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

9. Lecture

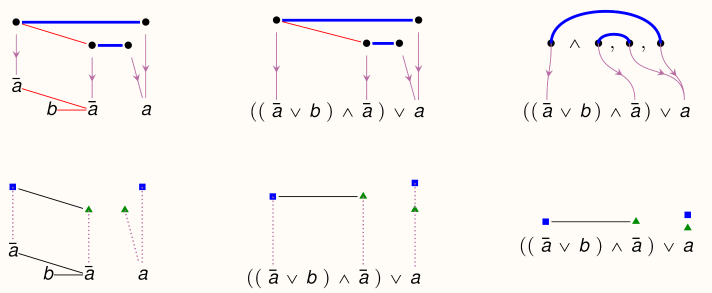
Intuitionistic Combinatorial Proofs

Willem Heijltjes and Lutz Straßburger

A Last Word on Classical Combinatorial Proofs

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

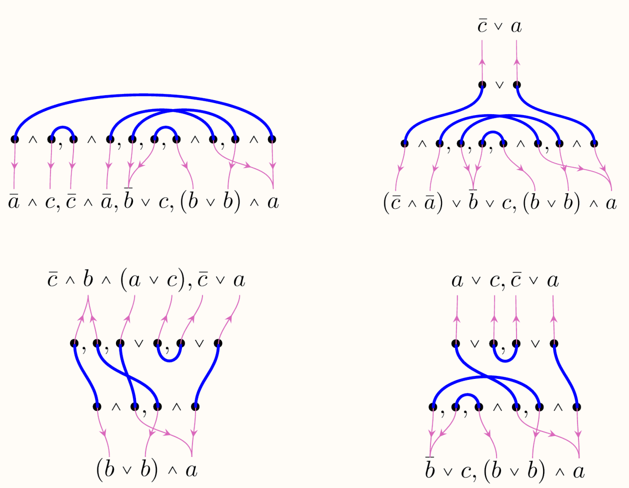
Example:



- In different publications and also in different lectures in this curse, different notations are used. But it should clear that these are indeed only different notations for the same thing.
- The last one on the first second row has the advantage of using the least amount of ink. It has been introduced in:
  - *Dominic Hughes:* **"Proofs Without Syntax".** *Annals of Mathematics, vol. 164, no. 3, pp. 1065–1076, 2006*
- The last one on the first row has been introduced in:
  - *Lutz Straßburger:* **"Combinatorial Flows and Their Normalisation".** *in 2nd International Conference on Formal Structures for Computation and Deduction (FSCD 2017). Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2017*

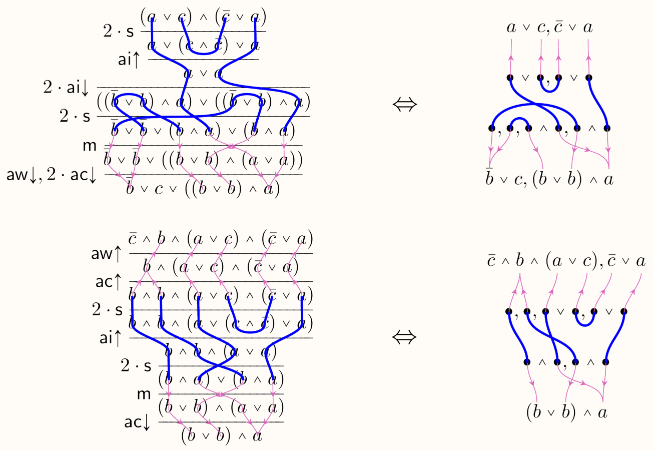
  It has the advantage that one can easily see the correspondence to the *flow graph* of the atoms in a derivation, as indicated on the following two slides.

Another Last Word on Classical Combinatorial Proofs

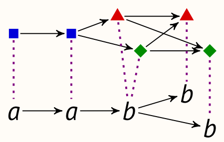


These are all the same combinatiorial proofs, just drawn in different ways with some fomulas in the conclusion flipped upside-down.

