Proof counts

Noam Zeilberger

Carnegie Mellon University

Rutgers Experimental Math Seminar

November 4, 2005

Not on the agenda

A proof of $P \supset P$:

1. $(P \supset ((P \supset P) \supset P)) \supset ((P \supset (P \supset P)) \supset (P \supset P))$
   by AX2 taking $A = P$, $B = P \supset P$, $C = P$
2. $P \supset ((P \supset P) \supset P)$
   by AX1 taking $A = P$, $B = P \supset P$
3. $(P \supset (P \supset P)) \supset (P \supset P)$
   applying MP to (1) and (2)
4. $P \supset (P \supset P)$
   by AX1 taking $A = P$, $B = P$
5. $P \supset P$
   applying MP on (3) and (4) $\square$

Structural proof theory

Studies proofs, not just provability, exposing their structure.

Why does structure matter?

- Structured proofs are easier to understand.
- Programs are proofs! Unstructured programming considered harmful.
- Create new logics/languages by manipulating structure.

Why you should know this stuff

To help me!

But also because proof theory led to "linear logic," which is expressive enough to represent many combinatorial problems.

- Can use automated theorem provers as an experimental tool.
- Find new solutions suggested by logical principles?

Talk outline

1. Sequent calculus: overview and results
2. Linear logic: an introduction
3. Encoding graph problems in linear logic
4. Bijections between proofs and various combinatorial objects

Talk outline

1. Sequent calculus: overview and results
2. Linear logic: an introduction
3. Encoding graph problems in linear logic
4. Bijections between proofs and various combinatorial objects

Part 4 intended to spark discussion.

Talk outline

1. Sequent calculus: overview and results
2. Linear logic: an introduction
3. Encoding graph problems in linear logic
4. Bijections between proofs and various combinatorial objects

Part 4 intended to spark discussion.

(In other words, it's sketchy.)

Logic without axioms

Sequent calculus: Gerhard Gentzen ’35
Invented to study “natural deduction”, a reaction to Principia Mathematica

Basic judgment:

$$\underbrace{A_1, \ldots, A_n}_{\text{hypotheses}} \quad \to \quad \underset{\text{conclusion}}{B}$$

Theoremhood is a special case: $\cdot \to B$

No axioms.

Primitives

"If A is a hypothesis, then we may conclude A":

$$\frac{}{\Gamma, A \rightarrow A}\;init$$

"If we can show A, we may assume it as a hypothesis to show C":

$$\frac{\Gamma \rightarrow A \quad \Gamma, A \rightarrow C}{\Gamma \rightarrow C}\;cut$$

Logical rules

Divided into left and right rules.

Right rules explain how to draw a conclusion.
Left rules explain how to use a hypothesis.

Intuitively, right rules define a connective's meaning; left rules apply its meaning.

Implication

$$\frac{\Gamma, A \rightarrow B}{\Gamma \rightarrow A \supset B} \supset R$$

$$\frac{\Gamma, A \supset B \rightarrow A \quad \Gamma, A \supset B, B \rightarrow C}{\Gamma, A \supset B \rightarrow C} \supset L$$

Example: $P \supset P$

$$\frac{\overline{P \rightarrow P}}{\cdot \rightarrow P \supset P}$$

Conjunction/disjunction

$$\frac{\Gamma \rightarrow A \quad \Gamma \rightarrow B}{\Gamma \rightarrow A \wedge B} \wedge R$$

$$\frac{\Gamma, A \wedge B, A \rightarrow C}{\Gamma, A \wedge B \rightarrow C} \wedge L_1 \qquad \frac{\Gamma, A \wedge B, B \rightarrow C}{\Gamma, A \wedge B \rightarrow C} \wedge L_2$$

$$\frac{\Gamma \rightarrow A}{\Gamma \rightarrow A \vee B} \vee R_1 \qquad \frac{\Gamma \rightarrow B}{\Gamma \rightarrow A \vee B} \vee R_2$$

$$\frac{\Gamma, A \vee B, A \rightarrow C \quad \Gamma, A \vee B, B \rightarrow C}{\Gamma, A \vee B \rightarrow C} \vee L$$

Units

$$\frac{}{\Gamma, F \rightarrow C}\ FL \qquad \frac{}{\Gamma \rightarrow T}\ TR$$

Units

$$\frac{}{\Gamma, F \to C}\ FL \qquad \frac{}{\Gamma \to T}\ TR$$

(No FR, TL.)

Sequent calculus properties

Can restrict to atomic initial sequents:

$$\overline{\Gamma, P \rightarrow P}\ init'$$

General $init$ is admissible, e.g.:

$$\dfrac{\dfrac{\dfrac{\vdots}{\Gamma, A \vee B, A \rightarrow A}}{\Gamma, A \vee B, A \rightarrow A \vee B} \quad \dfrac{\dfrac{\vdots}{\Gamma, A \vee B, B \rightarrow B}}{\Gamma, A \vee B, B \rightarrow A \vee B}}{\Gamma, A \vee B \rightarrow A \vee B}$$

Implies that left rules are "strong enough."

But more amazingly: can eliminate cut rule.

Cut elimination

(Counter-)intuitively: "Any proof that uses lemmas can be converted into one that doesn't."

Cut-free proofs serve as "normal forms" for general proofs (cf. values vs. programs).

Cut-elimination implies:

- consistency: $\cdot \not\to F$. Can extend this to FOL, Peano arithmetic…
- disjunction property: if $\cdot \to A \vee B$ then $\cdot \to A$ or $\cdot \to B$.

Cut elimination

(Counter-)intuitively: "Any proof that uses lemmas can be converted into one that doesn't."

Cut-free proofs serve as "normal forms" for general proofs (cf. values vs. programs).

Cut-elimination implies:

- consistency: $\cdot \not\to F$. Can extend this to FOL, Peano arithmetic…
- disjunction property: if $\cdot \to A \vee B$ then $\cdot \to A$ or $\cdot \to B$. Now wait a sec…

Classical logic

New judgment:

$$\underbrace{A_1, \ldots, A_n}_{\text{hypotheses}} \quad \rightarrow \quad \underbrace{B_1, \ldots, B_k}_{\text{possible conclusions}}$$

Symmetrize intuitionistic logic by allowing multiple conclusions (growing monotonically).

