On Proof Equivalence and Combinatorial Proofs

Matteo Acclavio

SDU
University of Southern Denmark

VILLUM FONDEN

"X-IDF: Explainable Internet Data Flows"

Urbino 05/09/2023

- What is a proof?
- When two proofs are the same? and why should we care about?
- Normalization vs Generality
- Proof equivalence via rule permutations
- From rule permutations to Generality
- Combinatorial Proofs and Proof Equivalence
- Comparing Proof Equivalences
- Related and Future Works

What is a proof?

A proof is...

- A sequence of instructions

A proof is...

- A sequence of instructions
- A strategy to win an argumentation

A proof is...

- A sequence of instructions
- A strategy to win an argumentation
- The sound relations between the components of a statement

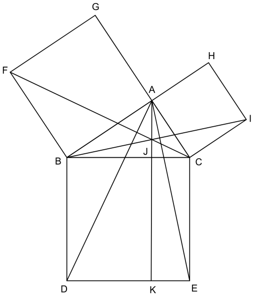
When two proofs are the same?

Pythagorean theorem

There are many different proofs of the Pythagorean theorem

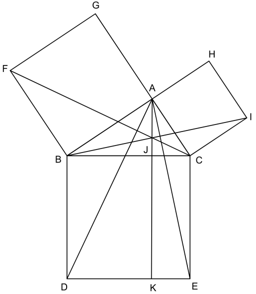
Pythagorean theorem

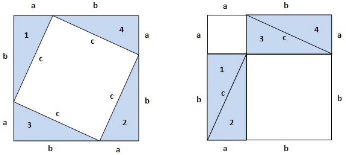
There are many different proofs of the Pythagorean theorem



Pythagorean theorem

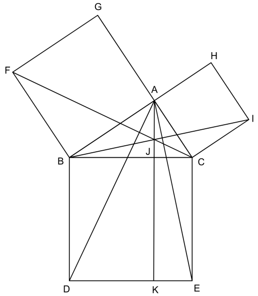
There are many different proofs of the Pythagorean theorem

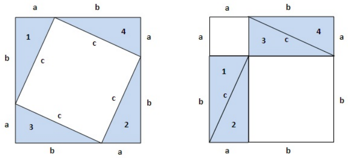




Pythagorean theorem

There are many different proofs of the Pythagorean theorem



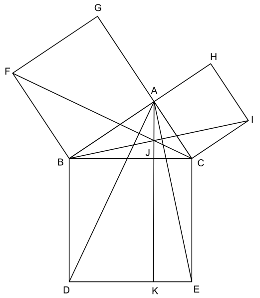


More proofs (122) available at

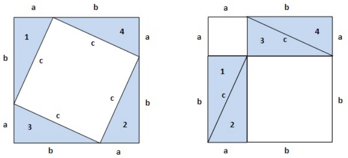
`http://www.cut-the-knot.org/pythagoras/index.shtml`

Pythagorean theorem

There are many different proofs of the Pythagorean theorem



$\stackrel{?}{\simeq}$



More proofs (122) available at

`http://www.cut-the-knot.org/pythagoras/index.shtml`

Why should we care about?

Definition

Proof theory is the branch of mathematical logic that studies proofs as formal mathematical objects.

Definition

Proof theory is the branch of mathematical logic that studies proofs as formal mathematical objects.

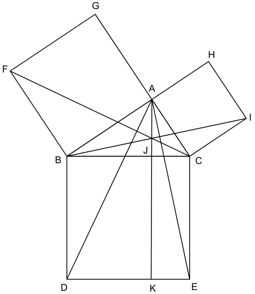
BUT

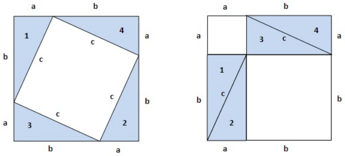
Definition

Proof theory is the branch of mathematical logic that studies proofs as formal mathematical objects.

BUT

“No entity without identity”



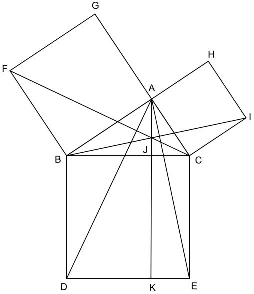


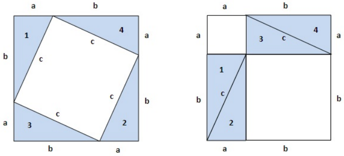
Definition

Proof theory is the branch of mathematical logic that studies proofs as formal mathematical objects.

BUT

“No entity without identity”





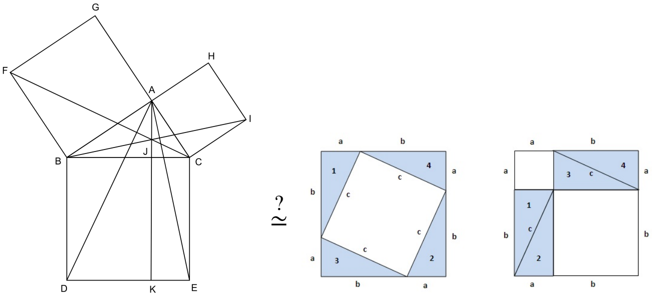
PROBLEM: no agreement on the meaning of “the same”

Definition

Proof theory is the branch of mathematical logic that studies proofs as formal mathematical objects.

BUT

“No entity without identity”



PROBLEM: no agreement on the meaning of “the same”

The 24th Hilbert problem[1]:

Criteria of simplicity, or proof of the greatest simplicity of certain proofs. [. . .]

[1] Found on notes discovered by Thiele in 2000

The 24th Hilbert problem[1]:

Criteria of simplicity, or proof of the greatest simplicity of certain proofs. [. . .] Under a given set of conditions there can be but one simplest proof. [. . .]

