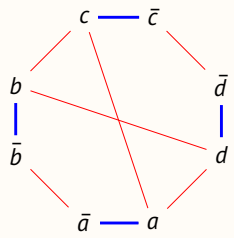
- *RB-cographs:*
  graphs with Red edges and Blue edges, such that
  - Red edges : cograph
  - Blue edges : perfect matching

- *Translating MLL sequent proof into and RB-cograph:*
  - axioms → Blue edges
  - cograph of conclusion → Red edges

From MLL to RB-cographs

Example:

$$\bar{a} \wedge \bar{b}, b \wedge c, a \wedge d, \bar{c} \wedge \bar{d}$$



Definition: An RB-cograph is *critically chorded* iff

- there is no chordless æ-cycle, and
- any two vertices are connected by a chordless æ-path.

Theorem:
An RB-cograph is the translation of a sequent proof iff it is critically chorded.

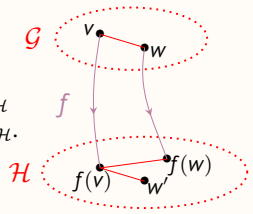
Overview

- formulas without syntax ⇒ cographs
- linear proofs without syntax ⇒ RB-cographs
- contraction-weakening derivations without syntax
- decomposition theorems without syntax
- cut elimination without syntax

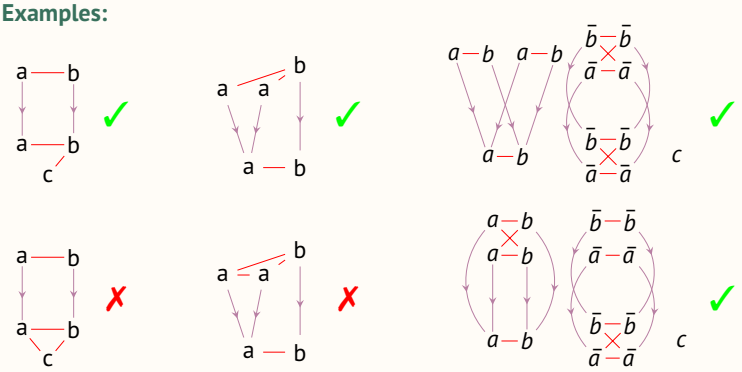
- This work is due to Christian Retoré:
  - Christian Retoré: **"Handsome proof-nets: perfect matchings and cographs".** *Theoretical Computer Science 294 (2003) 473–488*
  - Christian Retoré: **"Handsome proof-nets: R&B-graphs, perfect matchings and series-parallel graphs".** *Rapport de Recherche RR-3652, INRIA*

Skew fibrations

Definition:
A *skew fibration* is a graph homomorphism $f : \mathcal{G} \to \mathcal{H}$ such that for all $v \in V_{\mathcal{G}}$ and $w' \in V_{\mathcal{H}}$, if $\{f(v), w'\} \in E_{\mathcal{H}}$ then there is a w with $\{v, w\} \in E_{\mathcal{G}}$ and $\{w', f(w)\} \notin E_{\mathcal{H}}$.



Examples:



Skew fibrations

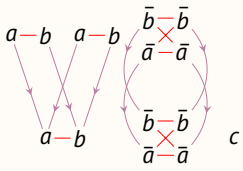
Recall the rules:

$$\mathrm{c}\downarrow \frac{A \vee A}{A} \qquad \mathrm{w}\downarrow \frac{B}{B \vee A}$$

Theorem: Let A and B be (classical logic) formulas.