Classical logic

New judgment:

$$\underbrace{A_1, \ldots, A_n}_{\text{hypotheses}} \quad \longrightarrow \quad \underbrace{B_1, \ldots, B_k}_{\text{possible conclusions}}$$

Symmetrize intuitionistic logic by allowing multiple conclusions (growing monotonically).

$$\frac{}{\Gamma, A \to A}\ init \qquad \frac{\Gamma \to A \quad \Gamma, A \to C}{\Gamma \to A}\ cut$$

Classical logic

New judgment:

$$\underbrace{A_1, \ldots, A_n}_{\text{hypotheses}} \quad \longrightarrow \quad \underbrace{B_1, \ldots, B_k}_{\text{possible conclusions}}$$

Symmetrize intuitionistic logic by allowing multiple conclusions (growing monotonically).

$$\frac{}{\Gamma, A \rightarrow A, \Delta}\, init \qquad \frac{\Gamma \rightarrow A, \Delta \quad \Gamma, A \rightarrow \Delta}{\Gamma \rightarrow \Delta}\, cut$$

Classical logic

New judgment:

$$\underbrace{A_1, \ldots, A_n}_{\text{hypotheses}} \quad \longrightarrow \quad \underbrace{B_1, \ldots, B_k}_{\text{possible conclusions}}$$

Symmetrize intuitionistic logic by allowing multiple conclusions (growing monotonically).

$$\frac{\Gamma, A \to B}{\Gamma \to A \supset B} \supset R$$

$$\frac{\Gamma, A \supset B \to A \quad \Gamma, A \supset B, B \to C}{\Gamma, A \supset B \to C} \supset L$$

Classical logic

New judgment:

$$\underbrace{A_1, \ldots, A_n}_{\text{hypotheses}} \quad \rightarrow \quad \underbrace{B_1, \ldots, B_k}_{\text{possible conclusions}}$$

Symmetrize intuitionistic logic by allowing multiple conclusions (growing monotonically).

$$\frac{\Gamma, A \rightarrow B, A \supset B, \Delta}{\Gamma \rightarrow A \supset B, \Delta} \supset R$$

$$\frac{\Gamma, A \supset B \rightarrow A, \Delta \quad \Gamma, A \supset B, B \rightarrow \Delta}{\Gamma, A \supset B \rightarrow \Delta} \supset L$$

Classical logic

New judgment:

$$\underbrace{A_1, \ldots, A_n}_{\text{hypotheses}} \quad \longrightarrow \quad \underbrace{B_1, \ldots, B_k}_{\text{possible conclusions}}$$

Symmetrize intuitionistic logic by allowing multiple conclusions (growing monotonically).

[et cetera]

Classical logic

New judgment:

$$\underbrace{A_1, \ldots, A_n}_{\text{hypotheses}} \quad \longrightarrow \quad \underbrace{B_1, \ldots, B_k}_{\text{possible conclusions}}$$

Proof of excluded middle:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \longrightarrow A, A \supset F, A \vee (A \supset F)}\ init}{\cdot \longrightarrow A, A \supset F, A \vee (A \supset F)}\ {\supset}R}{\cdot \longrightarrow A, A \vee (A \supset F)}\ {\vee}R_2}{\cdot \longrightarrow A \vee (A \supset F)}\ {\vee}R_1$$

Sequent calculus: conclusions

Exposes the nature of logic as reasoning under hypotheses.

Cut-free proofs provide interesting objects of study; justified by cut-elimination.

Philosophical arguments over axioms become concrete differences in proof structure.

But are there still unquestioned assumptions in the structure of the sequent calculus?

Logic without eternity

Linear logic: Jean-Yves Girard ′87

Linear hypothetical judgment:

$$A_1, \ldots, A_n \Rightarrow B$$

Must use hypotheses $A_1, \ldots A_n$ *exactly once*.

No longer maintain structural properties of:

1. Weakening: if $\Gamma \rightarrow C$ then $\Gamma, A \rightarrow C$
2. Contraction: if $\Gamma, A, A \rightarrow C$ then $\Gamma, A \rightarrow C$

New primitives

$$\frac{}{\Gamma, A \rightarrow A}\; init \qquad \frac{\Gamma \rightarrow A \quad \Gamma, A \rightarrow C}{\Gamma \rightarrow C}\; cut$$

New primitives

$$\frac{}{A \Rightarrow A}\; init \qquad \frac{\Gamma \rightarrow A \quad \Gamma, A \rightarrow C}{\Gamma \rightarrow C}\; cut$$

New primitives

$$\frac{}{A \Rightarrow A}\ init \qquad \frac{\Gamma \Rightarrow A \quad \Delta, A \Rightarrow C}{\Gamma, \Delta \Rightarrow C}\ cut$$

Linear implication

$$\frac{\Gamma, A \supset B \to A \quad \Gamma, A \supset B, B \to C}{\Gamma, A \supset B \to C} \supset L$$

Linear implication

$$\frac{\Gamma \qquad\qquad \to A \quad \Gamma \qquad\qquad , B \to C}{\Gamma, A \supset B \to C} \supset L$$

Linear implication

$$\frac{\Gamma \rightarrow A \quad \Gamma, B \rightarrow C}{\Gamma, A \supset B \rightarrow C} \supset L$$

Linear implication

$$\frac{\Gamma \to A \quad \Delta, B \to C}{\Gamma, \Delta, A \supset B \to C} \supset L$$

Linear implication

$$\frac{\Gamma \Rightarrow A \quad \Delta, B \Rightarrow C}{\Gamma, \Delta, A \multimap B \Rightarrow C} \multimap L$$

Linear implication

$$\frac{\Gamma \Rightarrow A \quad \Delta, B \Rightarrow C}{\Gamma, \Delta, A \multimap B \Rightarrow C} \multimap L$$

Can *consume* A to *produce* B.

Right rule confirms this meaning:

$$\frac{\Gamma, A \Rightarrow B}{\Gamma \Rightarrow A \multimap B} \multimap R$$

Linear conjunction

$$\frac{\Gamma, A \wedge B, A \to C}{\Gamma, A \wedge B \to C} \wedge L_1 \qquad \frac{\Gamma, A \wedge B, B \to C}{\Gamma, A \wedge B \to C} \wedge L_2$$

Linear conjunction

$$\frac{\Gamma \qquad\qquad\qquad , A \rightarrow C}{\Gamma, A \wedge B \rightarrow C} \wedge L_1 \qquad \frac{\Gamma \qquad\qquad\qquad , B \rightarrow C}{\Gamma, A \wedge B \rightarrow C} \wedge L_2$$

Linear conjunction

$$\frac{\Gamma, A \to C}{\Gamma, A \wedge B \to C} \wedge L_1 \qquad \frac{\Gamma, B \to C}{\Gamma, A \wedge B \to C} \wedge L_2$$

Linear conjunction

$$\frac{\Gamma, A \Rightarrow C}{\Gamma, A \mathbin{\&} B \Rightarrow C} \;\&L_1 \qquad \frac{\Gamma, B \Rightarrow C}{\Gamma, A \mathbin{\&} B \Rightarrow C} \;\&L_2$$

Linear conjunction

$$\frac{\Gamma, A \Rightarrow C}{\Gamma, A \mathbin{\&} B \Rightarrow C}\ \&L_1 \qquad \frac{\Gamma, B \Rightarrow C}{\Gamma, A \mathbin{\&} B \Rightarrow C}\ \&L_2$$

Choice between A and B.

