Introduction to Proof Theory

Lecture 3 - Gentzen's sequent calculus

Anupam Das

University of Birmingham

21st Midlands Graduate School
in Foundations of Computing Science

Sheffield University (virtual)

12 - 16 April 2021

These slides are available at `http://www.anupamdas.com/mgs21`.

Based on slides from ESSLLI'18, prepared with Thomas Powell.

Outline

Proofs, provability and systems

So far we have studied one particular proof system, the Hilbert-Frege system $\mathcal{F}$.

Proofs, provability and systems

So far we have studied one particular proof system, the Hilbert-Frege system $\mathcal{F}$.

But there are many other ones to consider!

- **Natural deduction.** (Normalisation as computation)
- **Sequent calculus.** (General metalogical framework)
- **Resolution.** (Automated theorem proving)
- **Analytic tableaux.** (Semantics)
- Systems with **Extension** or **Substitution**. (Proof complexity)
- **Algebraic** and **Geometric** systems. (Structural proof theory)
- ...

So far we have studied one particular proof system, the Hilbert-Frege system $\mathcal{F}$.

But there are many other ones to consider!

- **Natural deduction.** (Normalisation as computation)
- **Sequent calculus.** (General metalogical framework)
- **Resolution.** (Automated theorem proving)
- **Analytic tableaux.** (Semantics)
- Systems with **Extension** or **Substitution**. (Proof complexity)
- **Algebraic** and **Geometric** systems. (Structural proof theory)
- ...

Question: Why is one system better than another? We will consider just one desideratum here...

The problem with proof search

The problem with proof search

Remember *modus ponens*:

$$(mp)\,\frac{A \quad A \to B}{B}$$

When we are trying to prove a theorem, we often construct proofs bottom-up.

The problem with proof search

Remember *modus ponens*:

$$(mp)\ \frac{A \quad A \to B}{B}$$

When we are trying to prove a theorem, we often construct proofs bottom-up.

ISSUE WITH *MODUS PONENS*: we are trying to prove B, but we have to guess A.

The problem with proof search

Remember *modus ponens*:

$$(mp)\ \frac{A \quad A \to B}{B}$$

When we are trying to prove a theorem, we often construct proofs bottom-up.

Issue with *modus ponens*: we are trying to prove B, but we have to guess A.

This is a serious issue, but reflects the difficulty of the problem at hand:

Proposition

- *Checking whether a propositional formula is valid is* **coNP***-complete*.
- *Checking whether a first-order formula is valid is undecidable*.

The problem with proof search

Remember *modus ponens*:

$$(mp)\ \frac{A \quad A \to B}{B}$$

When we are trying to prove a theorem, we often construct proofs bottom-up.

ISSUE WITH *MODUS PONENS*: we are trying to prove B, but we have to guess A.

This is a serious issue, but reflects the difficulty of the problem at hand:

Proposition

- *Checking whether a propositional formula is valid is* **coNP**-*complete*.
- *Checking whether a first-order formula is valid is undecidable*.

DESIDERATUM: Proofs in $\mathcal{F}$ are rather short (believe it or not): can we trade off proof size for less nondeterminism in proof search?

On analyticity

On analyticity

The gold standard in structural proof theory is analyticity.

The gold standard in structural proof theory is analyticity. It was first considered by Bolzano in the early 19th century:

"*a proof is **analytic** if it does not use concepts beyond its subject matter*"

On analyticity

The gold standard in structural proof theory is analyticity. It was first considered by Bolzano in the early 19th century:

*“a proof is **analytic** if it does not use concepts beyond its subject matter”*

In modern proof theory, ‘concepts’ are interpreted as **subformulae**, *i.e.* ones already *inside* the formula we are trying to prove.

On analyticity

The gold standard in structural proof theory is analyticity. It was first considered by Bolzano in the early 19th century:

*"a proof is **analytic** if it does not use concepts beyond its subject matter"*

In modern proof theory, 'concepts' are interpreted as **subformulae**, *i.e.* ones already *inside* the formula we are trying to prove.

Question

Can we construct a proof system that uses only subformulae of the conclusion?

Three puzzles: guess the invariant!

Three puzzles: guess the invariant!