A Final Last Word on Classical Combinatorial Proofs (and Deep Inference)



From Classical to Intuitionistic Combinatorial Proofs



arena net

skew fibration

arena

$((a \supset a) \supset b) \supset (b \wedge b)$

cograph $=$ classical logic formula up to associativity and commutativity

arena $=$ intuitionistic logic formula up to associativity and commutativity

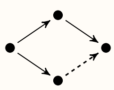
- ingredients to a combinatorial proof:

classical	intuitionistic
cograph	arena
RB-cograph	linked arena
critically chorded RB-cograph nicely colored cograph	arena net
skew fibration	skew fibration

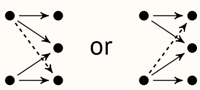
Arenas

Definition: An *arena* is a directed acyclic graph (dag) that is

- *L-free:* if $v \leftarrow u \rightarrow x \rightarrow w$ then $v \rightarrow w$

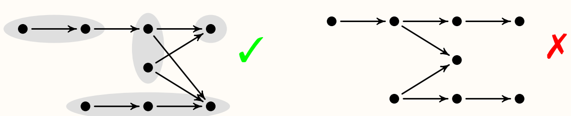


- *Σ-free:* if $u \leftarrow x \rightarrow v \leftarrow y \rightarrow w$ then $x \rightarrow w$ or $y \rightarrow u$



- and has a *partition* (equivalence relation $\sim$ on vertices)

Example:



The details for the material in this lecture can be found in

- *Willem Heijltjes and Dominic Hughes and Lutz Straßburger:* **"Intuitionistic Proofs without Syntax".** *LICS 2019*

From Formulas to Arenas

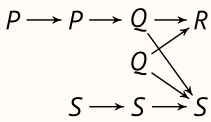
- *Operations on dags:*

$\mathcal{G}+\mathcal{H}$ $\qquad$ $\mathcal{G} \rhd \mathcal{H}$

- *Formulas:* $\quad A, B ::= P \mid A \wedge B \mid A \supset B$
- *Translating formulas to dags:*

$[\![P]\!] = \bullet \qquad [\![A\wedge B]\!] = [\![A]\!] + [\![B]\!] \qquad [\![A\supset B]\!] = [\![A]\!] \rhd [\![B]\!]$

Example: $\quad ((P \supset P) \supset Q) \wedge Q \;\supset\; R \wedge ((S \supset S) \supset S)$



From Formulas to Arenas

Example: $\quad ((P \supset P) \supset Q) \wedge Q \;\supset\; R \wedge ((S \supset S) \supset S)$

Theorem: A dag is an arena iff it is the translation of a formula.

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

where $\equiv$ is generated from

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

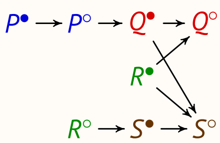
and $A \equiv B$ if A and B are the same up to a renaming of atoms.

- The term *arena* comes from games semantics, e.g.:
  - *Martin Hyland and Luke Ong:* **"On Full Abstraction for PCF: I. Models, observables and the full abstraction problem, II. Dialogue games and innocent strategies, III. A fully abstract and universal game model".** *Information and Computation 163, pp.285–408, 2000*
- However, the definition we present here originates from:
  - *Willem Heijltjes and Dominic Hughes and Lutz Straßburger:* **"Intuitionistic Proofs without Syntax".** *LICS 2019*
- The purpose of our definition definition is to cover exactly the notion of IPL formula modulo $\equiv$.

Arena Nets

- *linked arena:* every partition (link) consists of exactly two vertices: one even and one odd

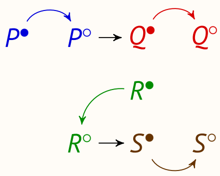
Example:



odd vertex (•) = odd depth
even vertex (◦) = even depth

- *link graph (of a linked arena):* remove all edges into even vertices add a link edge for each link (from odd to even)

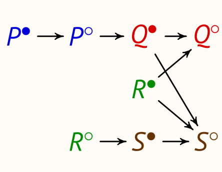
Example:



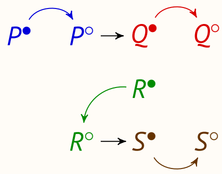
Arena Nets

Example:

linked arena



link graph



Definition: An *arena net* is a linked arena satisfying:

- *Acyclicity:* The link graph is acyclic.
- *Functionality:* In the link graph, every path from an odd vertex v to a root visits a consequent of v (in the arena).

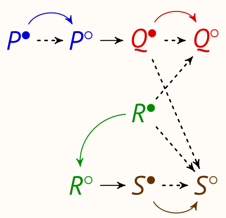
- An *arena net* is a linked arena that obeys a correctness criterion, i.e., that is a linked arena that comes from a proof.

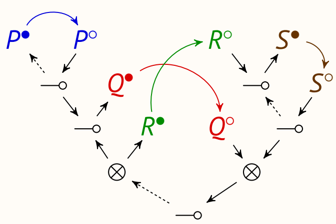
Arena Nets

Theorem: Let $[\![A]\!]$ be a linked arena. TFAE:

1. $[\![A]\!]$ is an arena net;
2. the corresponding linking on A forms an IMLL proof net for A;
3. $[\![A]\!]$ can be constructed via IMLL sequent calculus.