Justified by right rule:

$$\frac{\Gamma \Rightarrow A \quad \Gamma \Rightarrow B}{\Gamma \Rightarrow A \mathbin{\&} B}\ \&R$$

Linear conjunction, version two

But consider alternative left rule for $\wedge$:

$$\frac{\Gamma, A \wedge B, A, B \rightarrow C}{\Gamma, A \wedge B \rightarrow C} \wedge L$$

Linear conjunction, version two

But consider alternative left rule for $\wedge$:

$$\frac{\Gamma \qquad\qquad , A, B \to C}{\Gamma, A \wedge B \to C} \wedge L$$

Linear conjunction, version two

But consider alternative left rule for $\wedge$:

$$\frac{\Gamma, A, B \Rightarrow C}{\Gamma, A \otimes B \Rightarrow C} \otimes L$$

Linear conjunction, version two

But consider alternative left rule for $\wedge$:

$$\frac{\Gamma, A, B \Rightarrow C}{\Gamma, A \otimes B \Rightarrow C} \otimes L$$

Both A and B.

Corresponding right rule:

$$\frac{\Gamma \Rightarrow A \quad \Delta \Rightarrow B}{\Gamma, \Delta \Rightarrow A \otimes B} \otimes R$$

Linear disjunction

$$\frac{\Gamma, A \vee B, A \to C \quad \Gamma, A \vee B, B \to C}{\Gamma, A \vee B \to C} \vee L$$

Linear disjunction

$$\frac{\Gamma, A \Rightarrow C \quad \Gamma, B \Rightarrow C}{\Gamma, A \oplus B \Rightarrow C} \oplus L$$

Linear disjunction

$$\frac{\Gamma, A \Rightarrow C \quad \Gamma, B \Rightarrow C}{\Gamma, A \oplus B \Rightarrow C} \oplus L$$

Choice of A or B: but not your choice!

Linear disjunction

$$\frac{\Gamma, A \Rightarrow C \quad \Gamma, B \Rightarrow C}{\Gamma, A \oplus B \Rightarrow C} \oplus L$$

Choice of A or B: but not your choice!

Right rules:

$$\frac{\Gamma \Rightarrow A}{\Gamma \Rightarrow A \oplus B} \oplus R_1 \qquad \frac{\Gamma \Rightarrow B}{\Gamma \Rightarrow A \oplus B} \oplus R_2$$

Linear units

$$\frac{}{\Gamma, F \rightarrow C}\ FL \qquad \frac{}{\Gamma \rightarrow T}\ TR$$

Linear units

$$\frac{}{\Gamma, 0 \Rightarrow C}\ 0L \qquad \frac{}{\Gamma \Rightarrow \top}\ \top R$$

Linear units

$$\frac{}{\Gamma, 0 \Rightarrow C}\ 0L \qquad \frac{}{\Gamma \Rightarrow \top}\ \top R$$

$$\frac{\Gamma \Rightarrow C}{\Gamma, 1 \Rightarrow C}\ 1L \qquad \frac{}{\cdot \Rightarrow 1}\ 1R$$

Linear units

$$\frac{}{\Gamma, 0 \Rightarrow C}\ 0L \qquad \frac{}{\Gamma \Rightarrow \top}\ \top R$$

$$\frac{\Gamma \Rightarrow C}{\Gamma, 1 \Rightarrow C}\ 1L \qquad \frac{}{\cdot \Rightarrow 1}\ 1R$$

$$A \oplus 0 \Leftrightarrow A \quad A \,\&\, \top \Leftrightarrow A \quad A \otimes 1 \Leftrightarrow A$$

Summary of connectives

$A \multimap B$	consume A to produce B
$A \mathbin{\&} B$	your choice between A and B
$A \otimes B$	both A and B
$A \oplus B$	adversary's choice of A or B
$\top$	something
1	nothing
0	anything

Summary of connectives

$A \multimap B$	consume A to produce B
$A \mathbin{\&} B$	your choice between A and B
$A \otimes B$	both A and B
$A \oplus B$	adversary's choice of A or B
$\top$	something
1	nothing
0	anything

But what about our old friends $\supset$, $\wedge$, and $\vee$?

Regaining ordinary logic

Use notion of *persistent* resource.

Rules now carry persistent context Π:

Regaining ordinary logic

Use notion of *persistent* resource.

Rules now carry persistent context Π:

$$\frac{}{A \Rightarrow A}\ init$$

Regaining ordinary logic

Use notion of *persistent* resource.

Rules now carry persistent context Π:

$$\overline{\Pi; A \Rightarrow A}\ init$$

Regaining ordinary logic

Use notion of *persistent* resource.

Rules now carry persistent context Π:

$$\frac{\Gamma \Rightarrow A \quad \Delta, B \Rightarrow C}{\Gamma, \Delta, A \multimap B \Rightarrow C} \multimap L$$

$$\frac{\Gamma, A \Rightarrow B}{\Gamma \Rightarrow A \multimap B} \multimap R$$

Regaining ordinary logic

Use notion of *persistent* resource.

Rules now carry persistent context Π:

$$\frac{\Pi; \Gamma \Rightarrow A \quad \Pi; \Delta, B \Rightarrow C}{\Pi; \Gamma, \Delta, A \multimap B \Rightarrow C} \multimap L$$

$$\frac{\Pi; \Gamma, A \Rightarrow B}{\Pi; \Gamma \Rightarrow A \multimap B} \multimap R$$

Regaining ordinary logic

Use notion of *persistent* resource.

Rules now carry persistent context Π:

[et cetera]

Regaining ordinary logic

Use notion of *persistent* resource.

Rules now carry persistent context Π:

Additional rule:

$$\frac{\Pi, A; \Gamma, A \Rightarrow C}{\Pi, A; \Gamma \Rightarrow C}\ copy$$

Regaining ordinary logic (cont.)

Internalize persistence with ! modality:

$$\frac{\Pi, A; \Gamma \Rightarrow C}{\Pi; \Gamma, !\, A \Rightarrow C} \; !L \qquad \frac{\Pi; \cdot \Rightarrow A}{\Pi; \cdot \Rightarrow !\, A} \; !R$$

Regaining ordinary logic (cont.)

Internalize persistence with ! modality:

$$\frac{\Pi, A; \Gamma \Rightarrow C}{\Pi; \Gamma, !\,A \Rightarrow C}\ !L \qquad \frac{\Pi; \cdot \Rightarrow A}{\Pi; \cdot \Rightarrow !\,A}\ !R$$

Can decompose ordinary connectives:

$$\text{“}A \supset B\text{”} = !\,A \multimap B$$
$$\text{“}A \wedge B\text{”} = !\,A \otimes !\,B = !(A \,\&\, B)$$
$$\text{“}A \vee B\text{”} = !\,A \oplus !\,B$$

A delicious proposition

"trick or treat!"

