Introduction to Proof Theory

Lectures 3 & 4 - The sequent calculus and analyticity

Anupam Das

University of Copenhagen

Logic Summer School

Australian National University

6th December 2018

These slides are available at `http://www.anupamdas.com/wp/lss18/`.

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)
- …

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)
- ...

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*:

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

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

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*:

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

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.

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"*

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.

NB: this is a subject of intense debate!

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.

NB: this is a subject of intense debate!

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 a 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?

Three puzzles: guess the invariant!

Puzzle

Dominoes are 2×1 shapes. Given a 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 a 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.

Three puzzles: guess the invariant!

Puzzle

Dominoes are 2×1 shapes. Given a 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 a 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*. □

Puzzle

Dominoes are 2×1 shapes. Given a 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

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.

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.:

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

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.

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:

Definition (Sequents)

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

Sequents

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.

Sequents

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:

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

Sequents

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:

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

Similarly to deduction, when Γ is empty, we identify it with $\top$, and when Δ is empty we identify it with $\bot$ (remember Lecture 1!).

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:

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

Similarly to deduction, when Γ is empty, we identify it with $\top$, and when Δ is empty we identify it with $\bot$ (remember Lecture 1!). 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 free variables for terms).*

Outline

Initial and structural rules

Gentzen's system for first-order logic is called LK.

Let us see what his rules look like, and how we might justify them.

Initial and structural rules

Gentzen's system for first-order logic is called LK.

Let us see what his rules look like, and how we might justify them.

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

Initial and structural rules

Gentzen's system for first-order logic is called LK.

Let us see what his rules look like, and how we might justify them.

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

- (**Identity**, id) corresponds to the axiom $A \to A$ we derived in Lecture 1.

Initial and structural rules

Gentzen's system for first-order logic is called LK.

Let us see what his rules look like, and how we might justify them.

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

- (**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.

Initial and structural rules

Gentzen's system for first-order logic is called LK.

Let us see what his rules look like, and how we might justify them.

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

- (**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.
- (**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!

Propositional connectives

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

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 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:

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

Propositional connectives

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 have two symmetric rules for implication:

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

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

Quantifier rules

Quantifier rules

Importantly, LK has the following rules for the quantifiers:

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

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. (Remember Lecture 3!)
- Notice the duality between $\exists$ and $\forall$ here.

The cut

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

The cut

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

There is one crucial exception:

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

The cut

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

There is one crucial exception:

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

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…

Equivalence of LK and $\mathcal{F}$

Equivalence of LK and $\mathcal{F}$

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

Equivalence of LK and $\mathcal{F}$

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 $\Gamma \vdash A$.

Equivalence of LK and $\mathcal{F}$

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 case is in simulating *modus ponens*:

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

□

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 case is in simulating *modus ponens*:

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

□

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

Outline

Structural proof theory

Structural proof theory *is the study of normal forms and normalisation*

Structural proof theory

Structural proof theory *is the study of normal forms and normalisation*

Gentzen was the founder of structural proof theory, and his *Hauptsatz* was far beyond his time.

Not only does it yield our much sought after analytic system, it is one of the most powerful tools in all of logic

Structural proof theory

Structural proof theory *is the study of normal forms and normalisation*

Gentzen was the founder of structural proof theory, and his *Hauptsatz* was far beyond his time.

Not only does it yield our much sought after analytic system, it is one of the most powerful tools in all of logic

"cut-elimination is the most beautiful result with the most horrible proof"

Structural proof theory

Structural proof theory *is the study of normal forms and normalisation*

Gentzen was the founder of structural proof theory, and his *Hauptsatz* was far beyond his time.

Not only does it yield our much sought after analytic system, it is one of the most powerful tools in all of logic

"cut-elimination is the most beautiful result with the most horrible proof"

This is one of the hardest termination arguments in graduate mathematics and computer science!

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 variables for terms.*

How cut-elimination works

How cut-elimination works

Basic idea, in a nutshell

"push" the cuts ***upwards*** *in a proof, until they disappear completely!*

How cut-elimination works

Basic idea, in a nutshell

*"push" the cuts **upwards** in a proof, until they disappear completely!*

I will cover the main ideas behind the argument, but understanding comes through practice! I recommend standard references for detailed proofs:

- [Buss, 1998]. *Handbook of Proof Theory*.
- [Troelstra and Schwichtenberg, 1996]. *Basic Proof Theory*.
- [Negri and von Plato, 2001]. *Structural Proof Theory*.