Puzzle

Dominoes are 2×1 shapes. Given an 8×8 board:

1. Can you tile it with dominoes?
2. What if you remove one corner piece?
3. What if you remove two opposite corner pieces?

Puzzle

Dominoes are 2×1 shapes. Given an 8×8 board:

1. Can you tile it with dominoes?
2. What if you remove one corner piece?
3. What if you remove two opposite corner pieces?

Answers.

1. **Yes!** Do it in the naive way.

Three puzzles: guess the invariant!

Puzzle

Dominoes are 2×1 shapes. Given an 8×8 board:

1. Can you tile it with dominoes?
2. What if you remove one corner piece?
3. What if you remove two opposite corner pieces?

Answers.

1. **Yes!** Do it in the naive way.
2. **No!** Dominoes can only tile an even number of squares.

Puzzle

Dominoes are 2×1 shapes. Given an 8×8 board:

1. Can you tile it with dominoes?
2. What if you remove one corner piece?
3. What if you remove two opposite corner pieces?

Answers.

1. **Yes!** Do it in the naive way.
2. **No!** Dominoes can only tile an even number of squares.
3. **No**, but a little more creative.

Three puzzles: guess the invariant!

Puzzle

Dominoes are 2×1 shapes. Given an 8×8 board:

1. Can you tile it with dominoes?
2. What if you remove one corner piece?
3. What if you remove two opposite corner pieces?

Answers.

1. **Yes!** Do it in the naive way.
2. **No!** Dominoes can only tile an even number of squares.
3. **No**, but a little more creative. Imagine the board is a chess board:
   - Any domino must cover a white square and a black square.
   - Thus any tiling covers the same number of black and white squares.
   - However, two opposite corner squares have the same colour, so tiling by dominoes is *impossible*. □

Three puzzles: guess the invariant!

Puzzle

Dominoes are 2×1 shapes. Given an 8×8 board:

1. Can you tile it with dominoes?
2. What if you remove one corner piece?
3. What if you remove two opposite corner pieces?

Answers.

1. **Yes!** Do it in the naive way.
2. **No!** Dominoes can only tile an even number of squares.
3. **No**, but a little more creative. Imagine the board is a chess board:
   - Any domino must cover a white square and a black square.
   - Thus any tiling covers the same number of black and white squares.
   - However, two opposite corner squares have the same colour, so tiling by dominoes is *impossible*. □

NB: If you want more of these, come speak to me!

Outline

Deduction and duality

Deduction and duality

Gentzen's systems deviate in two fundamental ways from Hilbert-Frege systems.

Both are inspired by the utility of the deduction theorem for theorem proving.

Deduction and duality

Gentzen's systems deviate in two fundamental ways from Hilbert-Frege systems.
Both are inspired by the utility of the deduction theorem for theorem proving.

Rules instead of axioms

Gentzen favoured a rule-based system over an axiom-based system.

Deduction and duality

Gentzen's systems deviate in two fundamental ways from Hilbert-Frege systems.

Both are inspired by the utility of the deduction theorem for theorem proving.

Rules instead of axioms

Gentzen favoured a rule-based system over an axiom-based system. E.g.:

$$(A \wedge B) \to A \quad \rightsquigarrow \quad \frac{A \wedge B}{A}$$

Deduction and duality

Gentzen's systems deviate in two fundamental ways from Hilbert-Frege systems.

Both are inspired by the utility of the deduction theorem for theorem proving.

Rules instead of axioms

Gentzen favoured a rule-based system over an axiom-based system. E.g.:

$$(A \wedge B) \rightarrow A \quad \rightsquigarrow \quad \frac{A \wedge B}{A}$$

Bringing duality to the forefront

Duality is at the heart of proof theory; we should combine this with deduction.

Deduction and duality

Gentzen's systems deviate in two fundamental ways from Hilbert-Frege systems.

Both are inspired by the utility of the deduction theorem for theorem proving.

Rules instead of axioms

Gentzen favoured a rule-based system over an axiom-based system. E.g.:

$$(A \wedge B) \rightarrow A \quad \rightsquigarrow \quad \frac{A \wedge B}{A}$$

Bringing duality to the forefront

Duality is at the heart of proof theory; we should combine this with deduction.