$\multimap$

$\otimes$

A delicious proposition

“trick or treat!”

$\multimap$

 & 

A delicious proposition

“trick or treat!”

$$\multimap$$

$!$ 

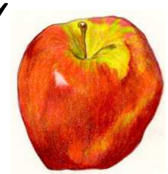
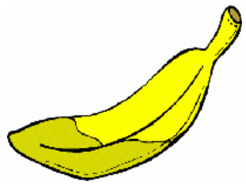
A delicious proposition

"trick or treat!"

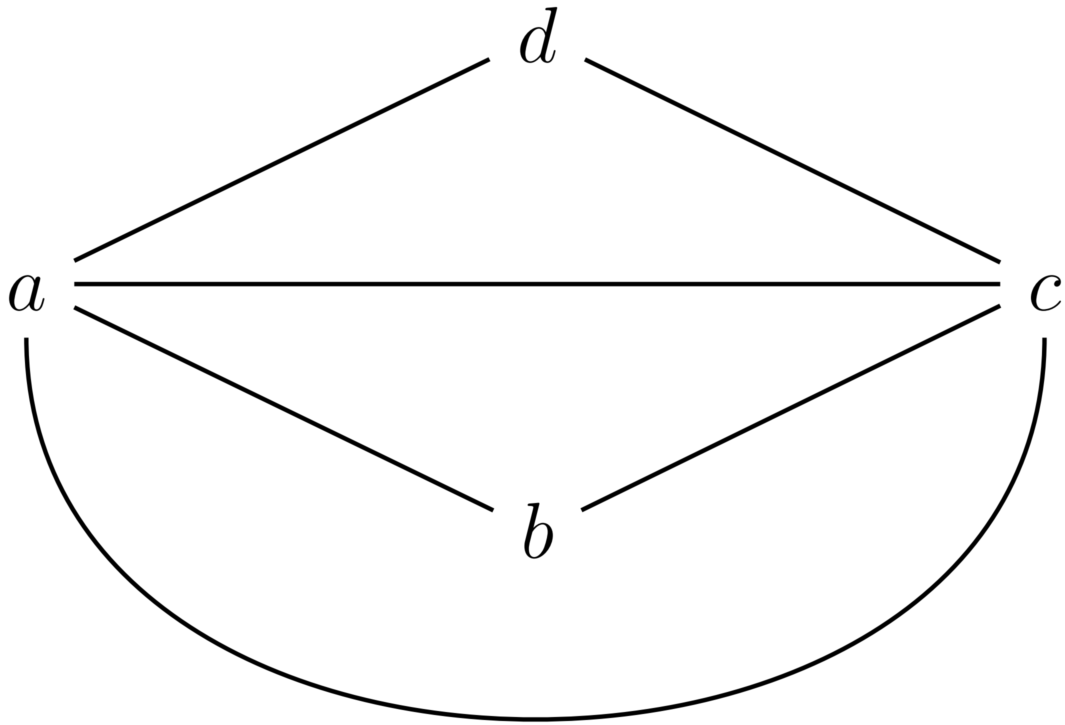
$\multimap$

$\Bigg($ 

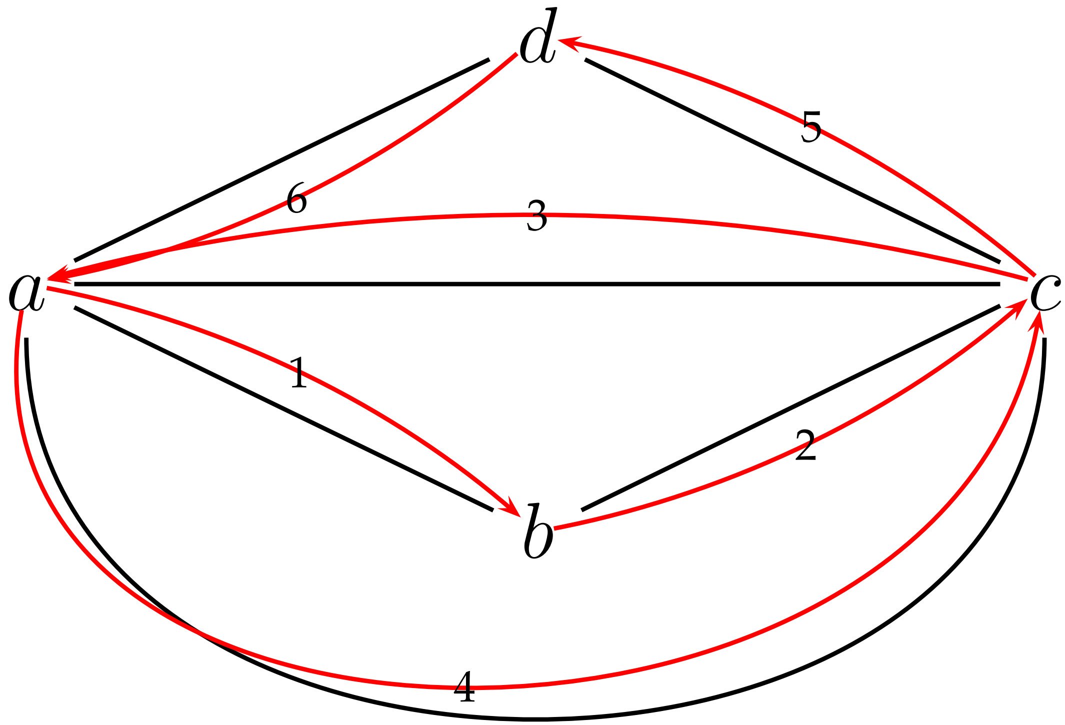
$\otimes$ 

$\Bigg) \oplus \Bigg($  $\&$  $\Bigg) \oplus !$  $\oplus \ldots$

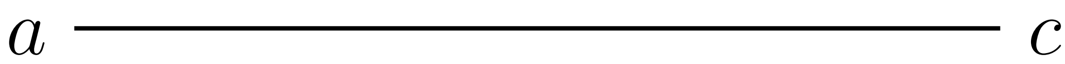
Euler tours



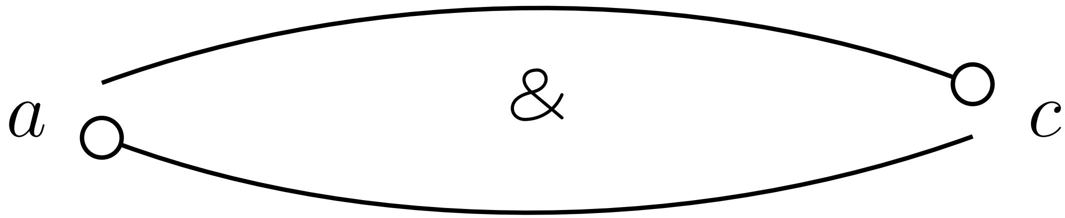
Euler tours



Euler tours



Euler tours



"a" means I am at a
"$a \multimap c$" means I will go from a to c
"$(a \multimap c) \,\&\, (c \multimap a)$" means I can go either way