How cut-elimination works

Basic idea, in a nutshell

*"push" the cuts **upwards** in a proof, until they disappear completely!*

I will cover the main ideas behind the argument, but understanding comes through practice! I recommend standard references for detailed proofs:

- [Buss, 1998]. *Handbook of Proof Theory*.
- [Troelstra and Schwichtenberg, 1996]. *Basic Proof Theory*.
- [Negri and von Plato, 2001]. *Structural Proof Theory*.
- [Szabo, 1972]. *The Collected Papers of Gerhard Gentzen*.

How cut-elimination works

Basic idea, in a nutshell

*"push" the cuts **upwards** in a proof, until they disappear completely!*

I will cover the main ideas behind the argument, but understanding comes through practice! I recommend standard references for detailed proofs:

- [Buss, 1998]. *Handbook of Proof Theory*.
- [Troelstra and Schwichtenberg, 1996]. *Basic Proof Theory*.
- [Negri and von Plato, 2001]. *Structural Proof Theory*.
- [Szabo, 1972]. *The Collected Papers of Gerhard Gentzen*.
- Or do it *yourself*!

Basic idea, in a nutshell

*"push" the cuts **upwards** in a proof, until they disappear completely!*

I will cover the main ideas behind the argument, but understanding comes through practice! I recommend standard references for detailed proofs:

- [Buss, 1998]. *Handbook of Proof Theory*.
- [Troelstra and Schwichtenberg, 1996]. *Basic Proof Theory*.
- [Negri and von Plato, 2001]. *Structural Proof Theory*.
- [Szabo, 1972]. *The Collected Papers of Gerhard Gentzen*.
- Or do it *yourself*!

Let us at least see some of the key ideas…

Key propositional case

Key propositional case

$$
\dfrac{
\rightarrow\text{-}r\ \dfrac{\overset{1}{\nabla}\quad \Gamma, A \vdash \Delta, B}{\Gamma \vdash \Delta, A \rightarrow B}
\qquad
\rightarrow\text{-}l\ \dfrac{\overset{2}{\nabla}\quad \Gamma' \vdash \Delta', A \qquad \overset{3}{\nabla}\quad \Gamma', B \vdash \Delta'}{\Gamma', A \rightarrow B \vdash \Delta'}
}{
\Gamma, \Gamma' \vdash \Delta, \Delta'
}\ \mathit{cut}
$$

Key propositional case

$$
\dfrac{
  \dfrac{\overset{1}{\vdots}\\ \Gamma, A \vdash \Delta, B}{\Gamma \vdash \Delta, A \to B}\;{\to}\text{-}r
  \qquad
  \dfrac{\overset{2}{\vdots}\\ \Gamma' \vdash \Delta', A \quad \overset{3}{\vdots}\\ \Gamma', B \vdash \Delta'}{\Gamma', A \to B \vdash \Delta'}\;{\to}\text{-}l
}{\Gamma, \Gamma' \vdash \Delta, \Delta'}\;\mathit{cut}
$$

$$
\rightsquigarrow \quad
\dfrac{
  \dfrac{
    \dfrac{\overset{2}{\vdots}\ \Gamma' \vdash \Delta', A \quad \overset{1}{\vdots}\ \Gamma, A \vdash \Delta, B}{\Gamma, \Gamma' \vdash \Delta, \Delta', B}\;\mathit{cut}
    \qquad
    \overset{3}{\vdots}\ \Gamma', B \vdash \Delta'
  }{\Gamma, \Gamma', \Gamma' \vdash \Delta, \Delta', \Delta'}\;\mathit{cut}
}{\Gamma, \Gamma' \vdash \Delta, \Delta'}\;c
$$

Key quantifier case

Key quantifier case

$$
\dfrac{\exists\text{-}r\ \dfrac{\overset{1}{\bigtriangledown}\\ \Gamma \vdash \Delta, A(t)}{\Gamma \vdash \Delta, \exists x.A(x)} \qquad \exists\text{-}l\ \dfrac{\overset{2(x)}{\bigtriangledown}\\ \Gamma', A(x) \vdash \Delta'}{\Gamma', \exists x.A(x) \vdash \Delta'}}{\Gamma, \Gamma' \vdash \Delta, \Delta'}\ \mathit{cut}
$$