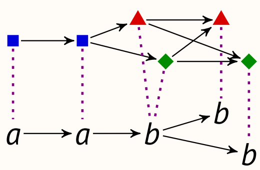
Example: $((P \supset P) \supset Q) \wedge R \;\supset\; Q \wedge ((R \supset S) \supset S)$





- Recall: IMLL stands for *intuitionistic multiplicative linear logic*.
- This theorem is due to
  - *Willem Heijltjes, Dominic Hughes and Lutz Straßburger:* **"Intuitionistic Proofs without Syntax".** *LICS 2019*
- Its proof shows the equivalence between the arena correctness criterion and the *essential net criterion* due to François Lamarche:
  - *François Lamarche:* **"Proof nets for intuitionistic linear logic I: Essential nets".** *Technical Report, Imperial College, London, 2004*

Intuitionistic Combinatorial Proofs



arena net

skew fibration

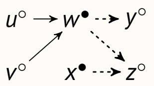
arena

$((a \supset a) \supset b) \supset (b \wedge b)$

Skew fibrations

$v \curlywedge w$ iff v and w are distinct and meet at odd depth or do not meet at all
$v \not\curlywedge w$ otherwise

Example:



$u \curlywedge v$ | $w \not\curlywedge x$
$u \curlywedge w$ | $w \not\curlywedge z$
$w \not\curlywedge w$ | $x \curlywedge y$

Definition: A *skew fibration* $f\colon \mathcal{G} \to \mathcal{H}$, of an arena $\mathcal{G}$ over an arena $\mathcal{H}$, is a function $f\colon V_\mathcal{G} \to V_\mathcal{H}$ which preserves

$$\begin{array}{rlll} \text{edges:} & v \rightarrowtriangle_\mathcal{G} w & \text{implies} & f(v) \rightarrowtriangle_\mathcal{H} f(w) \\ \text{equivalence:} & v \sim_\mathcal{G} w & \text{implies} & f(v) \sim_\mathcal{H} f(w) \\ \text{roots:} & r \not\rightarrowtriangle_\mathcal{G} & \text{implies} & f(r) \not\rightarrowtriangle_\mathcal{H} \\ \text{conjuncts:} & v \curlywedge_\mathcal{G} w & \text{implies} & f(v) \curlywedge_\mathcal{H} f(w) \end{array}$$

and satisfies the following *skew lifting* condition:

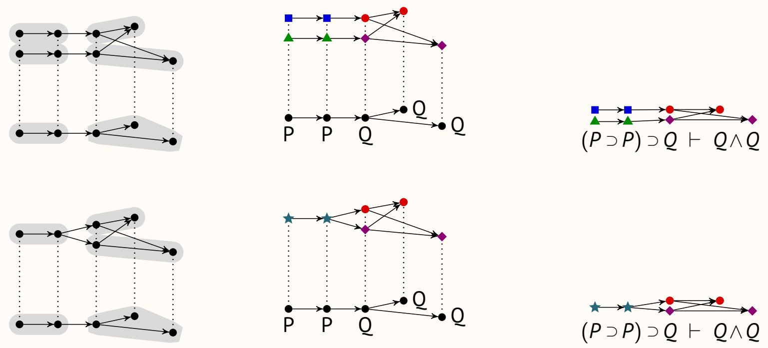
- if $f(v) \curlywedge_\mathcal{H} w$ then there exists u with $v \curlywedge_\mathcal{G} u$ and $f(u) \not\curlywedge_\mathcal{H} w$.

- The $\curlywedge$-relation simply recovers the cograph structure: If we translate $A \supset B$ to $\bar{A} \vee B$, and then translate the resulting formula into a cograph as discussed earlier this week, then we have $v \curlywedge w$ iff there is an edge between the corresponding vertices in the cograph.
- **Exercise 9.1:** : Prove that.
- As in all cases before, a skew fibration is a structure preserving map that additionally obeys *skew lifting*. The first two conditions in the definition demand that f is an arena homomophism, and the last one that it is a graph homomporphism on the cographs. The third condition is there since in intuitiionistic logic, $A \not\equiv \neg\neg A$.