[1] Found on notes discovered by Thiele in 2000

The 24th Hilbert problem[1]:

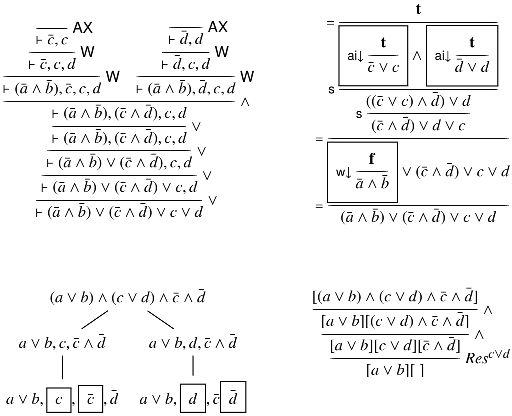
Criteria of simplicity, or proof of the greatest simplicity of certain proofs. [. . .] Under a given set of conditions there can be but one simplest proof. [. . .] Quite generally, if there are two proofs for a theorem, you must keep going until you have derived each from the other, or until it becomes quite evident what variant conditions (and aids) have been used in the two proofs. [. . .]

[1] Found on notes discovered by Thiele in 2000

Why (also) computer scientists should care about it?

“[God] caused a tumult among them, by producing in them diverse languages, and causing that, through the multitude of those languages, they should not be able to understand one another.”
(Flavius Josephus, Antiquities of the Jews, c. 94 CE)

“[God] caused a tumult among them, by producing in them diverse languages, and causing that, through the multitude of those languages, they should not be able to understand one another.”
(Flavius Josephus, Antiquities of the Jews, c. 94 CE)



“[God] caused a tumult among them, by producing in them diverse languages, and causing that, through the multitude of those languages, they should not be able to understand one another.”
(Flavius Josephus, Antiquities of the Jews, c. 94 CE)

Coq $\leftrightsquigarrow$ Lean

Proof equivalence as blueprint for program equivalence:

VILLUM FONDEN

"X-IDF: Explainable Internet Data Flows"

Logic Programming:

- a proof system (set of rules) is a program
- a proof is a possible execution of the program

Proof equivalence can be read as execution equivalences (via bisimulations)

Two Approaches to Proof Equivalence

- **Normalization**: $\pi_1 = \pi_2 \iff \exists \hat{\pi}$ s.t. $\pi_1 \rightsquigarrow \hat{\pi}$ and $\pi_2 \rightsquigarrow \hat{\pi}$
  - Normalization may forget information (see classical logic)
  - Close to denotational semantics/categorical semantics/game semantics approaches
- **Generality**: $\pi_1 = \pi_2 \iff [\![\pi_1]\!] = [\![\pi_2]\!]$
  - two proofs are equivalent if we can associate both a same mathematical object
  - No normalization is involved: two programs computing a same function can still be different

Equivalence via rule permutations (Sequent Calculi)

$$\dfrac{\Gamma_1, \Delta_1 \qquad \dfrac{\Gamma_2, \Delta_2, \Delta_3 \qquad \Gamma_3, \Delta_4}{\Gamma_2, \Gamma_3, \Delta_2, \Sigma_2}\,\rho_2}{\Gamma_1, \Gamma_2, \Gamma_3, \Sigma_1, \Sigma_2}\,\rho_1 \quad \equiv \quad \dfrac{\dfrac{\Gamma_1, \Delta_1 \qquad \Gamma_1, \Delta_2, \Delta_3}{\Gamma_1, \Gamma_2, \Sigma_1, \Delta_3,}\,\rho_1 \qquad \Gamma_3, \Delta_4}{\Gamma_1, \Gamma_2, \Gamma_3, \Sigma_1, \Sigma_2}\,\rho_2$$

$$\dfrac{\dfrac{\Gamma, \Delta_1, \Delta_2}{\Gamma, \Sigma_1, \Delta_2}\,\rho_1}{\Gamma, \Sigma_1, \Sigma_2}\,\rho_2 \quad \equiv \quad \dfrac{\dfrac{\Gamma, \Delta_1, \Delta_2}{\Gamma, \Delta_1, \Sigma_2}\,\rho_2}{\Gamma, \Sigma_1, \Sigma_2}\,\rho_1$$

$$\dfrac{\dfrac{\Gamma, \Delta_1, \Delta_2 \qquad \Gamma_2, \Delta_3}{\Gamma_1, \Gamma_2, \Delta_1, \Sigma_2}\,\rho_2}{\Gamma_1, \Gamma_2, \Sigma_1, \Sigma_2}\,\rho_1 \quad \equiv \quad \dfrac{\dfrac{\Gamma, \Delta_1, \Delta_2}{\Gamma, \Sigma_1, \Delta_2}\,\rho_1 \qquad \Gamma_2, \Delta_3}{\Gamma_1, \Gamma_2, \Sigma_1, \Sigma_2}\,\rho_2$$

We consider some derivations to be the same proof:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{a,\bar{a}}\,\mathsf{AX}\qquad \dfrac{}{\bar{b},b}\,\mathsf{AX}}{a,\bar{a}\otimes\bar{b},b}\,\otimes}{a \parr (\bar{a}\otimes\bar{b}),b}\,\parr \qquad \dfrac{\dfrac{}{c,\bar{c}}\,\mathsf{AX}\qquad \dfrac{}{\bar{d},d}\,\mathsf{AX}}{c,\bar{c}\otimes\bar{d},d}\,\otimes}{a \parr (\bar{a}\otimes\bar{b}),b\otimes c,d,\bar{c}\otimes\bar{d}}\,\otimes}{a \parr (\bar{a}\otimes\bar{b}),(b\otimes c)\parr d,\bar{c}\otimes\bar{d}}\,\parr$$

We consider some derivations to be the same proof:

$$
\dfrac{
  \dfrac{
    \dfrac{
      \dfrac{
        \dfrac{}{a, \bar{a}}\,\mathsf{AX}
        \qquad
        \dfrac{}{\bar{b}, b}\,\mathsf{AX}
      }{a, \bar{a} \otimes \bar{b}, b}\,\otimes
      \qquad
      \dfrac{
        \dfrac{}{c, \bar{c}}\,\mathsf{AX}
        \qquad
        \dfrac{}{\bar{d}, d}\,\mathsf{AX}
      }{c, \bar{c} \otimes \bar{d}, d}\,\otimes
    }{a, (\bar{a} \otimes \bar{b}), b \otimes c, d, \bar{c} \otimes \bar{d}}\,\otimes
  }{a \parr (\bar{a} \otimes \bar{b}), b \otimes c, d, \bar{c} \otimes \bar{d}}\,\parr
}{a \parr (\bar{a} \otimes \bar{b}), (b \otimes c) \parr d, \bar{c} \otimes \bar{d}}\,\parr
$$