Euler tours: encoding

$$Euler(G) = \bigotimes_{\{x,y\} \in G_E} (x \multimap y) \,\&\, (y \multimap x)$$

G has an Euler tour starting at $s \in G_V$ iff:

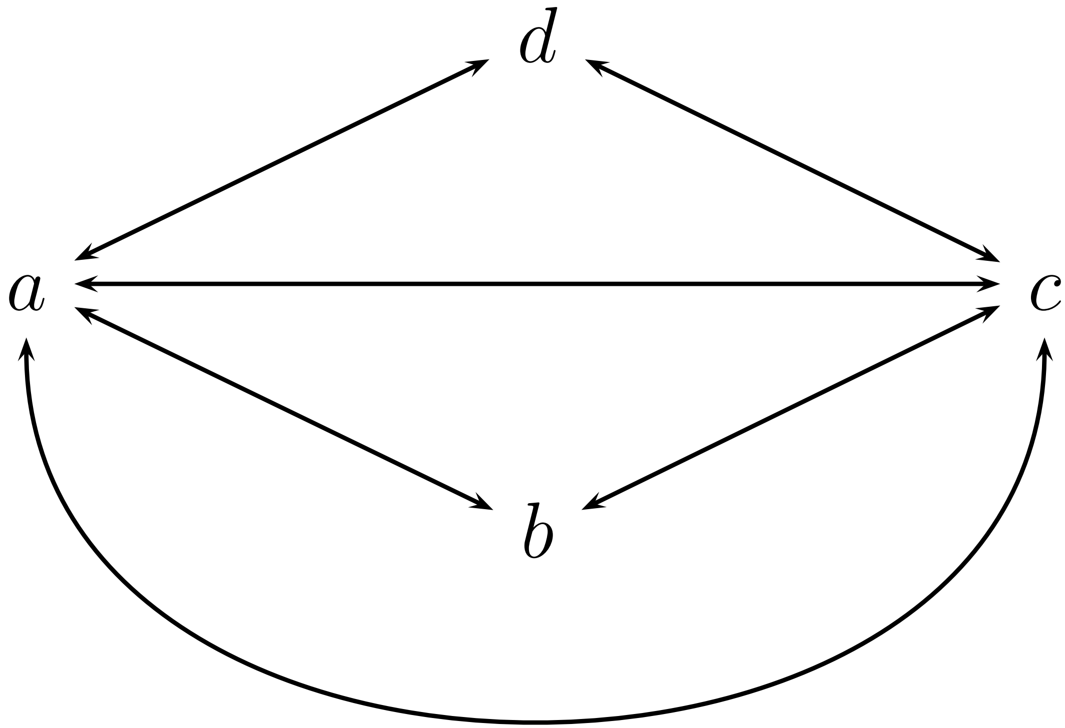
$$Euler(G) \Rightarrow s \multimap s$$

(Compare deducing $s \supset s$ in ordinary logic.)

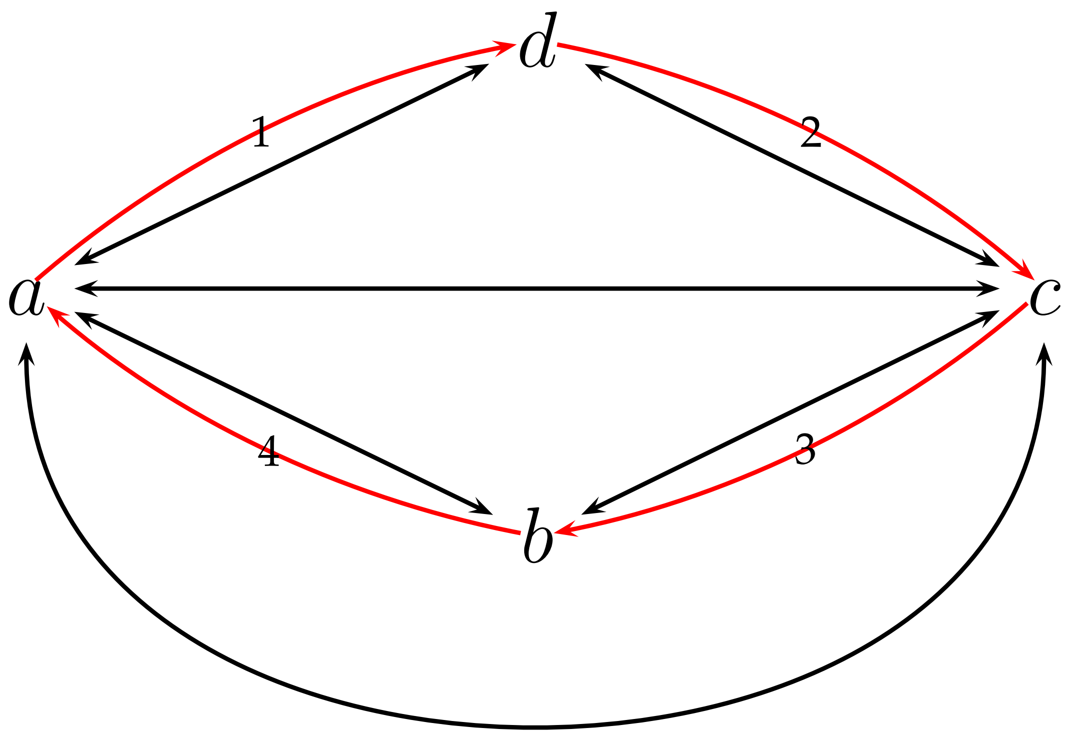
Euler tours: derivation

$$
\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{a \Rightarrow a \qquad b \Rightarrow b}{a \multimap b, a \Rightarrow b} \qquad c \Rightarrow c}{a \multimap b, b \multimap c, a \Rightarrow c} \qquad a \Rightarrow a}{a \multimap b, c \multimap a, b \multimap c, a \Rightarrow a} \qquad c \Rightarrow c}{a \multimap b, c \multimap a, a \multimap c, b \multimap c, a \Rightarrow c} \qquad d \Rightarrow d}{a \multimap b, c \multimap a, a \multimap c, b \multimap c, c \multimap d, a \Rightarrow d} \qquad a \Rightarrow a}{a \multimap b, c \multimap a, a \multimap c, d \multimap a, b \multimap c, c \multimap d, a \Rightarrow a}}{Euler(G), a \Rightarrow a}\ \&L^{*}}{Euler(G) \Rightarrow a \multimap a}\ \multimap R
$$