Recall the following notation:

$\Gamma \vdash A$: "all the formulas of Γ imply A"

Deduction and duality

Gentzen's systems deviate in two fundamental ways from Hilbert-Frege systems.

Both are inspired by the utility of the deduction theorem for theorem proving.

RULES INSTEAD OF AXIOMS

Gentzen favoured a rule-based system over an axiom-based system. E.g.:

$$(A \wedge B) \to A \quad \rightsquigarrow \quad \frac{A \wedge B}{A}$$

BRINGING DUALITY TO THE FOREFRONT

Duality is at the heart of proof theory; we should combine this with deduction.

Recall the following notation:

$\Gamma \vdash A$: "all the formulas of Γ imply A"

Gentzen's insight was to dualise this notion:

$\Gamma \vdash \Delta$: "all the formulae of Γ imply some of the formulae of Δ"

Sequents

The desire of “fully dualised” systems motivates the following notion:

list without order
set with multiple occurrences

Definition (Sequents)

A **sequent** is an expression $\Gamma \vdash \Delta$, where Γ and Δ are multisets of formulae.

The desire of "fully dualised" systems motivates the following notion:

Definition (Sequents)

A **sequent** is an expression $\Gamma \vdash \Delta$, where Γ and Δ are multisets of formulae.

NB: A multiset is just like a list, but we do not care about the order. In other settings, Γ and Δ may be *lists* or *sets* rather than multisets.

The desire of "fully dualised" systems motivates the following notion:

Definition (Sequents)

A **sequent** is an expression $\Gamma \vdash \Delta$, where Γ and Δ are multisets of formulae.

NB: A multiset is just like a list, but we do not care about the order. In other settings, Γ and Δ may be *lists* or *sets* rather than multisets.

We write sequents as $A_1, \ldots, A_m \vdash B_1, \ldots, B_n$, and interpret them as:

$$\bigwedge_{i=1}^{m} A_i \vdash \bigvee_{j=1}^{n} B_j$$

The desire of "fully dualised" systems motivates the following notion:

Definition (Sequents)

A **sequent** is an expression $\Gamma \vdash \Delta$, where Γ and Δ are multisets of formulae.

NB: A multiset is just like a list, but we do not care about the order. In other settings, Γ and Δ may be *lists* or *sets* rather than multisets.

We write sequents as $A_1, \ldots, A_m \vdash B_1, \ldots, B_n$, and interpret them as:

$$\bigwedge_{i=1}^{m} A_i \vdash \bigvee_{j=1}^{n} B_j$$

When Γ is empty, we identify it with $\top$. When Δ is empty we identify it with $\bot$. So:

- $\Gamma \vdash$ means "Γ is inconsistent".
- $\vdash \Delta$ means "some formula in Δ is true".

A calculus for metatheory

A calculus for metatheory

The notion of deduction made it easier to reason about proofs and provability.

A calculus for metatheory

The notion of deduction made it easier to reason about proofs and provability.

Gentzen used sequents as a way of studying the metatheory of proof systems.

The notion of deduction made it easier to reason about proofs and provability.

Gentzen used sequents as a way of studying the metatheory of proof systems.

Gentzen proposed a system called LK, which notably enjoys the following completeness property:

Theorem (Subformula property, Gentzen '34)

If A is valid, it has an LK *proof containing only subformulae of A (up to substitution of terms for free variables).*

Outline

Initial and structural rules

Initial and structural rules

$$\text{id}\,\frac{}{A \vdash A} \qquad \textit{w-l}\,\frac{\Gamma \vdash \Delta}{\Gamma, A \vdash \Delta} \qquad \textit{w-r}\,\frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, A} \qquad \textit{c-l}\,\frac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta} \qquad \textit{c-r}\,\frac{\Gamma \vdash \Delta, A, A}{\Gamma \vdash \Delta, A}$$

Initial and structural rules

"$\Gamma \vdash \Delta$" : "$\bigwedge \Gamma \to \bigvee \Delta$"
$\Rightarrow \bigwedge \Gamma \to \bigvee \Delta \vee A$

$\Gamma, A := \Gamma \cup \{A\}$

$$\text{id}\ \frac{}{A \vdash A} \qquad w\text{-}l\ \frac{\Gamma \vdash \Delta}{\Gamma, A \vdash \Delta} \qquad w\text{-}r\ \frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, A} \qquad c\text{-}l\ \frac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta} \qquad c\text{-}r\ \frac{\Gamma \vdash \Delta, A, A}{\Gamma \vdash \Delta, A}$$

$A \vee A \Downarrow A$

- (**Identity**, id) corresponds to the axiom $A \to A$ we derived in Lecture 1.
- (**Weakening**, w) corresponds to a relaxation of any deduction:

$$\textit{if } \Gamma \vdash B \textit{ then also } \Gamma, A \vdash B$$

The right version is just the dual version.