We consider some derivations to be the same proof:

$$
\dfrac{\dfrac{\dfrac{\dfrac{}{a, \bar{a}}\,\mathsf{AX} \qquad \dfrac{\dfrac{\dfrac{}{\bar{b}, b}\,\mathsf{AX} \quad \dfrac{}{c, \bar{c}}\,\mathsf{AX}}{\bar{b}, b \otimes c, \bar{c}}\,\otimes \qquad \dfrac{}{\bar{d}, d}\,\mathsf{AX}}{\bar{b}, b \otimes c, \bar{c} \otimes \bar{d}, d}\,\otimes}{a, \bar{a} \otimes \bar{b}, b \otimes c, d, \bar{c} \otimes \bar{d}}\,\otimes}{a \parr (\bar{a} \otimes \bar{b}), b \otimes c, d, \bar{c} \otimes \bar{d}}\,\parr}{a \parr (\bar{a} \otimes \bar{b}), (b \otimes c) \parr d, \bar{c} \otimes \bar{d}}\,\parr
$$

We consider some derivations to be the same proof:

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{AX}
\UnaryInfC{$a, \bar{a}$}
\AxiomC{}
\RightLabel{AX}
\UnaryInfC{$\bar{b}, b$}
\AxiomC{}
\RightLabel{AX}
\UnaryInfC{$c, \bar{c}$}
\RightLabel{$\otimes$}
\BinaryInfC{$\bar{b}, b \otimes c, \bar{c}$}
\AxiomC{}
\RightLabel{AX}
\UnaryInfC{$\bar{d}, d$}
\RightLabel{$\otimes$}
\BinaryInfC{$\bar{b}, b \otimes c, \bar{c} \otimes \bar{d}, d$}
\RightLabel{$\parr$}
\UnaryInfC{$\bar{b}, (b \otimes c) \parr d, \bar{c} \otimes \bar{d}$}
\RightLabel{$\otimes$}
\BinaryInfC{$a, \bar{a} \otimes \bar{b}, (b \otimes c) \parr d, \bar{c} \otimes \bar{d}$}
\RightLabel{$\parr$}
\UnaryInfC{$a \parr (\bar{a} \otimes \bar{b}), (b \otimes c) \parr d, \bar{c} \otimes \bar{d}$}
\end{prooftree}
$$

We consider some derivations to be the same proof:

$$
\dfrac{
  \dfrac{
    \dfrac{
      \dfrac{}{a, \bar{a}}\,\mathsf{AX}
      \quad
      \dfrac{}{\bar{b}, b}\,\mathsf{AX}
    }{a, \bar{a} \otimes \bar{b}, b}\,\otimes
  }{a \parr (\bar{a} \otimes \bar{b}), b}\,\parr
  \qquad
  \dfrac{
    \dfrac{}{c, \bar{c}}\,\mathsf{AX}
    \quad
    \dfrac{}{\bar{d}, d}\,\mathsf{AX}
  }{c, \bar{c} \otimes \bar{d}, d}\,\otimes
}{
  \dfrac{a \parr (\bar{a} \otimes \bar{b}), b \otimes c, d, \bar{c} \otimes \bar{d}}{a \parr (\bar{a} \otimes \bar{b}), (b \otimes c) \parr d, \bar{c} \otimes \bar{d}}\,\parr
}\,\otimes
\quad \simeq \quad
\dfrac{
  \dfrac{
    \dfrac{}{a, \bar{a}}\,\mathsf{AX}
    \qquad
    \dfrac{
      \dfrac{
        \dfrac{
          \dfrac{}{\bar{b}, b}\,\mathsf{AX}
          \quad
          \dfrac{}{c, \bar{c}}\,\mathsf{AX}
        }{\bar{b}, b \otimes c, \bar{c}}\,\otimes
        \quad
        \dfrac{}{\bar{d}, d}\,\mathsf{AX}
      }{\bar{b}, b \otimes c, \bar{c} \otimes \bar{d}, d}\,\otimes
    }{\bar{b}, (b \otimes c) \parr d, \bar{c} \otimes \bar{d}}\,\parr
  }{a, \bar{a} \otimes \bar{b}, (b \otimes c) \parr d, \bar{c} \otimes \bar{d}}\,\otimes
}{a \parr (\bar{a} \otimes \bar{b}), (b \otimes c) \parr d, \bar{c} \otimes \bar{d}}\,\parr
$$

Sequences are... sequential (no space for parallelism)

$$
\dfrac{\dfrac{\dfrac{\dfrac{}{a, \bar{a}}\,\mathsf{AX} \quad \dfrac{}{b, \bar{b}}\,\mathsf{AX}}{a, \bar{a} \otimes \bar{b}, b}\,\otimes}{a \parr (\bar{a} \otimes \bar{b}), b}\,\parr \qquad \dfrac{\dfrac{}{c, \bar{c}}\,\mathsf{AX} \quad \dfrac{}{d, \bar{d}}\,\mathsf{AX}}{c, \bar{c} \otimes \bar{d}, d}\,\otimes}{\dfrac{a \parr (\bar{a} \otimes \bar{b}), b \otimes c, d, \bar{c} \otimes \bar{d}}{a \parr (\bar{a} \otimes \bar{b}), (b \otimes c) \parr d, \bar{c} \otimes \bar{d}}\,\parr}\,\otimes
$$

$$\simeq$$

$$
\dfrac{\dfrac{\dfrac{}{a, \bar{a}}\,\mathsf{AX} \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{b, \bar{b}}\,\mathsf{AX} \quad \dfrac{}{c, \bar{c}}\,\mathsf{AX}}{\bar{b}, b \otimes c, \bar{c}}\,\otimes \quad \dfrac{}{d, \bar{d}}\,\mathsf{AX}}{\bar{b}, b \otimes c, d, \bar{c} \otimes \bar{d}}\,\otimes}{(b \otimes c) \parr d, \bar{c} \otimes \bar{d}}\,\parr}{a, (\bar{a} \otimes \bar{b}), (b \otimes c) \parr d, \bar{c} \otimes \bar{d}}\,\otimes}{a \parr (\bar{a} \otimes \bar{b}), (b \otimes c) \parr d, \bar{c} \otimes \bar{d}}\,\parr
$$