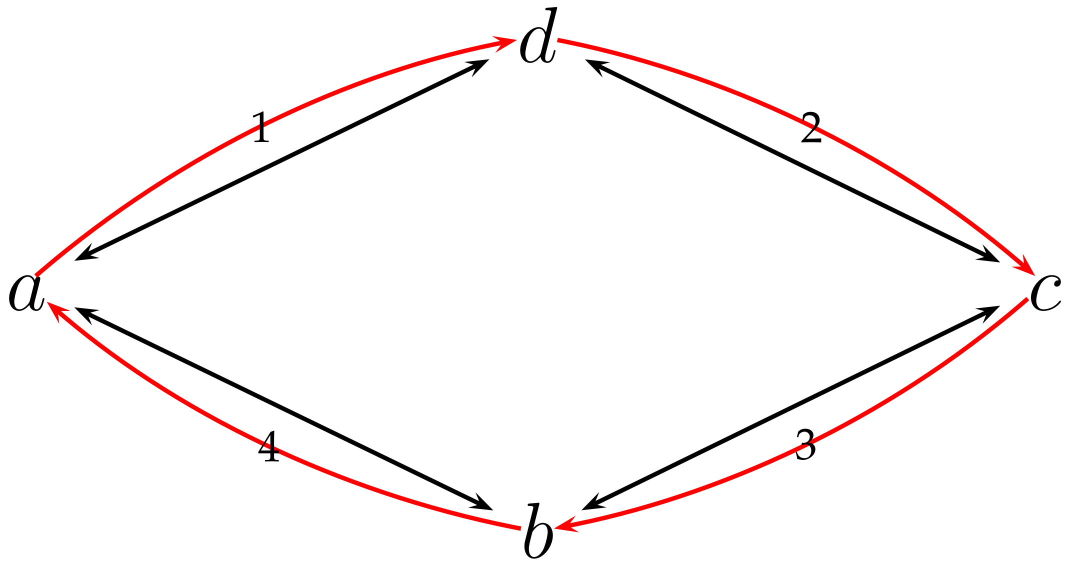
Hamiltonian tours



Hamiltonian tours



Hamiltonian tours



Resource interpretation:

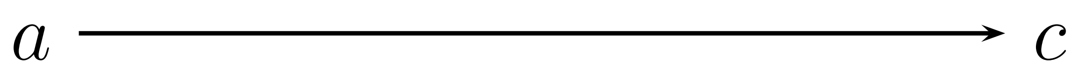
- Fact u_x holds while node x remains unvisited
- Visiting x "consumes" the fact u_x

Hamiltonian tours

$$a \longrightarrow c$$

Interpretation of an edge?

Hamiltonian tours



Interpretation of an edge: $(a \otimes u_c) \multimap c$?

Hamiltonian tours

$$a \longrightarrow c$$

Interpretation of an edge: $((a \otimes u_c) \multimap c) \,\&\, 1$

An edge is an “affine” resource.

Hamiltonian tours: encoding

$$Hamilton(G) =$$
$$\left(\bigotimes_{x \in G_V} u_x\right) \otimes \left(\bigotimes_{(x,y) \in G_E} ((x \otimes u_y) \multimap y) \mathbin{\&} 1\right)$$

G has a Hamiltonian tour starting at $s \in G_V$ iff:

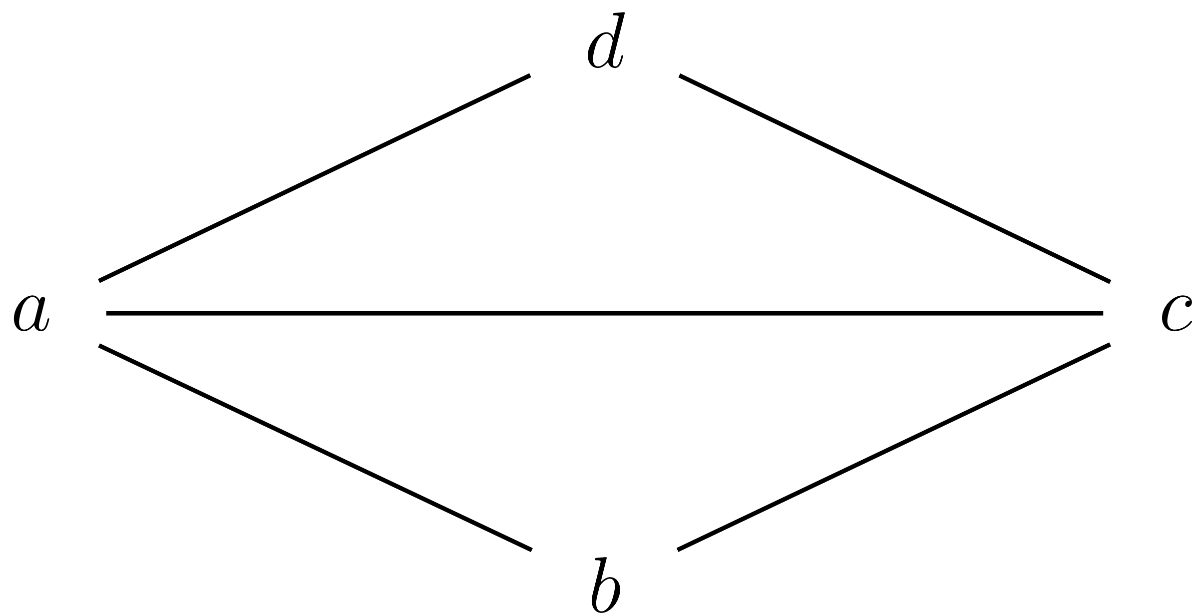
$$Hamilton(G) \Rightarrow s \multimap s$$

(Thanks to Jason Reed for this encoding.)