$\Gamma \vdash B$
$\Gamma, A \vdash B$

$\Gamma \quad \neg A$

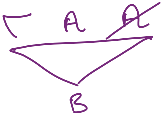
- (**Contraction**, c) corresponds to the tautologies:

$$A \to (A \wedge A) \qquad \text{and} \qquad (A \vee A) \to A$$

Alternatively: if I already have A as a hypothesis, I do not need two copies of it!

w-l: $A \wedge B \to A$

w-r: $A \to A \vee B$



(Blank slide)

Propositional connectives

We only present the rules for $\rightarrow$ and $\bot$, since that was our basis for $\mathcal{F}$.

We only present the rules for $\rightarrow$ and $\bot$, since that was our basis for $\mathcal{F}$.

There is only one rule for $\bot$:

$$\bot\text{-}l \; \frac{}{\bot \vdash} \qquad \left(\textit{optional} : \; \bot\text{-}r \; \frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, \bot} \right)$$

This is *ex falso quod libet*, that we proved before: $\bot \rightarrow A$ is valid for any formula A.
This is simulated by the rule above and *w-r*.

We only present the rules for $\to$ and $\bot$, since that was our basis for $\mathcal{F}$.

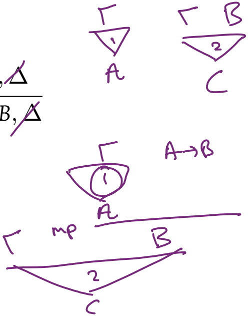
There is only one rule for $\bot$:

$$\bot\text{-}l\ \frac{}{\bot \vdash} \qquad \left(\mathit{optional}:\ \bot\text{-}r\ \frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, \bot} \right)$$

This is *ex falso quod libet*, that we proved before: $\bot \to A$ is valid for any formula A. This is simulated by the rule above and *w-r*.

We have two symmetric rules for implication:

$$\to\text{-}l\ \frac{\Gamma \vdash \Delta, A \quad B, \Gamma \vdash \Delta}{\Gamma, A \to B \vdash \Delta} \qquad \to\text{-}r\ \frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \to B, \Delta}$$



Propositional connectives

We only present the rules for $\to$ and $\bot$, since that was our basis for $\mathcal{F}$.

There is only one rule for $\bot$:

$$\bot\text{-}l \, \frac{}{\bot \vdash} \qquad \left(\textit{optional} : \; \bot\text{-}r \, \frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, \bot} \right)$$

This is *ex falso quod libet*, that we proved before: $\bot \to A$ is valid for any formula A.
This is simulated by the rule above and *w-r*.

We have two symmetric rules for implication:

$$\to\text{-}l \, \frac{\Gamma \vdash \Delta, A \quad B, \Gamma \vdash \Delta}{\Gamma, A \to B \vdash \Delta} \qquad \to\text{-}r \, \frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \to B, \Delta}$$

- The *left* rule allows us to 'compose' derivations.
- The *right* rule is just a generalisation of the deduction theorem.

(Blank slide)

Quantifier rules

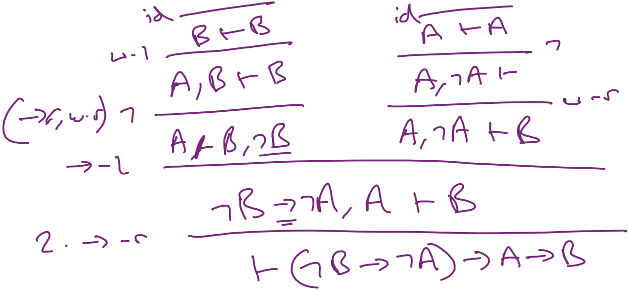
Importantly, LK has the following rules for the quantifiers:

$$\forall\text{-}l\ \frac{\Gamma, A[t/x] \vdash \Delta}{\Gamma, \forall x.A \vdash \Delta} \qquad \forall\text{-}r\ \frac{\Gamma \vdash \Delta, A[y/x]}{\Gamma \vdash \Delta, \forall x.A}\ y \notin \mathsf{FV}(\Gamma, \Delta, A)$$

$$\exists\text{-}r\ \frac{\Gamma \vdash \Delta, A[t/x]}{\Gamma \vdash \Delta, \exists x.A} \qquad \exists\text{-}l\ \frac{\Gamma, A[y/x] \vdash \Delta}{\Gamma, \exists x.A \vdash \Delta}\ y \notin \mathsf{FV}(\Gamma, \Delta, A)$$

- In $\exists$-l and $\forall$-r the variable x may not occur free in Γ, Δ.
- Notice the duality between $\exists$ and $\forall$ here.

Outline


id
B ⊢ B
w-l
A, B ⊢ B
(→r, w-r) ¬
A ⊢ B, ¬B
id
A ⊢ A
¬
A, ¬A ⊢
w-r
A, ¬A ⊢ B
→-l
¬B → ¬A, A ⊢ B
2. →-r
⊢ (¬B → ¬A) → A → B

Contraposition

$$
{\scriptstyle \to\text{-}r}\;\dfrac{
{\scriptstyle \to\text{-}r}\;\dfrac{
{\scriptstyle \to\text{-}l}\;\dfrac{
{\scriptstyle \to\text{-}r}\;\dfrac{{\scriptstyle w}\;\dfrac{{\scriptstyle \text{id}}\;\dfrac{}{B \vdash B}}{A, B \vdash B}}{A \vdash B, \neg B}
\qquad
{\scriptstyle \to\text{-}l}\;\dfrac{{\scriptstyle w}\;\dfrac{{\scriptstyle \text{id}}\;\dfrac{}{A \vdash A}}{A \vdash A, B} \quad {\scriptstyle w}\;\dfrac{{\scriptstyle \bot\text{-}l}\;\dfrac{}{\bot \vdash}}{\bot \vdash B}}{A, \neg A \vdash B}
}{\neg B \to \neg A, A \vdash B}
}{\neg B \to \neg A \vdash A \to B}
}{\vdash (\neg B \to \neg A) \to A \to B}
$$

Pierce's law

$$\dfrac{\dfrac{\dfrac{\overline{A \vdash A}}{A \vdash A, B}\ w}{\vdash A, A \to B} \qquad \overline{A \vdash A}}{(A \to B) \to A \vdash A}\ \to l$$

$$\dfrac{(A \to B) \to A \vdash A}{\vdash ((A \to B) \to A) \to A}\ \to r$$

Pierce's law

$$\to\text{-}r\;\dfrac{\to\text{-}l\;\dfrac{\to\text{-}r\;\dfrac{w\;\dfrac{\mathsf{id}\;\dfrac{}{A \vdash A}}{A \vdash A, B}}{\vdash A, A \to B} \qquad \mathsf{id}\;\dfrac{}{A \vdash A}}{(A \to B) \to A \vdash A}}{\vdash ((A \to B) \to A) \to A}$$

Drinker's paradox

Drinker's paradox

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{D(v) \vdash D(v)}\,\textsf{id}}{D(u), D(v) \vdash D(v), \forall y.D(y)}\,w}{D(u) \vdash D(v), D(v) \to \forall y.D(y)}\,{\to}\text{-}r}{D(u) \vdash D(v), \exists x.(D(x) \to \forall y.D(y))}\,\exists\text{-}r}{D(u) \vdash \forall x.D(x), \exists x.(D(x) \to \forall y.D(y))}\,\forall\text{-}r}{\vdash D(u) \to \forall y.D(y), \exists x.(D(x) \to \forall y.D(y))}\,{\to}\text{-}r}{\vdash \exists x.(D(x) \to \forall y.D(y)), \exists x.(D(x) \to \forall y.D(y))}\,\exists\text{-}r}{\vdash \exists x.(D(x) \to \forall y.D(y))}\,c
$$

Outline

The cut

Until now, every rule we have seen satisfies the subformula property: only subformulae of the conclusion appear in premisses (up to substitution).