From Rule Permutations to Generality

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$a, \bar{a}$}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$\bar{b}, b$}
\RightLabel{$\otimes$}
\BinaryInfC{$a, \bar{a} \otimes \bar{b}, b$}
\RightLabel{$\parr$}
\UnaryInfC{$a \parr (\bar{a} \otimes \bar{b}), b$}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$c, \bar{c}$}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$\bar{d}, d$}
\RightLabel{$\otimes$}
\BinaryInfC{$c, \bar{c} \otimes \bar{d}, d$}
\RightLabel{$\otimes$}
\BinaryInfC{$a \parr (\bar{a} \otimes \bar{b}), b \otimes c, d, \bar{c} \otimes \bar{d}$}
\RightLabel{$\parr$}
\UnaryInfC{$a \parr (\bar{a} \otimes \bar{b}), (b \otimes c) \parr d, \bar{c} \otimes \bar{d}$}
\end{prooftree}
$$

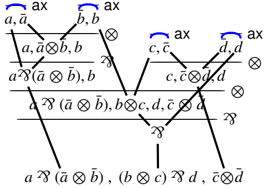
$$\simeq$$

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$a, \bar{a}$}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$\bar{b}, b$}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$c, \bar{c}$}
\RightLabel{$\otimes$}
\BinaryInfC{$\bar{b}, b \otimes c, \bar{c}$}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$\bar{d}, d$}
\RightLabel{$\otimes$}
\BinaryInfC{$\bar{b}, b \otimes c, \bar{c} \otimes \bar{d}, d$}
\RightLabel{$\parr$}
\UnaryInfC{$(b \otimes c) \parr d, \bar{c} \otimes \bar{d}$}
\RightLabel{$\otimes$}
\BinaryInfC{$a, \bar{a} \otimes \bar{b}, (b \otimes c) \parr d, \bar{c} \otimes \bar{d}$}
\RightLabel{$\parr$}
\UnaryInfC{$a \parr (\bar{a} \otimes \bar{b}), (b \otimes c) \parr d, \bar{c} \otimes \bar{d}$}
\end{prooftree}
$$

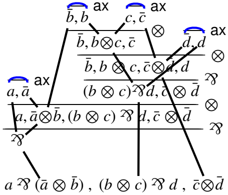
$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{a,\bar a}\,\text{ax}\qquad \dfrac{}{\bar b, b}\,\text{ax}}{a,\bar a\otimes\bar b, b}\,\otimes}{a\parr(\bar a\otimes\bar b), b}\,\parr \qquad \dfrac{\dfrac{}{c,\bar c}\,\text{ax}\qquad\dfrac{}{\bar d,d}\,\text{ax}}{c,\bar c\otimes\bar d, d}\,\otimes}{a\parr(\bar a\otimes\bar b), b\otimes c, d, \bar c\otimes\bar d}\,\otimes}{a\parr(\bar a\otimes\bar b), (b\otimes c)\parr d, \bar c\otimes\bar d}\,\parr$$

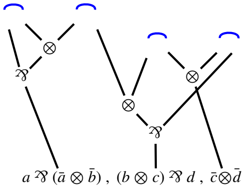
$$\simeq$$

$$\dfrac{\dfrac{\dfrac{}{a,\bar a}\,\text{ax}\qquad \dfrac{\dfrac{\dfrac{\dfrac{}{\bar b, b}\,\text{ax}\qquad\dfrac{}{c,\bar c}\,\text{ax}}{\bar b, b\otimes c, \bar c}\,\otimes\qquad\dfrac{}{\bar d, d}\,\text{ax}}{\bar b, b\otimes c, \bar c\otimes\bar d, d}\,\otimes}{(b\otimes c)\parr d, \bar c\otimes\bar d}\,\parr}{a,\bar a\otimes\bar b,(b\otimes c)\parr d,\bar c\otimes\bar d}\,\otimes}{a\parr(\bar a\otimes\bar b),(b\otimes c)\parr d,\bar c\otimes\bar d}\,\parr$$

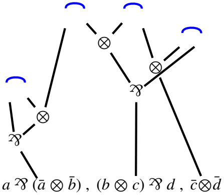

ax
$a, \bar{a}$
$\bar{b}, b$
$c, \bar{c}$
$\bar{d}, d$
$a, \bar{a} \otimes \bar{b}, b$
$a ⅋ (\bar{a} \otimes \bar{b}), b$
$c, \bar{c} \otimes \bar{d}, d$
$a ⅋ (\bar{a} \otimes \bar{b}), b \otimes c, d, \bar{c} \otimes \bar{d}$
$a ⅋ (\bar{a} \otimes \bar{b})\,,\ (b \otimes c) ⅋ d\,,\ \bar{c} \otimes \bar{d}$

$\simeq$


ax
$\bar{b}, b$
$c, \bar{c}$
$\bar{d}, d$
$a, \bar{a}$
$\bar{b}, b \otimes c, \bar{c}$
$\bar{b}, b \otimes c, \bar{c} \otimes \bar{d}, d$
$(b \otimes c) ⅋ d, \bar{c} \otimes \bar{d}$
$a, \bar{a} \otimes \bar{b}, (b \otimes c) ⅋ d, \bar{c} \otimes \bar{d}$
$a ⅋ (\bar{a} \otimes \bar{b})\,,\ (b \otimes c) ⅋ d\,,\ \bar{c} \otimes \bar{d}$



$\simeq$



This is an MLL-proof net [Gir87]

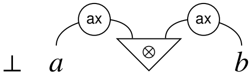
Bad news and Good news

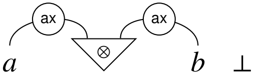
Problem: no proof nets* for extensions of MLL [Hei&Hou14]

$$
\dfrac{\dfrac{\dfrac{}{a, \bar{a}}\,\mathsf{ax}}{a, \bar{a}, \bot}\,\bot \qquad \dfrac{}{b, \bar{b}}\,\mathsf{ax}}{a, \bar{a} \otimes \bar{b}, b, \bot}\,\otimes
\quad \equiv \quad
\dfrac{\dfrac{\dfrac{}{a, \bar{a}}\,\mathsf{ax} \qquad \dfrac{}{a, \bar{a}}\,\mathsf{ax}}{a, \bar{a} \otimes \bar{b}, a}\,\otimes}{a, \bar{a} \otimes \bar{b}, b, \bot}\,\bot
\quad \equiv \quad
\dfrac{\dfrac{}{a, \bar{a}}\,\mathsf{ax} \qquad \dfrac{\dfrac{}{b, \bar{b}}\,\mathsf{ax}}{b, \bar{b}, \bot}\,\bot}{a, \bar{a} \otimes \bar{b}, b, \bot}\,\otimes
$$