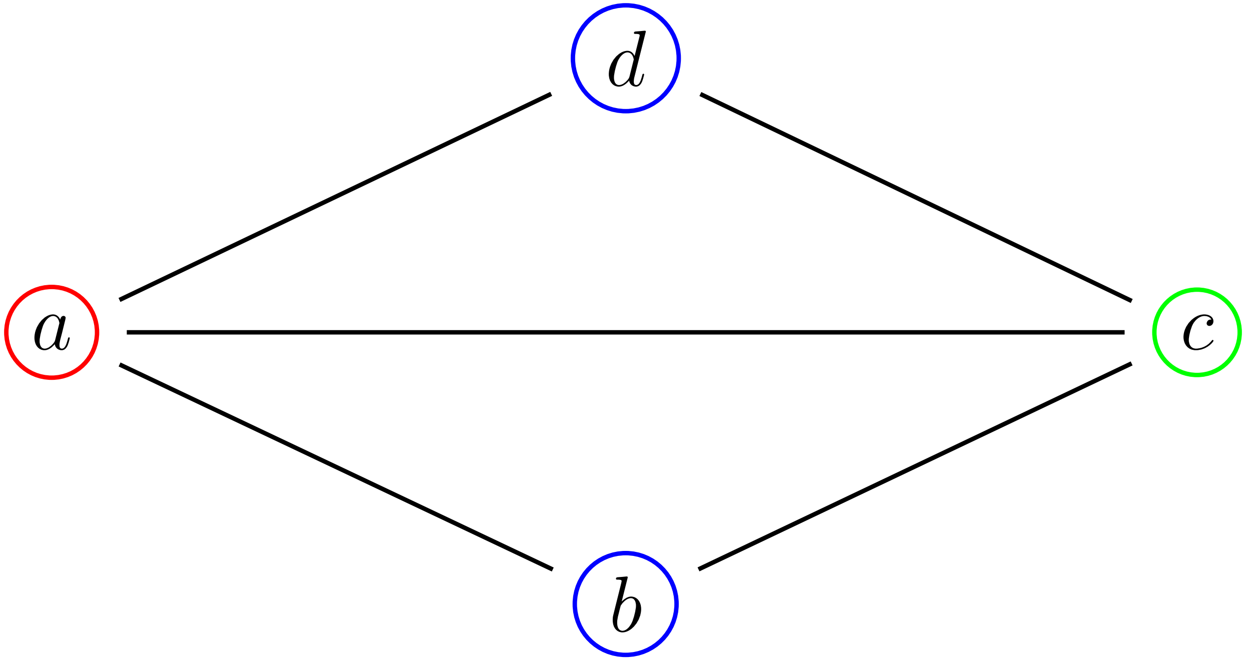
Hamiltonian tours: derivation

$$\dfrac{a, u_d \Rightarrow a \otimes {\color{red}u_d} \quad \dfrac{d, u_c \Rightarrow d \otimes {\color{red}u_c} \quad \dfrac{c, u_b \Rightarrow c \otimes {\color{red}u_b} \quad \dfrac{b, u_a \Rightarrow b \otimes {\color{red}u_a} \quad a \Rightarrow a}{u_a, b, (b \otimes u_a) \multimap a \Rightarrow a}}{u_a, u_b, c, (c \otimes u_b) \multimap b, (b \otimes u_a) \multimap a \Rightarrow a}}{u_a, u_b, u_c, d, (d \otimes u_c) \multimap c, (c \otimes u_b) \multimap b, (b \otimes u_a) \multimap a \Rightarrow a}}{\dfrac{u_a, u_b, u_c, u_d, (a \otimes u_d) \multimap d, (d \otimes u_c) \multimap c, (c \otimes u_b) \multimap b, (b \otimes u_a) \multimap a, a \Rightarrow a}{Hamilton(G), a \Rightarrow a}}$$

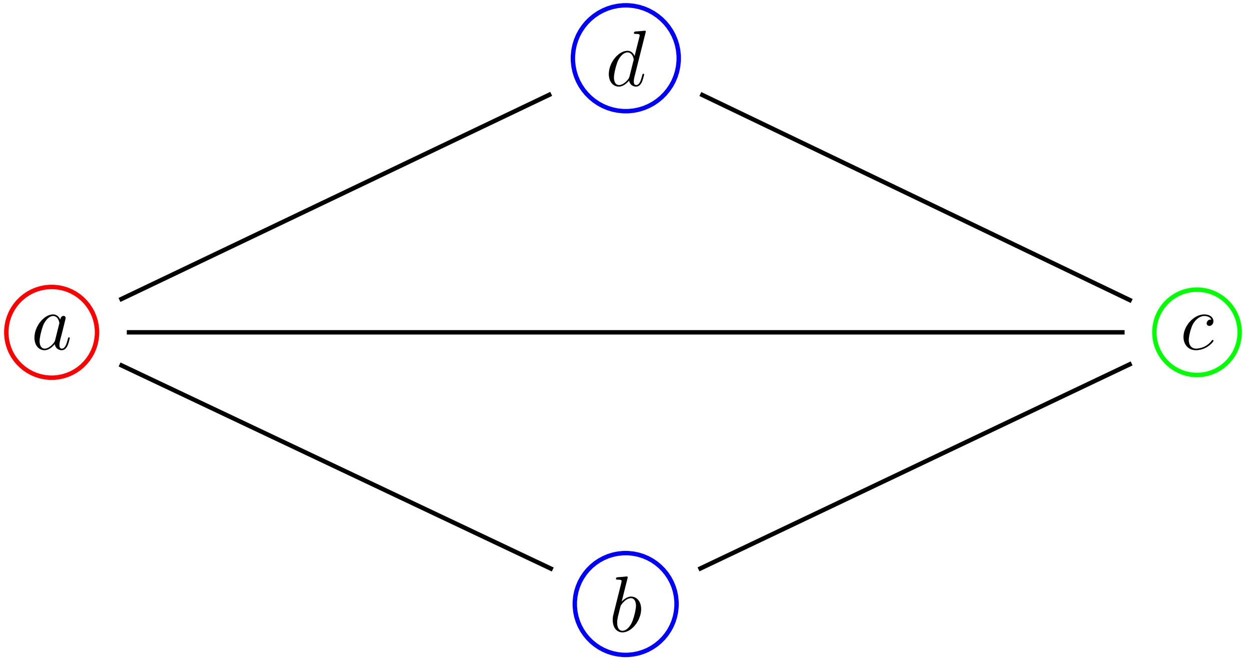
Graph colorings



Graph colorings



Graph colorings



Key to linear logic interpretation:

- A node's color doesn't change (!)
- But we can assign it a color only once ($\&$)

Graph colorings: encoding

$$
\begin{aligned}
color_x &= !x_r \& !x_g \& !x_b \\
okay_x &= \left(x_r \otimes \bigotimes_{\{x,y\} \in G_E} (y_g \oplus y_b) \right) \oplus \\
&\quad \left(x_g \otimes \bigotimes_{\{x,y\} \in G_E} (y_r \oplus y_b) \right) \oplus \\
&\quad \left(x_b \otimes \bigotimes_{\{x,y\} \in G_E} (y_r \oplus y_g) \right)
\end{aligned}
$$

Graph colorings: encoding

Graph is 3-colorable iff:

$$\bigotimes_{x \in G_V} color_x \Rightarrow \bigotimes_{x \in G_V} okay_x$$

Counting proofs

Since linear logic is constructive, proofs of propositions correspond to actual Euler tours, Hamiltonian tours, graph colorings, etc.