Then there is a skew fibration $f : [\![A]\!] \to [\![B]\!]$ iff $\begin{array}{l} A \\ \| \, \mathrm{c}\downarrow,\mathrm{w}\downarrow,\equiv \\ B \end{array}$

Example:



$$\mathrm{w}\downarrow \frac{(a \wedge b) \vee (a \wedge b) \vee ((\bar{a} \vee \bar{b}) \wedge (\bar{a} \vee \bar{b}))}{\mathrm{c}\downarrow \dfrac{(a \wedge b) \vee (a \wedge b) \vee ((\bar{a} \vee \bar{b}) \wedge (\bar{a} \vee \bar{b})) \vee c}{(a \wedge b) \vee ((\bar{a} \vee \bar{b}) \wedge (\bar{a} \vee \bar{b})) \vee c}}$$

- formulas without syntax ⇒ cographs
- linear proofs without syntax ⇒ RB-cographs
- contraction-weakening derivations without syntax ⇒ skew fibrations
- decomposition theorems without syntax
- cut elimination without syntax

- This theorem has been proved independently by
  - Dominic Hughes: **"Towards Hilbert's 24th Problem: Combinatorial Proof Invariants: (Preliminary version)".** *ENTCS 165, 37–63, 2006*

  and
  - Lutz Straßburger: **"A Characterisation of Medial as Rewriting Rule".** *Proceedings of RTA 2007*

  by very different proofs.
- **Exercise 7.1:** Prove that

$$\begin{array}{l} A \\ \| \, \mathrm{c}\downarrow,\mathrm{w}\downarrow,\equiv \\ B \end{array} \quad \text{iff} \quad \begin{array}{l} A \\ \| \, \mathrm{ac}\downarrow,\mathrm{m},\mathrm{w}\downarrow,\equiv \\ B \end{array}$$

(this holds in the system with units as well as in the system without units.)

Yesterday: Decomposition theorems

unit-free variant of System SKS:

$$\mathsf{ai}{\downarrow}\ \frac{B}{B \wedge (a \vee \bar{a})} \qquad \mathsf{s}\ \frac{A \wedge (B \vee C)}{(A \wedge B) \vee C} \qquad \equiv \frac{A}{B} \qquad \mathsf{ai}{\uparrow}\ \frac{B \vee (a \wedge \bar{a})}{B}$$

$$\mathsf{w}{\downarrow}\ \frac{B}{B \vee A} \qquad \mathsf{ac}{\downarrow}\ \frac{a \vee a}{a} \qquad \mathsf{m}\ \frac{(A \wedge C) \vee (B \wedge D)}{(A \vee B) \wedge (C \vee D)} \qquad \mathsf{ac}{\uparrow}\ \frac{a}{a \wedge a} \qquad \mathsf{w}{\uparrow}\ \frac{B \wedge A}{B}$$

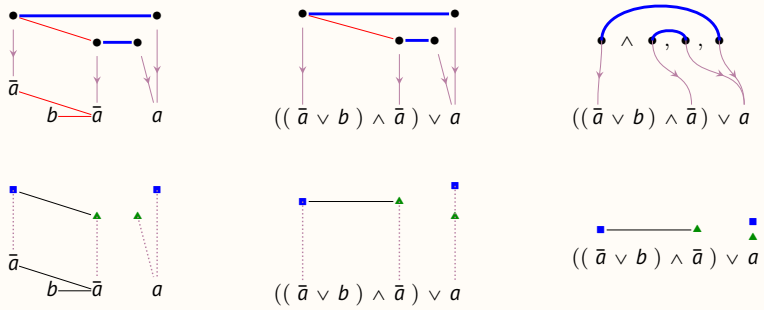
Theorem:

If $\begin{array}{l} A \\ \Vert\ \mathsf{SKS} \\ B \end{array}$ then $\begin{array}{l} A \\ \Vert\ \mathsf{w}{\uparrow},\mathsf{ac}{\uparrow},\mathsf{m} \\ A' \\ \Vert\ \mathsf{ai}{\downarrow},\mathsf{s},\mathsf{ai}{\uparrow} \\ B' \\ \Vert\ \mathsf{w}{\downarrow},\mathsf{ac}{\downarrow},\mathsf{m} \\ B \end{array}$ for some A', B'.