Problem: no proof nets* for extensions of MLL [Hei&Hou14]

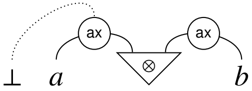
$$\dfrac{\dfrac{\dfrac{}{a,\bar{a}}\,\text{ax}}{a,\bar{a},\bot}\,\bot \qquad \dfrac{}{b,\bar{b}}\,\text{ax}}{a,\bar{a}\otimes\bar{b},b,\bot}\,\otimes \quad\equiv\quad \dfrac{\dfrac{\dfrac{}{a,\bar{a}}\,\text{ax} \qquad \dfrac{}{a,\bar{a}}\,\text{ax}}{a,\bar{a}\otimes\bar{b},a}\,\otimes}{a,\bar{a}\otimes\bar{b},b,\bot}\,\bot \quad\equiv\quad \dfrac{\dfrac{}{a,\bar{a}}\,\text{ax} \qquad \dfrac{\dfrac{}{b,\bar{b}}\,\text{ax}}{b,\bar{b},\bot}\,\bot}{a,\bar{a}\otimes\bar{b},b,\bot}\,\otimes$$

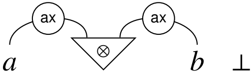




Problem: no proof nets* for extensions of MLL [Hei&Hou14]

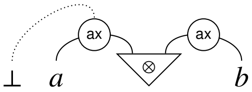
$$\dfrac{\dfrac{\dfrac{}{a,\bar{a}}\,\text{ax}}{a,\bar{a},\bot}\,\bot \qquad \dfrac{}{b,\bar{b}}\,\text{ax}}{a,\bar{a}\otimes\bar{b},b,\bot}\,\otimes \quad \equiv \quad \dfrac{\dfrac{\dfrac{}{a,\bar{a}}\,\text{ax} \qquad \dfrac{}{a,\bar{a}}\,\text{ax}}{a,\bar{a}\otimes\bar{b},a}\,\otimes}{a,\bar{a}\otimes\bar{b},b,\bot}\,\bot \quad \equiv \quad \dfrac{\dfrac{}{a,\bar{a}}\,\text{ax} \qquad \dfrac{\dfrac{}{b,\bar{b}}\,\text{ax}}{b,\bar{b},\bot}\,\bot}{a,\bar{a}\otimes\bar{b},b,\bot}\,\otimes$$

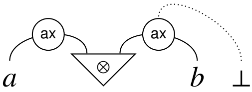




Problem: no proof nets* for extensions of MLL [Hei&Hou14]

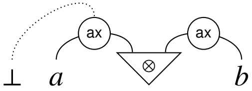
$$\dfrac{\dfrac{\dfrac{}{a,\bar{a}}\,\mathsf{ax}}{a,\bar{a},\bot}\,\bot \qquad \dfrac{}{b,\bar{b}}\,\mathsf{ax}}{a,\bar{a}\otimes\bar{b},b,\bot}\,\otimes \quad\equiv\quad \dfrac{\dfrac{\dfrac{}{a,\bar{a}}\,\mathsf{ax} \qquad \dfrac{}{a,\bar{a}}\,\mathsf{ax}}{a,\bar{a}\otimes\bar{b},a}\,\otimes}{a,\bar{a}\otimes\bar{b},b,\bot}\,\bot \quad\equiv\quad \dfrac{\dfrac{}{a,\bar{a}}\,\mathsf{ax} \qquad \dfrac{\dfrac{}{b,\bar{b}}\,\mathsf{ax}}{b,\bar{b},\bot}\,\bot}{a,\bar{a}\otimes\bar{b},b,\bot}\,\otimes$$

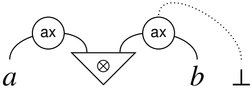




Problem: no proof nets* for extensions of MLL [Hei&Hou14]

$$\dfrac{\dfrac{\dfrac{}{a,\bar{a}}\,\text{ax}}{a,\bar{a},\bot}\,\bot \qquad \dfrac{}{b,\bar{b}}\,\text{ax}}{a,\bar{a}\otimes\bar{b},b,\bot}\,\otimes \quad \equiv \quad \dfrac{\dfrac{\dfrac{}{a,\bar{a}}\,\text{ax} \qquad \dfrac{}{a,\bar{a}}\,\text{ax}}{a,\bar{a}\otimes\bar{b},a}\,\otimes}{a,\bar{a}\otimes\bar{b},b,\bot}\,\bot \quad \equiv \quad \dfrac{\dfrac{}{a,\bar{a}}\,\text{ax} \qquad \dfrac{\dfrac{}{b,\bar{b}}\,\text{ax}}{b,\bar{b},\bot}\,\bot}{a,\bar{a}\otimes\bar{b},b,\bot}\,\otimes$$

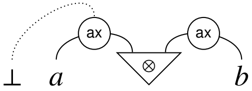


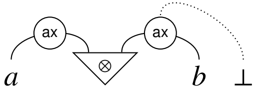


* proof equivalence is P-space

Problem: no proof nets* for extensions of MLL [Hei&Hou14]

$$\dfrac{\dfrac{\dfrac{}{a,\bar{a}}\,\mathsf{ax}}{a,\bar{a},\bot}\,\bot \qquad \dfrac{}{b,\bar{b}}\,\mathsf{ax}}{a,\bar{a}\otimes\bar{b},b,\bot}\,\otimes \quad\equiv\quad \dfrac{\dfrac{\dfrac{}{a,\bar{a}}\,\mathsf{ax} \qquad \dfrac{}{a,\bar{a}}\,\mathsf{ax}}{a,\bar{a}\otimes\bar{b},a}\,\otimes}{a,\bar{a}\otimes\bar{b},b,\bot}\,\bot \quad\equiv\quad \dfrac{\dfrac{}{a,\bar{a}}\,\mathsf{ax} \qquad \dfrac{\dfrac{}{b,\bar{b}}\,\mathsf{ax}}{b,\bar{b},\bot}\,\bot}{a,\bar{a}\otimes\bar{b},b,\bot}\,\otimes$$