Key quantifier case

$$\dfrac{\dfrac{\overset{1}{\Gamma \vdash \Delta, A(t)}}{\Gamma \vdash \Delta, \exists x.A(x)}\,\exists\text{-}r \qquad \dfrac{\overset{2(x)}{\Gamma', A(x) \vdash \Delta'}}{\Gamma', \exists x.A(x) \vdash \Delta'}\,\exists\text{-}l}{\Gamma, \Gamma' \vdash \Delta, \Delta'}\,\mathit{cut} \quad \rightsquigarrow \quad \dfrac{\overset{1}{\Gamma \vdash \Delta, A(t)} \qquad \overset{2(t)}{\Gamma', A(t) \vdash \Delta'}}{\Gamma, \Gamma' \vdash \Delta, \Delta'}\,\mathit{cut}$$

Key quantifier case

$$
\dfrac{\exists\text{-}r\;\dfrac{\overset{1}{\vdots}\\ \Gamma \vdash \Delta, A(t)}{\Gamma \vdash \Delta, \exists x.A(x)} \qquad \exists\text{-}l\;\dfrac{\overset{2(x)}{\vdots}\\ \Gamma', A(x) \vdash \Delta'}{\Gamma', \exists x.A(x) \vdash \Delta'}}{\Gamma, \Gamma' \vdash \Delta, \Delta'}\;\textit{cut}
\quad\rightsquigarrow\quad
\dfrac{\overset{1}{\vdots}\\ \Gamma \vdash \Delta, A(t) \qquad \overset{2(t)}{\vdots}\\ \Gamma', A(t) \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}\;\textit{cut}
$$

- Implicitly assume free variable conditions are respected.
- Write $2(t)$ for the derivation arising from $2(x)$ by replacing every free occurrence of x by t.

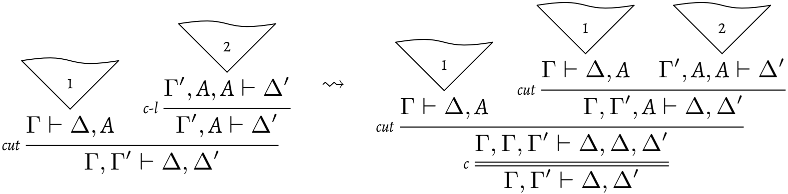
Termination

Termination

Proving that cut-elimination terminates is incredibly complex!

Proving that cut-elimination terminates is incredibly complex!

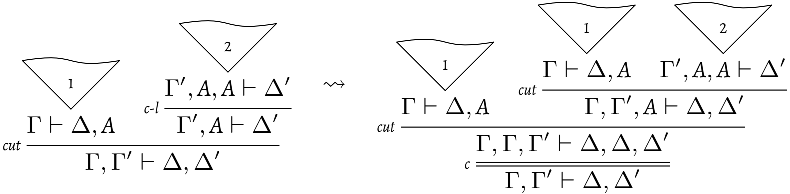
One particularly nasty issue is:



Termination

Proving that cut-elimination terminates is incredibly complex!

One particularly nasty issue is:



Here the entire subproof 1 is duplicated!

The need for ingenuity

Even worse, just blindly applying permutation rules will not work:

Even worse, just blindly applying permutation rules will not work:

$$
\dfrac{\dfrac{\overset{\triangledown\, 1}{\Gamma \vdash \Delta, A, A}}{\Gamma \vdash \Delta, A}\,\textit{c-r} \qquad \dfrac{\overset{\triangledown\, 2}{\Gamma', A, A \vdash \Delta'}}{\Gamma', A \vdash \Delta'}\,\textit{c-l}}{\Gamma, \Gamma' \vdash \Delta, \Delta'}\,\textit{cut}
\quad \rightsquigarrow \quad
\begin{array}{c}
\dfrac{\dfrac{\overset{\triangledown\, 1}{\Gamma \vdash \Delta, A, A} \qquad \overset{\triangledown\, 2}{\Gamma', A, A \vdash \Delta'}}{\Gamma, \Gamma', A \vdash \Delta, \Delta', A}\,\textit{cut}}{} \\
\vdots
\end{array}
$$

The sequent in red is trivial.