Intuitionistic combinatorial proofs

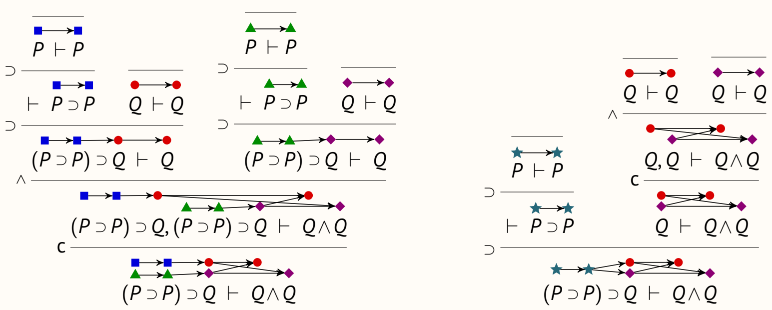
Definition: An *intuitionistic combinatorial proof* or *ICP* of a formula A is a skew fibration $f\colon \mathcal{G} \to [\![A]\!]$ of an arena net $\mathcal{G}$ over the arena $[\![A]\!]$.

Examples:



- In the examples, the actual ICPs are shown on the left. In the middle are the same objects in a more human-readable notation. On the right is a more compact notation, carrying the same information.
- Note that, different from the classical case, here we do not need the extra condition about the dual atoms in a link upstairs and the preservation of the labeling by the skew fibration. The reason is that in the intuitionistic case there are no negated atoms, and therefore the preservation of the partitioning by the skew fibration is enough.

From Sequent Calculus to ICP



Theorem: The translation $[\![\pi]\!]$ of a sequent proof π is an ICP.

Theorem: This translation is surjective.

Theorem: This translation is polynomial (in both directions).

Theorem: $[\![\pi_1]\!] = [\![\pi_2]\!]$ iff $\pi_1 \equiv \pi_2$ (modulo non-duplicating rule permutations).

- The statement of the third theorem is also called *polynomial full completeness* (and the term has been invented for ICP, following the *full completeness* known from game semantics).

Comparison to λ-Calculus

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{x:P\vdash x:P}}{\vdash \lambda x.x : P\supset P} \qquad \dfrac{}{w:Q\vdash w:Q}}{f_1:(P\supset P)\supset Q \vdash f_1(\lambda x.x):Q} \qquad \dfrac{\dfrac{\dfrac{}{y:P\vdash y:P}}{\vdash \lambda y.y : P\supset P} \qquad \dfrac{}{v:Q\vdash v:Q}}{f_2:(P\supset P)\supset Q \vdash f_2(\lambda y.y):Q}}{f_1:(P\supset P)\supset Q\,,\ f_2:(P\supset P)\supset Q \vdash \langle f_1(\lambda x.x), f_2(\lambda y.y)\rangle : Q\wedge Q}}{f:(P\supset P)\supset Q \vdash \langle f(\lambda x.x), f(\lambda y.y)\rangle : Q\wedge Q}$$

$$\dfrac{\dfrac{\dfrac{}{z:P\vdash z:P}}{\vdash \lambda z.z : P\supset P} \qquad \dfrac{\dfrac{\dfrac{}{v_1:Q\vdash v_1:Q} \quad \dfrac{}{v_2:Q\vdash v_2:Q}}{v_1:Q,\ v_2:Q \ \vdash\ \langle v_1,v_2\rangle : Q\wedge Q}}{v:Q\ \vdash\ \langle v,v\rangle : Q\wedge Q}}{f:(P\supset P)\supset Q \vdash \langle f(\lambda z.z), f(\lambda z.z)\rangle : Q\wedge Q}$$

Translating sequent proofs to λ-terms can cause exponential blow-up!

ICPs form a semantics of proofs that respects complexity.

Sequent Calculus Rule Permutations

$$\dfrac{\Gamma\vdash A \qquad \dfrac{B,\Delta,C\vdash D}{B,\Delta\vdash C\supset D}\supset_R}{\Gamma, A\supset B,\Delta\vdash C\supset D}\supset_L \quad\equiv\quad \dfrac{\dfrac{\Gamma\vdash A \qquad B,\Delta,C\vdash D}{\Gamma,A\supset B,\Delta,C\vdash D}\supset_L}{\Gamma,A\supset B,\Delta\vdash C\supset D}\supset_R \qquad ✓$$

$$\dfrac{\Gamma\vdash A \qquad \dfrac{\Delta\vdash C}{B,\Delta\vdash C}\text{weak}}{\Gamma,A\supset B,\Delta\vdash C}\supset_L \quad\equiv\quad \dfrac{\Delta\vdash C}{\Gamma,A\supset B,\Delta\vdash C}\text{weak} \qquad ✓$$

$$\dfrac{\Gamma\vdash A \qquad \dfrac{B,B,\Delta\vdash C}{B,\Delta\vdash C}\text{cont}}{\Gamma,A\supset B,\Delta\vdash C}\supset_L \quad\not\equiv\quad \dfrac{\dfrac{\Gamma\vdash A \qquad \dfrac{\Gamma\vdash A \qquad B,B,\Delta\vdash C}{B,\Gamma,A\supset B,\Delta\vdash C}\supset_L}{\Gamma,A\supset B,\Gamma,A\supset B,\Delta\vdash C}\supset_L}{\Gamma,A\supset B,\Delta\vdash C}\text{cont} \qquad ✗$$

- **Exercise 9.2:** How many possible rule permutations are there?