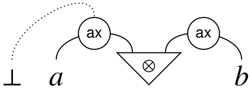


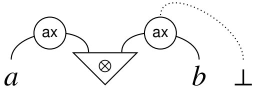


* proof equivalence is P-space BUT translation and check are P-time

Problem: no proof nets* for extensions of MLL [Hei&Hou14]

$$\dfrac{\dfrac{\dfrac{}{a,\bar{a}}\,\text{ax}}{a,\bar{a},\bot}\,\bot \qquad \dfrac{}{b,\bar{b}}\,\text{ax}}{a,\bar{a}\otimes\bar{b},b,\bot}\,\otimes \quad\equiv\quad \dfrac{\dfrac{\dfrac{}{a,\bar{a}}\,\text{ax} \qquad \dfrac{}{a,\bar{a}}\,\text{ax}}{a,\bar{a}\otimes\bar{b},a}\,\otimes}{a,\bar{a}\otimes\bar{b},b,\bot}\,\bot \quad\equiv\quad \dfrac{\dfrac{}{a,\bar{a}}\,\text{ax} \qquad \dfrac{\dfrac{}{b,\bar{b}}\,\text{ax}}{b,\bar{b},\bot}\,\bot}{a,\bar{a}\otimes\bar{b},b,\bot}\,\otimes$$

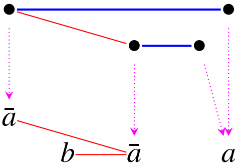




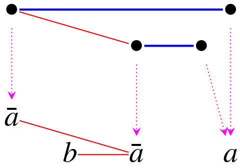
* proof equivalence is P-space BUT translation and check are P-time

This is not a limit of THIS syntax, but it depends on the logic!

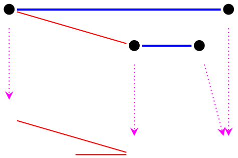
Combinatorial Proofs for various logics



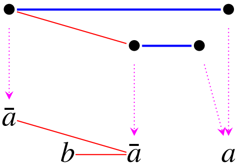
Combinatorial Proofs for various logics



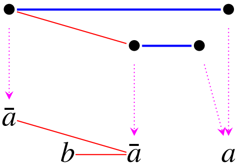
Combinatorial Proofs for various logics



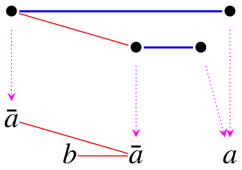
Combinatorial Proofs for various logics

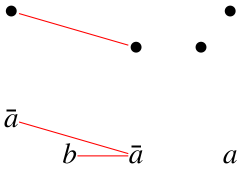


Combinatorial Proofs for various logics

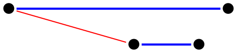


Combinatorial Proofs and Proof Equivalence

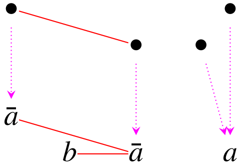

$\bar{a}$
b
$\bar{a}$
a



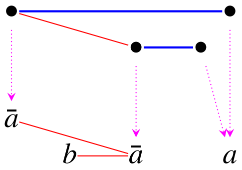
cographs = formulas



RB-cographs = linear proofs



skew fibration = resource management

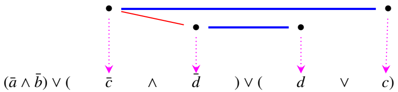


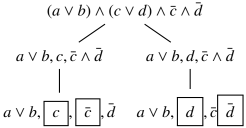
- Rule-free representation of proofs
- Canonical representation for (cut-free) proofs
- Topological characterization of “graphs representing proofs”
- Proof System (Cook-Reckhow)
- Polynomial translations

Combinatorial Proofs for Classical Logic [Hughes 2006]

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash \bar{c}, c}\,\mathsf{ax}}{\vdash \bar{c}, c, d}\,\mathsf{W}}{\vdash (\bar{a}\wedge\bar{b}), \bar{c}, c, d}\,\mathsf{W} \qquad \dfrac{\dfrac{\dfrac{}{\vdash \bar{d}, d}\,\mathsf{ax}}{\vdash \bar{d}, c, d}\,\mathsf{W}}{\vdash (\bar{a}\wedge\bar{b}), \bar{d}, c, d}\,\mathsf{W}}{\vdash (\bar{a}\wedge\bar{b}), (\bar{c}\wedge\bar{d}), c, d}\,\wedge}{\vdash (\bar{a}\wedge\bar{b}), (\bar{c}\wedge\bar{d}), c, d}\,\vee}{\vdash (\bar{a}\wedge\bar{b})\vee(\bar{c}\wedge\bar{d}), c, d}\,\vee}{\vdash (\bar{a}\wedge\bar{b})\vee(\bar{c}\wedge\bar{d})\vee c, d}\,\vee}{\vdash (\bar{a}\wedge\bar{b})\vee(\bar{c}\wedge\bar{d})\vee c\vee d}\,\vee
$$

$$
\begin{array}{l}
= \dfrac{\mathbf{t}}{\boxed{\mathsf{ai}\!\downarrow \dfrac{\mathbf{t}}{\bar{c}\vee c}} \wedge \boxed{\mathsf{ai}\!\downarrow \dfrac{\mathbf{t}}{\bar{d}\vee d}}} \\
\mathsf{s}\ \overline{\quad \mathsf{s}\ \dfrac{((\bar{c}\vee c)\wedge\bar{d})\vee d}{(\bar{c}\wedge\bar{d})\vee d\vee c} \quad} \\
= \overline{\boxed{\mathsf{w}\!\downarrow \dfrac{\mathbf{f}}{\bar{a}\wedge\bar{b}}} \vee (\bar{c}\wedge\bar{d})\vee c\vee d} \\
= \overline{(\bar{a}\wedge\bar{b})\vee(\bar{c}\wedge\bar{d})\vee c\vee d}
\end{array}
$$





$$
\dfrac{\dfrac{\dfrac{[(a\vee b)\wedge(c\vee d)\wedge\bar{c}\wedge\bar{d}]}{[a\vee b][(c\vee d)\wedge\bar{c}\wedge\bar{d}]}\,\wedge}{[a\vee b][c\vee d][\bar{c}\wedge\bar{d}]}\,\wedge}{[a\vee b][\,]}\,Res^{c\vee d}
$$

- sequent calculus [Hughes 2006]
- deep inference [Straßburger 2017]
- tableaux and resolution [Acclavio & Straßburger 2018]

Following the generality principle:

Two proofs are the same
iff
they can be represented by the same combinatorial proof

Following the generality principle:

Two proofs are the same
iff
they can be represented by the same combinatorial proof

What can we handle in this way?