The need for ingenuity

Even worse, just blindly applying permutation rules will not work:

$$\dfrac{\dfrac{\overset{1}{\Gamma \vdash \Delta, A, A}}{\Gamma \vdash \Delta, A}\,\textit{c-r} \qquad \dfrac{\overset{2}{\Gamma', A, A \vdash \Delta'}}{\Gamma', A \vdash \Delta'}\,\textit{c-l}}{\Gamma, \Gamma' \vdash \Delta, \Delta'}\,\textit{cut} \quad \rightsquigarrow \quad \begin{array}{c} \dfrac{\overset{1}{\Gamma \vdash \Delta, A, A} \qquad \overset{2}{\Gamma', A, A \vdash \Delta'}}{\Gamma, \Gamma', A \vdash \Delta, \Delta', A}\,\textit{cut} \\ \vdots \end{array}$$

The sequent in red is trivial.

This is known as **Lafont's counterexample**, cf. *non-confluence* of cut-elimination.

Outline

The contraction-tree

Definition

The **contraction-tree** of a formula occurrence A in a proof π is the tree induced by the *c-l* and *c-r* steps in π on that formula occurrence.

Example

$$
\dfrac{\dfrac{\dfrac{\dfrac{\Gamma, A, A \vdash \Delta, B, B, B, B}{\Gamma, A, A \vdash \Delta, B, B, B}\,c\text{-}r}{\Gamma, A, A \vdash \Delta, B, B}\,c\text{-}r}{\Gamma, A \vdash \Delta, B, B}\,c\text{-}l}{\Gamma, A \vdash \Delta, B}\,c\text{-}r
$$

The contraction-tree

Definition

The **contraction-tree** of a formula occurrence A in a proof π is the tree induced by the *c-l* and *c-r* steps in π on that formula occurrence.

Example

$$\cfrac{\cfrac{\cfrac{\cfrac{\Gamma, A, A \vdash \Delta, B, B, B, B}{\Gamma, A, A \vdash \Delta, B, B, B}\;c\text{-}r}{\Gamma, A, A \vdash \Delta, B, B}\;c\text{-}r}{\Gamma, A \vdash \Delta, B, B}\;c\text{-}l}{\Gamma, A \vdash \Delta, B}\;c\text{-}r$$

The contraction-trees of A and B are marked in blue and red respectively.

The contraction-tree

Definition

The **contraction-tree** of a formula occurrence A in a proof π is the tree induced by the *c-l* and *c-r* steps in π on that formula occurrence.

Example

$$\dfrac{\dfrac{\dfrac{\dfrac{\Gamma, A, A \vdash \Delta, B, B, B, B}{\Gamma, A, A \vdash \Delta, B, B, B}\,c\text{-}r}{\Gamma, A, A \vdash \Delta, B, B}\,c\text{-}r}{\Gamma, A \vdash \Delta, B, B}\,c\text{-}l}{\Gamma, A \vdash \Delta, B}\,c\text{-}r$$

The contraction-trees of A and B are marked in blue and red respectively.

NB: In the contraction-tree, we only count occurrences of the same formula, not its subformulae.

A crucial lemma

Lemma

For any proof

$$\textit{cut}\ \dfrac{\overset{\pi}{\Gamma \vdash \Delta, A} \qquad \overset{\pi'}{\Gamma', A \vdash \Delta'}}{\Gamma, \Gamma' \vdash \Delta, \Delta'},$$

where the subproofs π and π' are cut-free, there is a proof of the end-sequent $\Gamma, \Gamma' \vdash \Delta, \Delta'$ with only cut-formulas of size $< |A|$.

A crucial lemma

Lemma

For any proof $\dfrac{\overset{\pi}{\Gamma \vdash \Delta, A} \quad \overset{\pi'}{\Gamma', A \vdash \Delta'}}{\Gamma, \Gamma' \vdash \Delta, \Delta'}\,\textit{cut}$, *where the subproofs* π *and* π' *are cut-free, there is a proof of the end-sequent* $\Gamma, \Gamma' \vdash \Delta, \Delta'$ *with only cut-formulas of size* $< |A|$.

