# On Intuitionistic Combinatorial Proofs

Willem B. Heijltjes, Dominic J. D. Hughes, and Lutz Straßburger

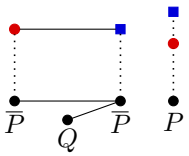
The objective of this presentation is simple to state:

1. Provide the most abstract, syntax-free representation of intuitionistic sequent calculus proofs possible, subject to:

2. Translation from a proof is polynomial-time.

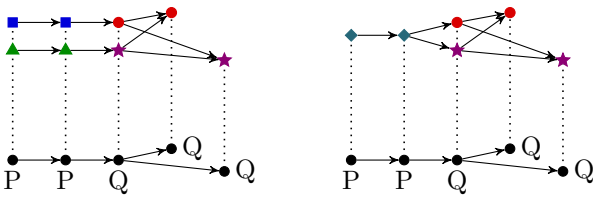
Conventional representations such as lambda calculus or game semantics fail to satisfy 2: by their extensional nature, they identify so many proofs that translation from a proof blows up exponentially in size.

Our solution is to define a notion of *combinatorial proof* for intuitionistic propositional sequent calculus. Combinatorial proofs were introduced as a syntax-free reformulation of classical propositional logic [Hug06a, Hug06b]. For example, here is a combinatorial proof of Peirce's Law $((P \Rightarrow Q) \Rightarrow P) \Rightarrow P$:




The lower graph abstracts the formula (one vertex per propositional variable, edges encoding conjunctive relationships); the upper graph has two colour classes, ● ● and ■ ■, each expressing an axiom $P \Rightarrow P$; the dotted lines define a *skew fibration* from the upper graph to the lower graph, a lax notion of graph fibration. The upper graph captures the axioms and logical rules in a proof, the lower graph captures the formula proved, and the skew fibration captures all contraction and weakening, simultaneously and in parallel [Hug06b, Str07].

The intuitionistic setting required reformulating combinatorial proofs with directed edges for implicative relationships. Here are two intuitionistic combinatorial proofs on $(P \Rightarrow P) \Rightarrow Q \vdash Q \wedge Q$,




(1)

Each lower graph, called the *base*, is an abstraction of the formula (akin to a labelled a arena of game semantics [HO00]). Leaving base graphs implicit, we can render the combinatorial proofs compactly:


Using this compact notation, Figure 1 shows step-by-step translations of intuitionistic sequent calculus proofs into the respective intuitionsitic combinatorial proofs above. Figure 2

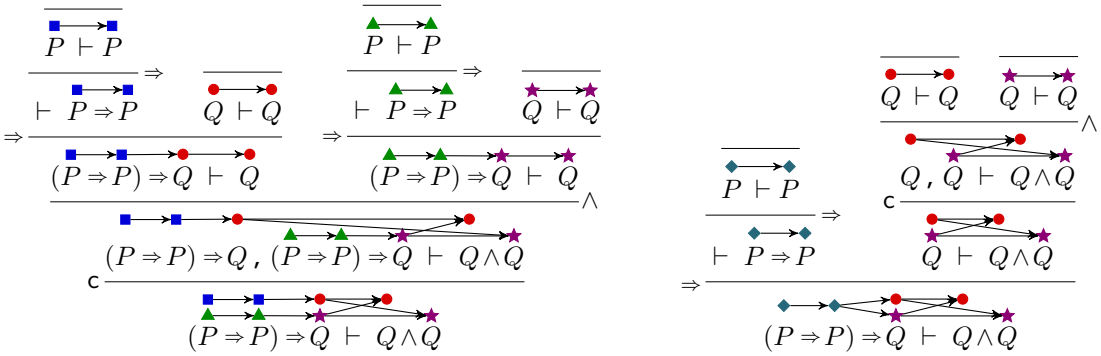



Figure 1: Translating two intuitionstic sequent calculus proofs to intuitionistic combinatorial proofs. The translation is very simple to define: (1) place a pair of tokens atop the propositional variables in each axiom, with a rightward directed edge; (2) trace the tokens down through the proof; (3) each left implication rule and right conjunction rule inserts edges.