- Relevant Logic = LK without weakening
- Affine Logic = LK without contraction

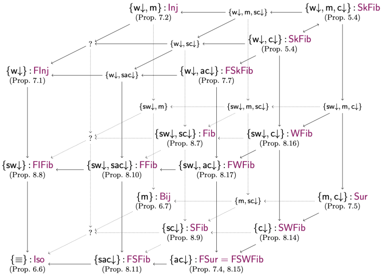


*figure from Ralph and Straßburger paper

[2] Ralph & Straßburger Tablueaux2019; Acclavio & Straßburger Wollic2019

Relevant and Affine Logics[2]

- Relevant Logic = LK without weakening
- Affine Logic = LK without contraction

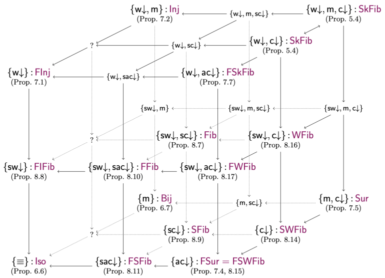


*figure from Ralph and Straßburger paper

- Entailment Logic ≃ Relevant + non associative connectives

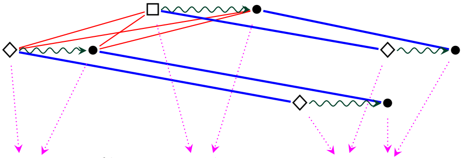
[2] Ralph & Straßburger Tablueaux2019; Acclavio & Straßburger Wollic2019

Modal Formulas

$$A, B := a \mid \bar{a} \mid A \wedge B \mid A \vee B \mid \Box A \mid \Diamond A$$

Sequent Calculus Rules

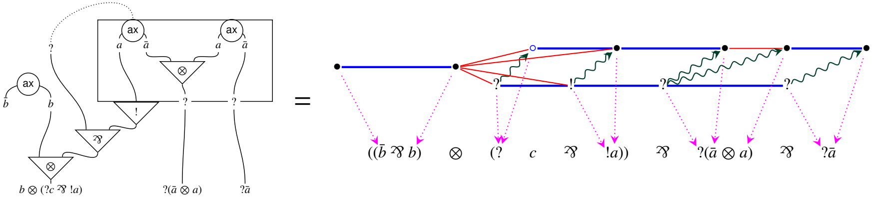
$$\mathsf{LK} \cup \left\{ \mathsf{K}\,\frac{A, \Gamma}{\Box A, \Diamond\Gamma} \quad , \quad \mathsf{D}\,\frac{A, \Gamma}{\Diamond A, \Diamond\Gamma} \quad , \quad \mathsf{T}_{\downarrow}\,\frac{C\,[A]}{C\,[\Diamond A]} \quad , \quad 4_{\downarrow}\,\frac{C\,[\Diamond\Diamond A]}{C\,[\Diamond A]} \right\}$$



$$((\Diamond\Diamond\bar{a} \quad \vee \Box b) \quad \wedge \quad \Box\bar{a}) \quad \vee \quad \Diamond \quad a$$

[3] Acclavio & Straßburger Tabuleaux2019

Multiplicative Linear Logic with Exponentials[4]

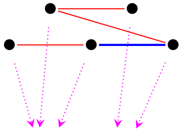


[4] Acclavio TLLA2020

Formulas

$$\begin{aligned} t &:= c \mid f(t_1, \ldots, t_n) \\ a &:= p(t_1, \ldots, t_n) \mid \bar{p}(t_1, \ldots, t_n) \\ A, B &:= a \mid A \wedge B \mid A \vee B \mid \forall x A \mid \exists x A \end{aligned}$$

Rules LK $\cup \left\{ \exists \dfrac{\Gamma, A[x/t]}{\Gamma, \exists x.A} \quad , \quad \forall \dfrac{\Gamma, A}{\Gamma, \forall x.A} \; x \text{ not free in } \Gamma \right\}$



$\exists x \bar{p}(x) \forall y p(y)$

[5] Hughes 2019; Hughes & Straßburger & Wu LICS2021

Intuitionistic Logic[6]

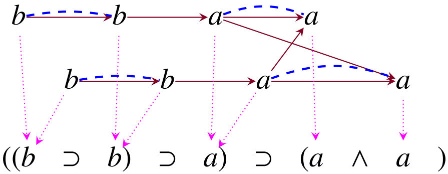
Formulas

$$A, B := a \mid A \wedge B \mid A \supset B$$

Sequent Calculus Rules

$$\frac{}{a \vdash a}\,\mathsf{ax} \qquad \frac{\Gamma, B \vdash A}{\Gamma \vdash B \supset A}\,\supset^{\mathsf{R}} \qquad \frac{\Gamma, B, C \vdash A}{\Gamma, B \wedge C \vdash A}\,\wedge^{\mathsf{L}} \qquad \frac{\Gamma \vdash A \quad \Delta \vdash B}{\Gamma, \Delta \vdash A \wedge B}\,\wedge^{\mathsf{R}} \qquad \frac{\Gamma \vdash A \quad \Delta, B \vdash C}{\Gamma, \Delta, A \supset B \vdash C}\,\supset^{\mathsf{L}}$$

$$\frac{}{\vdash 1}\,\mathsf{1} \qquad \frac{\Gamma, B, B \vdash A}{\Gamma, B \vdash A}\,\mathsf{C} \qquad \frac{\Gamma \vdash A}{\Gamma, B \vdash A}\,\mathsf{W}$$



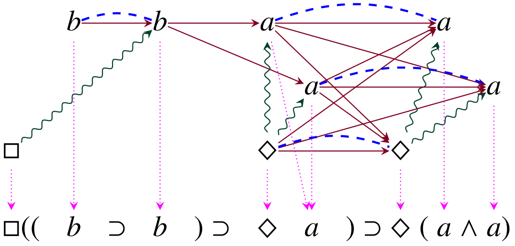
6 Heijltjes, Hughes & Straßburger LICS2019

Modal Formulas

$$A, B \coloneqq a \mid A \wedge B \mid A \supset B \mid \Box A \mid \Diamond A \mid 1$$