Proof idea.

We show the strengthening that this is possible while furthermore preserving the size of contraction-trees from the end-sequent, by induction on:

$$(\text{size of } \pi') \times (\text{size of contraction-tree of } A \text{ in } \pi').$$

A crucial lemma

Lemma

For any proof

$$\dfrac{\overset{\pi}{\nabla}\atop{\Gamma \vdash \Delta, A} \qquad \overset{\pi'}{\nabla}\atop{\Gamma', A \vdash \Delta'}}{\Gamma, \Gamma' \vdash \Delta, \Delta'}\,\textit{cut}$$

, where the subproofs π and π' are cut-free, there is a proof of the end-sequent $\Gamma, \Gamma' \vdash \Delta, \Delta'$ with only cut-formulas of size $< |A|$.

Proof idea.

We show the strengthening that this is possible while furthermore preserving the size of contraction-trees from the end-sequent, by induction on:

$$(\text{size of } \pi') \times (\text{size of contraction-tree of } A \text{ in } \pi').$$

The main interesting case is when π' finishes with a *c-l* step:

$$\dfrac{\Gamma \vdash \Delta, A \qquad \dfrac{\Gamma', A, A \vdash \Delta'}{\Gamma', A \vdash \Delta'}\,\textit{c-l}}{\Gamma, \Gamma' \vdash \Delta, \Delta'}\,\textit{cut} \quad \rightsquigarrow \quad \dfrac{\dfrac{\Gamma \vdash \Delta, A \qquad \dfrac{\Gamma \vdash \Delta, A \qquad \Gamma', A, A \vdash \Delta'}{\Gamma, \Gamma', A \vdash \Delta, \Delta'}\,\textit{cut}}{\Gamma, \Gamma, \Gamma' \vdash \Delta, \Delta, \Delta'}\,\textit{cut}}{\Gamma, \Gamma' \vdash \Delta, \Delta'}\,c$$

□

An induction measure

An induction measure

Definition (Multiset measure)

For two multisets M, N of natural numbers, we say $M \prec N$ if I may transform N into M by the continually applying the following operation:

delete a number $n \in N$ *and insert any number of numbers* $< n$

Definition (Multiset measure)

For two multisets M, N of natural numbers, we say $M \prec N$ if I may transform N into M by the continually applying the following operation:

delete a number $n \in N$ and insert any number of numbers $< n$

Example

$\{1, 2, 3, 4, 4, 5\} \prec \{2, 5, 5\}$ and $\{1, 1, 2, 2, 2, 2\} \prec \{1, 2, 3\}$.

Definition (Multiset measure)

For two multisets M, N of natural numbers, we say $M \prec N$ if I may transform N into M by the continually applying the following operation:

$$\textit{delete a number } n \in N \textit{ and insert any number of numbers} < n$$

Example

$\{1, 2, 3, 4, 4, 5\} \prec \{2, 5, 5\}$ and $\{1, 1, 2, 2, 2, 2\} \prec \{1, 2, 3\}$.

NB: This can also be seen as a lexicographic order.

Definition (Multiset measure)

For two multisets M, N of natural numbers, we say $M \prec N$ if I may transform N into M by the continually applying the following operation:

delete a number $n \in N$ *and insert any number of numbers* $< n$

Example

$\{1,2,3,4,4,5\} \prec \{2,5,5\}$ and $\{1,1,2,2,2,2\} \prec \{1,2,3\}$.

NB: This can also be seen as a lexicographic order.

Proposition

$\prec$ *is a well-order on the class of multisets of natural numbers.*

Putting it all together

Definition (Degrees)

The **degree** of a proof is the multiset of sizes of its cut-formulae.

Putting it all together

Definition (Degrees)

The **degree** of a proof is the multiset of sizes of its cut-formulae.

Proof sketch of cut-elimination.

By induction on the degree of a proof, under $\prec$:

- Identify a topmost cut in a proof, and apply the crucial lemma.
- The degree of the resulting proof will be smaller, under $\prec$.
- Thus we may conclude by the inductive hypothesis. □

Definition (Degrees)

The **degree** of a proof is the multiset of sizes of its cut-formulae.

Proof sketch of cut-elimination.