But is there a bijection (with *cut-free* proofs)?

Not quite:

$$
\dfrac{\dfrac{a \Rightarrow a \qquad \dfrac{b \Rightarrow b \quad c \Rightarrow c}{b, b \multimap c \Rightarrow c}}{a \multimap b, b \multimap c, a \Rightarrow c}}{a \multimap b, b \multimap c \Rightarrow a \multimap c}
\qquad
\dfrac{\dfrac{\dfrac{a \Rightarrow a \quad b \Rightarrow b}{a \multimap b, a \Rightarrow b} \qquad c \Rightarrow c}{a \multimap b, b \multimap c, a \Rightarrow c}}{a \multimap b, b \multimap c \Rightarrow a \multimap c}
$$

Counting proofs

Since linear logic is constructive, proofs of propositions correspond to actual Euler tours, Hamiltonian tours, graph colorings, etc.

But is there a bijection (with *cut-free* proofs)?

Not quite:

$$
\dfrac{\dfrac{a \Rightarrow a \qquad \dfrac{b \Rightarrow b \quad c \Rightarrow c}{b, b \multimap c \Rightarrow c}}{a \multimap b, b \multimap c, a \Rightarrow c}}{a \multimap b, b \multimap c \Rightarrow a \multimap c}
\qquad
\dfrac{\dfrac{\dfrac{a \Rightarrow a \quad b \Rightarrow b}{a \multimap b, a \Rightarrow b} \qquad c \Rightarrow c}{a \multimap b, b \multimap c, a \Rightarrow c}}{a \multimap b, b \multimap c \Rightarrow a \multimap c}
$$

Problem: left rules “commute.”

A more perfect syntax

Natural deduction: Gentzen '35

Connectives defined via "introduction" and "elimination" rules.

Instead of applying hypotheses to draw new hypotheses, elimination rules apply conclusions to draw new conclusions.

(Removes distinction hypothesis/conclusion.)

Natural deduction

Right rules become introduction rules:

$$\frac{\Gamma, A \Rightarrow B}{\Gamma \Rightarrow A \multimap B} \multimap R$$

$$\frac{\Gamma \Rightarrow A \quad \Gamma \Rightarrow B}{\Gamma \Rightarrow A \,\&\, B} \,\&R \qquad \frac{\Gamma \Rightarrow A \quad \Delta \Rightarrow B}{\Gamma, \Delta \Rightarrow A \otimes B} \otimes R$$

$$\frac{\Gamma \Rightarrow A}{\Gamma \Rightarrow A \oplus B} \oplus R_1 \quad \frac{\Gamma \Rightarrow B}{\Gamma \Rightarrow A \oplus B} \oplus R_2$$

$$\frac{}{\Gamma \Rightarrow \top} \top R \quad \frac{}{\cdot \Rightarrow 1} 1R$$

Natural deduction

Right rules become introduction rules:

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \multimap B} \multimap I$$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \,\&\, B} \,\&I \qquad \frac{\Gamma \vdash A \quad \Delta \vdash B}{\Gamma, \Delta \vdash A \otimes B} \otimes I$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \oplus B} \oplus I_1 \quad \frac{\Gamma \vdash B}{\Gamma \vdash A \oplus B} \oplus I_2$$

$$\frac{}{\Gamma \vdash \top} \top I \quad \frac{}{\cdot \vdash 1} 1I$$

Natural deduction

Right rules become introduction rules:

"Flip" left rules to make elimination rules:

$$\frac{\Gamma \Rightarrow A \quad \Delta, B \Rightarrow C}{\Gamma, \Delta, A \multimap B \Rightarrow C} \multimap L$$

$$\frac{\Gamma, A \Rightarrow C}{\Gamma, A \mathbin{\&} B \Rightarrow C} \mathbin{\&} L_1 \qquad \frac{\Gamma, B \Rightarrow C}{\Gamma, A \mathbin{\&} B \Rightarrow C} \mathbin{\&} L_2$$

Natural deduction

Right rules become introduction rules:

"Flip" left rules to make elimination rules:

$$\frac{\Gamma \vdash A \multimap B \quad \Delta \vdash A}{\Gamma, \Delta \vdash B} \multimap E$$

$$\frac{\Gamma \vdash A \,\&\, B}{\Gamma \vdash A} \,\&E_1 \qquad \frac{\Gamma \vdash A \,\&\, B}{\Gamma \vdash B} \,\&E_2$$

Natural deduction

Right rules become introduction rules:

"Flip" left rules to make elimination rules:

$$\frac{\Gamma \vdash A \multimap B \quad \Delta \vdash A}{\Gamma, \Delta \vdash B} \multimap E$$

$$\frac{\Gamma \vdash A \,\&\, B}{\Gamma \vdash A} \,\&E_1 \qquad \frac{\Gamma \vdash A \,\&\, B}{\Gamma \vdash B} \,\&E_2$$

$\otimes E, 1E, \oplus E, 0E$ complicate the picture.

Counting proofs, revisited

Only “normal” proofs: elims followed by intros.

Corresponds to restriction to cut-free proofs.

But different cut-free proofs give same normal proof:

$$\dfrac{b \multimap c \vdash b \multimap c \qquad \dfrac{a \multimap b \vdash a \multimap b \qquad a \vdash a}{a \multimap b, a \vdash b}\multimap E}{\dfrac{a \multimap b, b \multimap c, a \vdash c}{a \multimap b, b \multimap c \vdash a \multimap c}\multimap I}\multimap E$$

Proof counts

Bijective correspondence between normal proofs and solutions to combinatorial problems.

Let $\#[\Gamma \vdash A]$ = # normal proofs of $\Gamma \vdash A$.

- $\#[Euler(G) \vdash s \multimap s]$ = # Euler tours in G
- $\#[(x_1 \oplus \ldots \oplus x_n)^n \vdash (x_1 \oplus \ldots \oplus x_n)^k \otimes \top] = k!\binom{n}{k}$
- $\#[(H \,\&\, T)^n \vdash (H \oplus T)^n] = n! \cdot 2^n$
- $\#[(H \,\&\, T)^n \vdash H^k \otimes T^{n-k}] = k!(n-k)! \cdot \binom{n}{k}$

Future possibilities

Use linear logic theorem provers to enumerate solutions to combinatorial problems.

New theoretical approaches suggested by logical principles:

- Duality?
- Dynamic interpretation of non-normal proofs?

Future possibilities

Use linear logic theorem provers to enumerate solutions to combinatorial problems.

New theoretical approaches suggested by logical principles:

- Duality?
- Dynamic interpretation of non-normal proofs?

Is there a new logic waiting to be discovered by combinatorists?