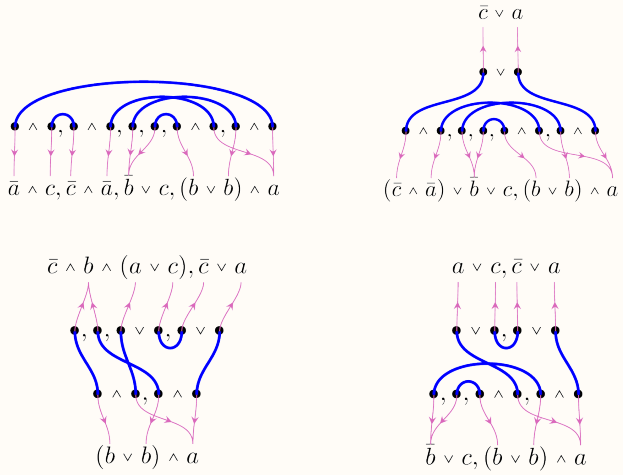
Combinatorial proofs (finally)

Definition:
A *combinatorial proof* of a formula A is a skew fibration $f : \mathcal{C} \to [\![A]\!]$ from a critically chorded RB-cograph $\mathcal{C}$ to the cograph of A, such that two vertices that paired in $\mathcal{C}$ are mapped to dual atoms in $[\![A]\!]$.

Example:



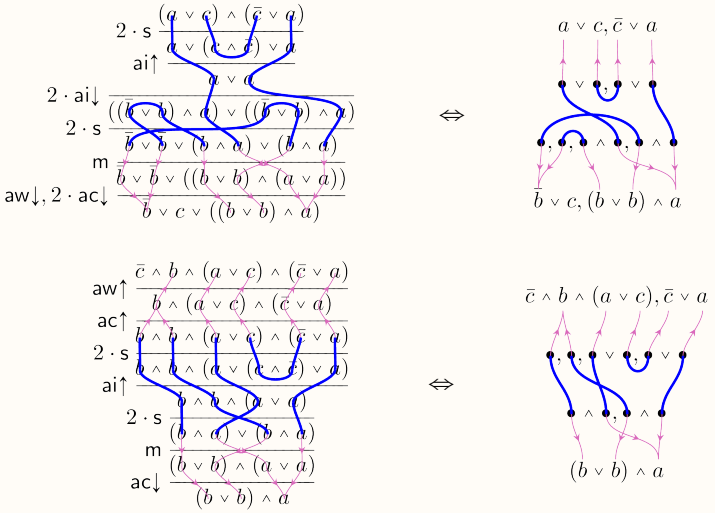
Combinatorial proofs and decomposition theorems



- Soundness and completeness of combinatorial proofs has been shown by
  - Dominic Hughes: **"Proofs Without Syntax".** *Annals of Mathematics 164(3), pp. 1065–1076, 2006*

- We can "flip" part of the conclusion.
- For details on this see
  - Lutz Straßburger: **"Combinatorial Flows and Their Normalisation".** *FSCD 2017*
  - Lutz Straßburger: **"Combinatorial Flows and Proof Compression".** *Inria RR-9048, 2017*

Combinatorial proofs and decomposition theorems

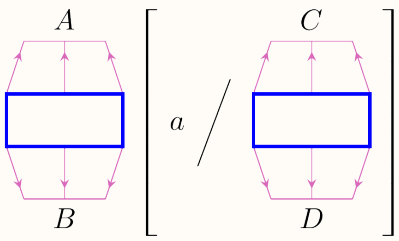


Overview

- formulas without syntax ⇒ cographs
- linear proofs without syntax ⇒ RB-cographs
- contraction-weakening derivations without syntax ⇒ skew fibrations
- decomposition theorems without syntax ⇒ combinatorial proofs
- cut elimination without syntax