By induction on the degree of a proof, under $\prec$:

- Identify a topmost cut in a proof, and apply the crucial lemma.
- The degree of the resulting proof will be smaller, under $\prec$.
- Thus we may conclude by the inductive hypothesis. $\square$

Exercise: Try work out explicitly the induction measure for yourself!

Outline

A cut-free proof of contraposition:

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

A cut-free proof of Pierce's law:

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

A cut-free proof of the Drinker's Paradox:

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

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

Outline

Perspectives

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)

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.

Perspectives

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

Its applications are numerous:

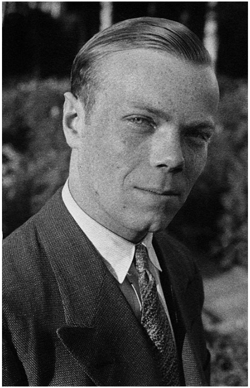
- Conservativity results. (mathematical logic)
- Automating proof search. (logic programming)
- Cut-elimination as a computational process. (*Curry-Howard* correspondence)
- Metalogical results. (structural proof theory)

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.

…and, of course, first-order logic remains undecidable.

Herbrand's theorem



Theorem (Herbrand's theorem)

If $\vDash \exists x.A(x)$ *then there is a finite set of terms* $\{t_i\}_{i=1}^{n}$ *s.t.* $\vDash A(t_1) \vee \cdots \vee A(t_n)$.

Proof idea of Herbrand's Theorem

The basic idea is that the terms in the Herbrand disjunction are just those from which the $\exists$ originates.

Proof idea of Herbrand's Theorem

The basic idea is that the terms in the Herbrand disjunction are just those from which the $\exists$ originates.

Formally, we can prove it by induction on the structure of a cut-free proof.

The basic idea is that the terms in the Herbrand disjunction are just those from which the $\exists$ originates.

Formally, we can prove it by induction on the structure of a cut-free proof.
The interesting cases are:

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

Proof idea of Herbrand's Theorem

The basic idea is that the terms in the Herbrand disjunction are just those from which the ∃ originates.

Formally, we can prove it by induction on the structure of a cut-free proof. The interesting cases are:

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

Exercise: Try to check how each of the other cases works for yourself!

Digression: recovering richer expressivity

Do we still have cut-free completeness for the richer language with $\vee$ and $\wedge$?

Digression: recovering richer expressivity

Do we still have cut-free completeness for the richer language with $\vee$ and $\wedge$? It turns out we can recover it directly from the current system!

Digression: recovering richer expressivity

Do we still have cut-free completeness for the richer language with $\vee$ and $\wedge$? It turns out we can recover it directly from the current system!

Definition

We say that a rule is **cut-free-invertible** if, whenever its conclusion is cut-free provable each of its premisses are too.

Do we still have cut-free completeness for the richer language with $\vee$ and $\wedge$? It turns out we can recover it directly from the current system!

Definition

We say that a rule is **cut-free-invertible** if, whenever its conclusion is cut-free provable each of its premisses are too.

Proposition

All of our propositional rules are cut-free-invertible.

Do we still have cut-free completeness for the richer language with $\vee$ and $\wedge$? It turns out we can recover it directly from the current system!

Definition

We say that a rule is **cut-free-invertible** if, whenever its conclusion is cut-free provable each of its premisses are too.

Proposition

All of our propositional rules are cut-free-invertible.

Proof idea.

By induction on the structure of the proof. Essentially we 'replace' each formula with its 'inverses'. □

Rules for $\vee$, $\wedge$ and an encoding in $\{\to, \bot\}$

Rules for $\vee$, $\wedge$ and an encoding in $\{\rightarrow, \bot\}$

Recall that we can encode $\vee$ and $\wedge$ in $\{\rightarrow, \bot\}$ by adequacy:

$$
\begin{aligned}
A \vee B &\equiv \neg A \rightarrow B \\
A \wedge B &\equiv \neg(A \rightarrow \neg B)
\end{aligned}
$$

Rules for $\vee$, $\wedge$ and an encoding in $\{\rightarrow, \bot\}$

Recall that we can encode $\vee$ and $\wedge$ in $\{\rightarrow, \bot\}$ by adequacy:

$$\begin{array}{lcl} A \vee B & \equiv & \neg A \rightarrow B \\ A \wedge B & \equiv & \neg(A \rightarrow \neg B) \end{array}$$