The cut

Until now, every rule we have seen satisfies the subformula property: only subformulae of the conclusion appear in premisses (up to substitution).

There is one crucial exception:

$$\textit{cut}\ \frac{\Gamma \vdash \Delta, A \qquad A, \Gamma' \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}$$

(This concludes the definition of LK.)

The cut

Until now, every rule we have seen satisfies the subformula property: only subformulae of the conclusion appear in premisses (up to substitution).

There is one crucial exception:

$$\text{cut}\ \frac{\Gamma \vdash \Delta, A \quad A, \Gamma' \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}$$

(This concludes the definition of LK.)

Notice that A here, the cut-formula, had to be guessed.

This is very similar to the situation for *modus ponens* and, indeed, allows us to easily simulate $\mathcal{F}$ proofs, or prove completeness at all…

Soundness and completeness of LK

Soundness and completeness of LK

1. LK is sound by structural induction as before for $\mathcal{F}$.

Soundness and completeness of LK

1. LK is sound by structural induction as before for $\mathcal{F}$.
2. LK is complete since it can simulate $\mathcal{F}$ proofs:

Theorem

If in $\mathcal{F}$ the formula A is derivable from hypotheses Γ, then there is an LK proof of $\Gamma \vdash A$.

Soundness and completeness of LK

1. LK is sound by structural induction as before for $\mathcal{F}$.
2. LK is complete since it can simulate $\mathcal{F}$ proofs:

Theorem
If in $\mathcal{F}$ the formula A is derivable from hypotheses Γ, then there is an LK proof of $\Gamma \vdash A$.

Proof idea.
By structural induction on a $\mathcal{F}$ proof.

1. LK is sound by structural induction as before for $\mathcal{F}$.
2. LK is complete since it can simulate $\mathcal{F}$ proofs:

Theorem

If in $\mathcal{F}$ the formula A is derivable from hypotheses Γ, then there is an LK *proof of* $\Gamma \vdash A$.

Proof idea.

By structural induction on a $\mathcal{F}$ proof. The base cases consist of deriving the axioms in LK,

1. LK is sound by structural induction as before for $\mathcal{F}$.
2. LK is complete since it can simulate $\mathcal{F}$ proofs:

Theorem

If in $\mathcal{F}$ the formula A is derivable from hypotheses Γ, then there is an LK proof of $\Gamma \vdash A$.

Proof idea.

By structural induction on a $\mathcal{F}$ proof. The base cases consist of deriving the axioms in LK, the interesting cases are simulating *generalisation* and *modus ponens*.

1. LK is sound by structural induction as before for $\mathcal{F}$.
2. LK is complete since it can simulate $\mathcal{F}$ proofs:

Theorem

If in $\mathcal{F}$ the formula A is derivable from hypotheses Γ, then there is an LK *proof of* $\Gamma \vdash A$.

Proof idea.

By structural induction on a $\mathcal{F}$ proof. The base cases consist of deriving the axioms in LK, the interesting cases are simulating *generalisation* and *modus ponens*. E.g.:

$$
(mp)\,\frac{A \quad A \to B}{B} \quad \rightsquigarrow \quad
cut\,\dfrac{\Gamma \vdash A \qquad cut\,\dfrac{\Gamma \vdash A \to B \qquad \to\text{-}l\,\dfrac{\text{id}\,\dfrac{}{A \vdash A} \qquad \text{id}\,\dfrac{}{B \vdash B}}{A, A \to B \vdash B}}{\Gamma, A \vdash B}}{\Gamma \vdash B}
$$

□

Soundness and completeness of LK

1. LK is sound by structural induction as before for $\mathcal{F}$.
2. LK is complete since it can simulate $\mathcal{F}$ proofs:

Theorem

If in $\mathcal{F}$ the formula A is derivable from hypotheses Γ, then there is an LK *proof of* $\Gamma \vdash A$.

Proof idea.