Comonoid Transformations

$$\dfrac{\dfrac{\dfrac{\Gamma,A,A,B,B\vdash C}{\Gamma,A,B,B\vdash C}\text{cont}}{\Gamma,A,B\vdash C}\text{cont}}{\Gamma,A\wedge B\vdash C}\wedge_L \quad\equiv\quad \dfrac{\dfrac{\dfrac{\Gamma,A,B,A,B\vdash C}{\Gamma,A\wedge B,A,B\vdash C}\wedge_L}{\Gamma,A\wedge B,A\wedge B\vdash C}\wedge_L}{\Gamma,A\wedge B\vdash C}\text{cont}$$

$$\dfrac{\dfrac{\dfrac{\Gamma\vdash C}{\Gamma,A\vdash C}\text{weak}}{\Gamma,A,B\vdash C}\text{weak}}{\Gamma,A\wedge B\vdash C}\wedge_L \quad\equiv\quad \dfrac{\Gamma\vdash C}{\Gamma,A\wedge B\vdash C}\text{weak}$$

$$\dfrac{\dfrac{\Gamma,A\vdash B}{\Gamma,A,A\vdash B}\text{weak}}{\Gamma,A\vdash B}\text{cont} \quad\equiv\quad \Gamma,A\vdash B$$

Formula-isomorphism transformations

$$\dfrac{\Gamma, A, B \vdash C}{\Gamma, A \wedge B \vdash C}\,\wedge_L \quad\equiv\quad \dfrac{\Gamma, A, B \vdash C}{\Gamma, B \wedge A \vdash C}\,\wedge_L$$

$$\dfrac{\Gamma \vdash A \quad \Delta \vdash B}{\Gamma, \Delta \vdash A \wedge B}\,\wedge_R \quad\equiv\quad \dfrac{\Delta \vdash B \quad \Gamma \vdash A}{\Gamma, \Delta \vdash B \wedge A}\,\wedge_R$$

$$\dfrac{\dfrac{\Gamma, A, B, C \vdash D}{\Gamma, A \wedge B, C \vdash D}\,\wedge_L}{\Gamma, (A \wedge B) \wedge C \vdash D}\,\wedge_L \quad\equiv\quad \dfrac{\dfrac{\Gamma, A, B, C \vdash D}{\Gamma, A, B \wedge C \vdash D}\,\wedge_L}{\Gamma, A \wedge (B \wedge C) \vdash D}\,\wedge_L$$

$$\dfrac{\dfrac{\Gamma \vdash A \quad \Delta \vdash B}{\Gamma, \Delta \vdash A \wedge B}\,\wedge_R \quad \Lambda \vdash C}{\Gamma, \Delta, \Lambda \vdash (A \wedge B) \wedge C}\,\wedge_R \quad\equiv\quad \dfrac{\Gamma \vdash A \quad \dfrac{\Delta \vdash B \quad \Lambda \vdash C}{\Delta, \Lambda \vdash B \wedge C}\,\wedge_R}{\Gamma, \Delta, \Lambda \vdash A \wedge (B \wedge C)}\,\wedge_R$$

$$\dfrac{\dfrac{\Gamma, A, B \vdash C}{\Gamma, A \wedge B \vdash C}\,\wedge_L}{\Gamma \vdash A \wedge B \supset C}\,\supset_R \quad\equiv\quad \dfrac{\dfrac{\Gamma, A, B \vdash C}{\Gamma, A \vdash B \supset C}\,\supset_R}{\Gamma \vdash A \supset B \supset C}\,\supset_R$$

$$\dfrac{\dfrac{\Gamma \vdash A \quad \Delta \vdash B}{\Gamma, \Delta \vdash A \wedge B}\,\wedge_R \quad C, \Lambda \vdash D}{\Gamma, \Delta, A \wedge B \supset C, \Lambda \vdash D}\,\supset_L \quad\equiv\quad \dfrac{\Gamma \vdash A \quad \dfrac{\Delta \vdash B \quad C, \Lambda \vdash D}{\Delta, B \supset C, \Lambda \vdash D}\,\supset_L}{\Gamma, \Delta, A \supset B \supset C, \Lambda \vdash D}\,\supset_L$$