---

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

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

Figure 2: Translating the same two intuitionstic sequent calculus proofs into lambda calculus terms. Note that (up to alpha-conversion, renaming bound variables $x$, $y$ and $z$) the two terms are the same. On the right, the subterm $\lambda z.z$ from the left sub-proof is duplicated, because of extensionality. In contrast, the translation to a combinatorial proof does not require such a duplication: on the right of Figure 1, the final rule keeps only one pair of tokens over $P \Rightarrow P$, from the left sub-proof.

---

shows the corresponding lambda calculus translations. The resulting lambda terms are identical (modulo alpha-conversion), and the right translation duplicates $\lambda z.z$. Because of iterated duplications, translation to a lambda term is exponential-time in the size of the proof. In contrast, translating the right proof to an intuitionistic combinatorial proof involves no duplication. More generally, a proof with $n$ axioms translates to an intuitionistic combinatorial proof with $n$ colour classes. Thus translation to an intuitionistic combinatorial proof is polynomial-time.

Just as the translation to lambda calculus is surjective, we can prove that the translation to intuitionistic combinatorial proofs is surjective. Thus intuitionistic combinatorial proofs are sound and complete for intuitionistic logic. We also prove that if two proofs are equivalent modulo rule commutations which do not involve duplications of entire subproofs, then they translate to the same combinatorial proofs. Taken together, these two theorems formalize the sense in which achieved the two goals stated at the start of this abstract.

In the presentation we will also compare the normalization procedures for classical combinatorial proofs (as presented in [Hug06b, Str17a, Str17b]) and for intuitionistic combinatorial proofs. A surprising observation is that in the intuitionistic case we need to rely on a normalization method for additive linear logic, as presented in [HH15].

If time permits, we will also show how we can translate between syntactic proofs and combinatorial proofs. Here we can observe for the intuitionistic case the same technical subtleties as for the classical case in [Hug06b, AS18].

# References


[AS18] Matteo Acclavio and Lutz Straßburger. From syntactic proofs to combinatorial proofs. In Didier Galmiche, Stephan Schulz, and Roberto Sebastiani, editors, *Automated Reasoning - 9th International Joint Conference, IJCAR 2018, Held as Part of the Federated Logic Conference, FloC 2018, Oxford, UK, July 14-17, 2018, Proceedings*, volume 10900, pages 481–497. Springer, 2018.

[HH15] Willem Heijltjes and Dominic J. D. Hughes. Complexity bounds for sum-product logic via additive proof nets and petri nets. In *LICS'15*, pages 80–91. IEEE Computer Society, 2015.

[HO00] J. M. E. Hyland and C.-H. Luke Ong. On full abstraction for PCF: I, II, and III. *Information and Computation*, 163(2):285–408, 2000.

[Hug06a] Dominic Hughes. Proofs Without Syntax. *Annals of Mathematics*, 164(3):1065–1076, 2006.

[Hug06b] Dominic Hughes. Towards Hilbert's $24^{\text{th}}$ problem: Combinatorial proof invariants: (preliminary version). *ENTCS*, 165:37–63, 2006.

[Str07] Lutz Straßburger. A characterisation of medial as rewriting rule. In Franz Baader, editor, *RTA'07*, volume 4533 of *LNCS*, pages 344–358. Springer, 2007.

[Str17a] Lutz Straßburger. Combinatorial Flows and Proof Compression. Research Report RR-9048, Inria Saclay, 2017.

[Str17b] Lutz Straßburger. Combinatorial flows and their normalisation. In Dale Miller, editor, *FSCD 2017*, volume 84 of *LIPIcs*, pages 31:1–31:17. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2017.