By structural induction on a $\mathcal{F}$ proof. The base cases consist of deriving the axioms in LK, the interesting cases are simulating *generalisation* and *modus ponens*. E.g.:

$$(mp)\,\frac{A \quad A \to B}{B} \quad \rightsquigarrow \quad \mathit{cut}\,\dfrac{\Gamma \vdash A \qquad \mathit{cut}\,\dfrac{\Gamma \vdash A \to B \qquad \to\text{-}l\,\dfrac{\mathsf{id}\,\dfrac{}{A \vdash A} \qquad \mathsf{id}\,\dfrac{}{B \vdash B}}{A, A \to B \vdash B}}{\Gamma, A \vdash B}}{\Gamma \vdash B}$$

□

NB: (1) may also be proved by simulation, but a little harder!

The *Hauptsatz*

Theorem (*Hauptsatz*, Gentzen '34)

Every theorem of LK *has a proof that does not use the cut rule.*

Theorem (*Hauptsatz*, Gentzen ’34)

Every theorem of LK *has a proof that does not use the cut rule.*

Corollary (Subformula property)

Every theorem of LK *has a proof that contains only subformulae of it, up to substitution of terms for variables.*

Outline

Cut-elimination is arguably one the most important results in all of logic.

Perspectives

Cut-elimination is arguably one the most important results in all of logic.

Its applications are numerous:

- Conservativity results. (mathematical logic)
- Automating proof search. (logic programming)
- Cut-elimination as a computational process. (*Curry-Howard* correspondence)
- Metalogical results. (structural proof theory)

Perspectives

Cut-elimination is arguably one the most important results in all of logic.

Its applications are numerous:

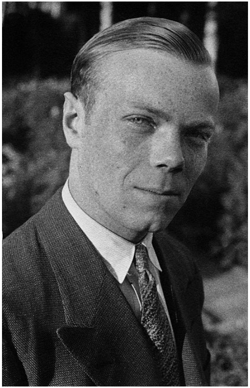
- Conservativity results. (mathematical logic)
- Automating proof search. (logic programming)
- Cut-elimination as a computational process. (*Curry-Howard* correspondence)
- Metalogical results. (structural proof theory)

As my old supervisor used to say: "*there is no such thing as a free lunch*".

Theorem (Statman '79, Orevkov '82)

Cut-elimination necessarily has a non-elementary cost in proof size.

Herbrand's theorem



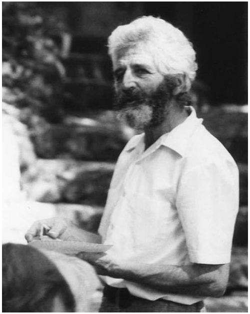
Theorem (Herbrand)

If $\models \exists x.A(x)$, *for A quantifier-free, then there is a finite set* $\{t_i\}_{i=1}^{n}$ *s.t.* $\models A(t_1) \vee \cdots \vee A(t_n)$.

Simple example: even numbers exist (blank slide)

Informal example: $\exists a, b \notin \mathbb{Q}. a^b \in \mathbb{Q}$ (blank slide)

Craig interpolation



Theorem (Craig Interpolation)

If $\vDash A \rightarrow B$*, there is some* I *in the common language of* A *and* B *s.t.* $\vDash A \rightarrow I$ *and* $\vDash I \rightarrow B$*.*

Example: disjoint **NP**-pairs (blank slide)

Outline

A remarkable observation

Gentzen noticed a startling fact:

Observation

Let LJ *be the restriction of* LK *where all sequents have exactly one formula on the RHS.*

A remarkable observation

Gentzen noticed a startling fact:

Observation

Let LJ *be the restriction of* LK *where all sequents have exactly one formula on the RHS.*
LJ *is sound and complete for intuitionistic logic.*

A remarkable observation

Gentzen noticed a startling fact:

Observation

Let LJ *be the restriction of* LK *where all sequents have exactly one formula on the RHS.*
LJ *is sound and complete for intuitionistic logic.*

Moreover, cut-elimination still holds!

A remarkable observation

Gentzen noticed a startling fact:

Observation

Let LJ *be the restriction of* LK *where all sequents have exactly one formula on the RHS.*
LJ *is sound and complete for intuitionistic logic.*

Moreover, cut-elimination still holds!