Substitution of combinatorial proofs

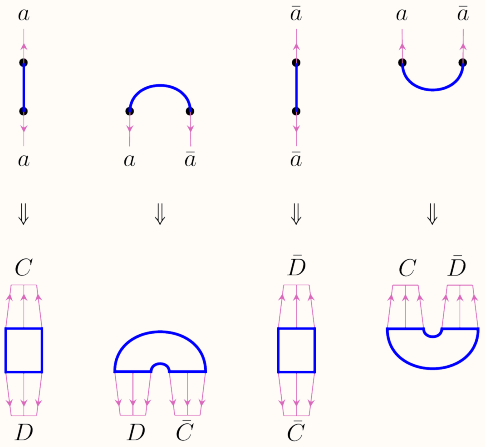
What is



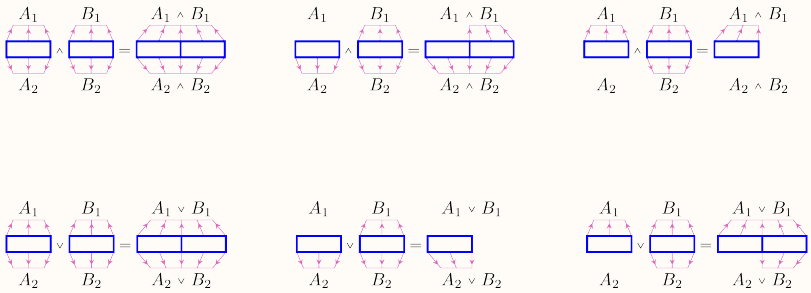
?

- We use here the *calculus of structures* notation, to make the correspondence between derivations and combinatorial proofs more visible.
- **Exercise 7.2:** Redo the pictures using *open deduction*.

Substitution of combinatorial proofs

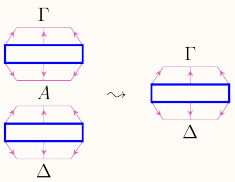


Horizontal composition of combinatorial proofs



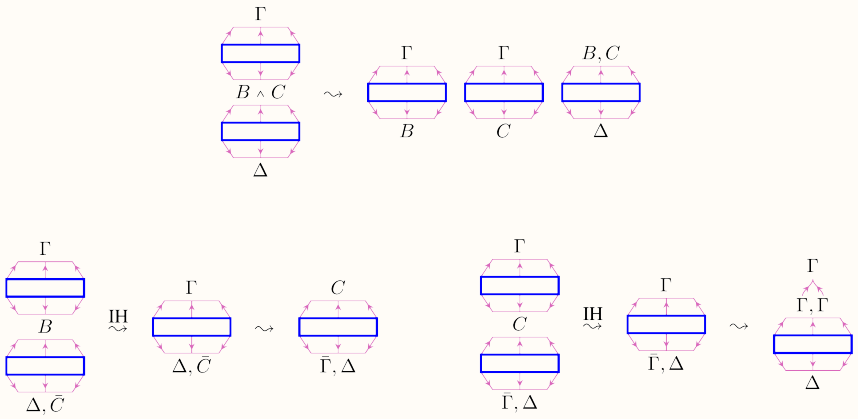
Vertical composition of combinatorial proofs

Wanted:

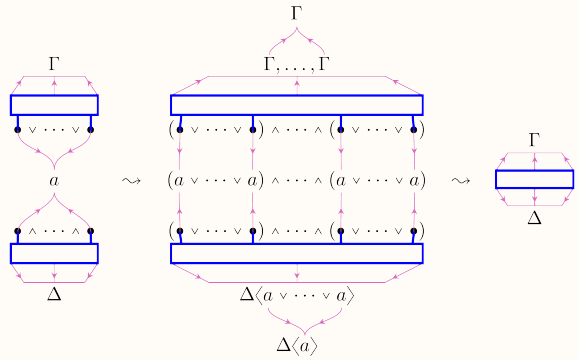


→ obtained by induction on *A*

Vertical composition of combinatorial proofs



Vertical composition of combinatorial proofs



Overview

- formulas without syntax ⇒ cographs
- linear proofs without syntax ⇒ RB-cographs
- contraction-weakening derivations without syntax ⇒ skew fibrations
- decomposition theorems without syntax ⇒ combinatorial proofs
- cut elimination without syntax ⇒ vertical composition of combinatorial proofs

Exercise 7.3: Do the case for $A = B \vee C$.