Additional Sequent Calculus Rules

$$\frac{\Gamma \vdash A}{\Box\Gamma \vdash \Box A}\,\mathsf{K}_\Box \qquad \frac{B, \Gamma \vdash A}{\Diamond B, \Box\Gamma \vdash \Diamond A}\,\mathsf{K}_\Diamond \qquad \frac{B, \Gamma \vdash A}{\Box\Gamma \vdash \Diamond A}\,\mathsf{D}$$



[7] Acclavio & Straßburger 2022

Comparing Proof Equivalences
(Case Study: Constructive Modal Logic)

Independent rules	$\equiv$		
Resource Management	$\dfrac{\dfrac{\Gamma,A,A,B,B\vdash C}{\Gamma,A,B\vdash C}\,2\times C}{\Gamma,A\wedge B\vdash C}\,\wedge^L \equiv_{c} \dfrac{\dfrac{\Gamma,A,A,B,B\vdash C}{\Gamma,A\wedge B,A\wedge B\vdash C}\,2\times\wedge^L}{\Gamma,A\wedge B\vdash C}\,C$	$\dfrac{\dfrac{\Gamma\vdash C}{\Gamma,A,B\vdash C}\,2\times W}{\Gamma,A\wedge B\vdash C}\,\wedge^L \equiv_{c} \dfrac{\Gamma\vdash C}{\Gamma,A\wedge B\vdash C}\,W$	
	$\dfrac{\dfrac{\Gamma,A,A\vdash B}{\Gamma,A\vdash B}\,C}{\Gamma,A,A\vdash B}\,W \equiv_{c} \Gamma,A,A\vdash B$	$\dfrac{\dfrac{\Gamma,A\vdash B}{\Gamma,A,A\vdash B}\,W}{\Gamma,A\vdash B}\,C \equiv_{c} \Gamma,A\vdash B$	
Excising and Unfolding	$\dfrac{\Gamma\vdash A \quad \dfrac{\Delta\vdash C}{B,\Delta\vdash C}\,W}{\Gamma,\Delta,A\supset B\vdash C}\,\supset^L \equiv_{e} \dfrac{\Delta\vdash C}{\Gamma,\Delta,A\supset B\vdash C}\,W$	$\dfrac{\Gamma\vdash A \quad \dfrac{\Delta,B,B\vdash C}{\Delta,B\vdash C}\,C}{\Gamma,A\supset B\vdash C}\,\supset^L \equiv_{u} \dfrac{\dfrac{\Gamma\vdash A \quad \dfrac{\Gamma\vdash A \quad \Delta,B,B\vdash C}{\Gamma,\Delta,A\supset B,B\vdash C}\,\supset^L}{\Gamma,\Gamma,\Delta,A\supset B,A\supset B\vdash C}\,\supset^L}{\Gamma,\Delta,A\supset B\vdash C}\,C$	
Structural vs K	$\dfrac{\dfrac{\Gamma\vdash A}{\Gamma,B\vdash A}\,W}{\Box\Gamma,\Box B\vdash\Box A}\,K_\Box \equiv_{\Box c} \dfrac{\dfrac{\Gamma\vdash A}{\Box\Gamma\vdash\Box A}\,K_\Box}{\Box\Gamma,\Box B\vdash\Box A}\,W$	$\dfrac{\dfrac{\Gamma,B,B\vdash A}{\Gamma,B\vdash A}\,C}{\Box\Gamma,\Box B\vdash\Box A}\,K_\Box \equiv_{\Box c} \dfrac{\dfrac{\Gamma,B,B\vdash A}{\Box\Gamma,\Box B,\Box B\vdash\Box A}\,K_\Box}{\Box\Gamma,\Box B\vdash\Box A}\,C$	
	$\dfrac{\dfrac{\Gamma,B\vdash A}{\Gamma,B,C\vdash A}\,W}{\Box\Gamma,\Diamond B,\Box C,\vdash\Box A}\,K_\Diamond \equiv_{\Box c} \dfrac{\dfrac{\Gamma,B\vdash A}{\Box\Gamma,\Diamond B\vdash\Diamond A}\,K_\Diamond}{\Box\Gamma,\Diamond B,\Box C\vdash\Box A}\,W$	$\dfrac{\dfrac{\Gamma,B,C,C\vdash A}{\Gamma,B,C\vdash A}\,C}{\Box\Gamma,\Diamond B,\Box C\vdash\Diamond A}\,K_\Box \equiv_{\Box c} \dfrac{\dfrac{\Gamma,B,C,C\vdash A}{\Box\Gamma,\Diamond B,\Box C,\Box C\Box\vdash\Diamond A}\,K_\Box}{\Box\Gamma,\Diamond B,\Box C\vdash\Diamond A}\,C$	
	$\dfrac{\dfrac{\dfrac{\Gamma\vdash A}{\Gamma,B\vdash A}\,W}{\Box\Gamma,\Diamond B\vdash\Diamond A}\,K_\Diamond}{\Box\Gamma,\Diamond B,\Diamond C\vdash\Diamond A}\,W \equiv_{\Diamond w} \dfrac{\dfrac{\dfrac{\Gamma\vdash A}{\Gamma,C\vdash A}\,W}{\Box\Gamma,\Diamond C\vdash\Diamond A}\,K_\Diamond}{\Box\Gamma,\Diamond B,\Diamond C\vdash\Diamond A}\,W$		

$\equiv_{CP} := (\equiv \cup \equiv_{c} \cup \equiv_{e}) \qquad \equiv_{\lambda} := (\equiv_{CP} \cup \equiv_{u}) \qquad \equiv_{WIS} := (\equiv_{\lambda} \cup \equiv_{\Box c}) \qquad \equiv_{\Diamond w} := (\equiv_{WIS} \cup \equiv_{\Box c})$

No possible proof systems capturing the whole proof equivalence

Related works
Work in Progress
Future works

Related works/Works in Progress:

- Compositionality for Combinatorial proofs
  - Classical [Hug06,Str17,Omi&Str22]
  - Linear [Acc20]
  - Intuitionistic [Hei&Hug&Str22]
- Combinatorial Proofs as proof certificates (theorem provers interoperability)
- Combinatorial Proofs for Higher-Order logics
- Combinatorial Proofs with Fixed-points
- Combinatorial Proofs and Game Semantics [Hei&Hug&Str19,Acc&Cat&Str21]

Thanks

Thanks

Questions?