Corollary

We have the following immediate consequences:

- *Intuitionistic propositional logic is decidable (even* **PSPACE***-complete).*
- *Intuitionistic logic enjoys the disjunction and existential properties:*

$$\begin{array}{lcl} \vdash_{\mathsf{LJ}} A \vee B & \Longrightarrow & \vdash_{\mathsf{LJ}} A \text{ or } \vdash_{\mathsf{LJ}} B \\ \vdash_{\mathsf{LJ}} \exists x A & \Longrightarrow & \vdash_{\mathsf{LJ}} A[t/x] \text{ for some term } t \end{array}$$

- *Craig interpolation still holds for intuitionistic logic.*

Example: Peirce's law is not intuitionistically valid (blank slide)

Outline

The system LK

INITIAL AND STRUCTURAL RULES

$$\text{id}\,\frac{}{A \vdash A} \qquad w\text{-}l\,\frac{\Gamma \vdash \Delta}{A, \Gamma \vdash \Delta} \qquad w\text{-}r\,\frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, A} \qquad c\text{-}l\,\frac{A, A, \Gamma \vdash \Delta}{A, \Gamma \vdash \Delta} \qquad c\text{-}r\,\frac{\Gamma \vdash \Delta, A, A}{\Gamma \vdash \Delta, A}$$

PROPOSITIONAL RULES:

$$\bot\text{-}l\,\frac{}{\bot \vdash} \qquad \left(\bot\text{-}r\,\frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, \bot}\right) \qquad \to\text{-}l\,\frac{\Gamma \vdash \Delta, A \quad B, \Gamma \vdash \Delta}{\Gamma, A \to B \vdash \Delta} \qquad \to\text{-}r\,\frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \to B, \Delta}$$

QUANTIFIER RULES:

$$\forall\text{-}l\,\frac{\Gamma, A[t/x] \vdash \Delta}{\Gamma, \forall x.A \vdash \Delta} \qquad \forall\text{-}r\,\frac{\Gamma \vdash \Delta, A[y/x]}{\Gamma \vdash \Delta, \forall x.A} \qquad \exists\text{-}r\,\frac{\Gamma \vdash \Delta, A[t/x]}{\Gamma \vdash \Delta, \exists x.A} \qquad \exists\text{-}l\,\frac{\Gamma, A[y/x] \vdash \Delta}{\Gamma, \exists x.A \vdash \Delta}$$

where $y \notin \mathsf{FV}(\Gamma, \Delta, A)$.

CUT RULE:

$$cut\,\frac{\Gamma \vdash \Delta, A \quad A, \Gamma' \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}$$

1. We saw that modus ponens could be simulated in LK. Give cut-free LK proofs for each of the three propositional axioms of $\mathcal{F}$:

$$\begin{array}{rl} (wk) & A \to (B \to A) \\ (dist) & (A \to (B \to C)) \to ((A \to B) \to (A \to C)) \\ (neg) & ((A \to \bot) \to \bot) \to A \end{array}$$

2. What about the quantifier axioms and rule:

$$gen\ \frac{A}{\forall x A} \qquad \begin{array}{l} \forall x.A \to A[t/x] \\ \forall x.(A \to B) \to (A \to \forall x.B) \quad \text{as long as } x \notin \mathsf{FV}(A) \end{array}$$

   (**NB:** this concludes the proof of completeness of LK).

3. What possible rules might we need if we had $\vee$ and $\wedge$ in our language?

4. (**Puzzle**). There are 100 ants on a 1m stick, facing either end of the stick. They start moving at 1m/s and, every time they collide, they perfectly rebound. How long does it take for all the ants to fall off the stick (in the worst case)?

5. (**Still hard**). Revisiting Exercise 4 (Propositional logic) from Lecture 1: can you now show that Peirce's law, $((A \to B) \to A) \to A$, is not intuitionistically valid?

   Hint: use completeness of cut-free proof search in LJ for intuitionistic logic.

Outline

References I

Buss, S. R., editor (1998).
Handbook of Proof Theory, volume 137 of *Studies in Logic and the Foundations of Mathematics*.
Elsevier.

Negri, S. and von Plato, J. (2001).
Structural proof theory.
Cambridge University Press.

Szabo, M. E. (1972).
The Collected Papers of Gerhard Gentzen.
Philosophy of Science, 39(1):91–91.

Troelstra, A. S. and Schwichtenberg, H. (1996).
Basic Proof Theory.
Cambridge University Press, New York, NY, USA.