We could also have native rules for $\vee$ and $\wedge$:

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

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

Rules for $\vee$, $\wedge$ and an encoding in $\{\to, \bot\}$

Recall that we can encode $\vee$ and $\wedge$ in $\{\to, \bot\}$ by adequacy:

$$
\begin{array}{ccc}
A \vee B & \equiv & \neg A \to B \\
A \wedge B & \equiv & \neg(A \to \neg B)
\end{array}
$$

We could also have native rules for $\vee$ and $\wedge$:

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

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

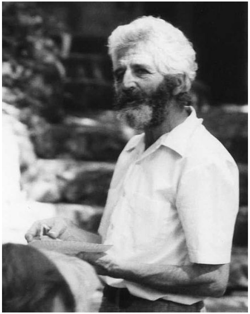
Proposition

The sequent system with $\vee$ and $\wedge$ native is also cut-free complete.

Proof idea.

Use cut-free-invertibility of the $\to$ and $\bot$ rules to simulate the rules above. □

Craig interpolation



Theorem (Craig Interpolation)

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

Proof of Craig Interpolation

By the previous arguments, we will work in the calculus including only the connectives $\neg$, $\vee$, $\wedge$ and all formulae in negation normal form, i.e. with negation only on atoms.

Proof of Craig Interpolation

By the previous arguments, we will work in the calculus including only the connectives $\neg$, $\vee$, $\wedge$ and all formulae in negation normal form, i.e. with negation only on atoms.

NB: This form means that formulas do not change sides. Beware, this is not always possible for other logics!

Proof of Craig Interpolation

By the previous arguments, we will work in the calculus including only the connectives $\neg, \vee, \wedge$ and all formulae in negation normal form, i.e. with negation only on atoms.

NB: This form means that formulas do not change sides. Beware, this is not always possible for other logics!

Proof idea of Craig Interpolation.

Structural induction on a cut-free proof. For instance, if the proof ends with,

$$\wedge\text{-}r\ \dfrac{\overset{\pi_0}{\Gamma \vdash \Delta, A} \qquad \overset{\pi_1}{\Gamma \vdash \Delta, B}}{\Gamma \vdash \Delta, A \wedge B}$$

and I_0, I_1 are interpolants obtained from π_0, π_1 resp., then we may define the new interpolant as $I_0 \wedge I_1$. □

Outline

The system LK

Initial and structural rules

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

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 $\mathcal{F}$:

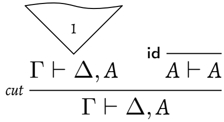
$$\begin{array}{rl} (wk) & A \to (B \to A) \\ (dist) & (A \to (B \to C)) \to ((A \to B) \to (A \to C)) \\ (neg) & ((A \to \bot) \to \bot) \to A \end{array}$$

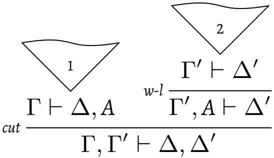
2. What about the quantifier axioms:

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

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

3. What is the Herbrand disjunction for the Drinker's Paradox?
4. How can we eliminate the cuts in the following cases?





Solutions to Exercise 1

$$(wk) \quad : \quad {\to}\text{-}r\,\dfrac{{\to}\text{-}r\,\dfrac{w\,\dfrac{\mathsf{id}\,\dfrac{}{A \vdash A}}{A, B \vdash A}}{A \vdash B \to A}}{\vdash A \to (B \to A)}$$

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

$$(dist) \quad : \quad 3\cdot{\to}\text{-}r\,\dfrac{{\to}\text{-}l\,\dfrac{w\,\dfrac{\mathsf{id}\,\dfrac{}{A \vdash A}}{A \to (B \to C), A \vdash A, C} \qquad {\to}\text{-}l\,\dfrac{w\,\dfrac{\mathsf{id}\,\dfrac{}{A \vdash A}}{B, A \vdash A, C} \qquad {\to}\text{-}l\,\dfrac{w\,\dfrac{\mathsf{id}\,\dfrac{}{B \vdash B}}{B, A \vdash B, C} \qquad w\,\dfrac{\mathsf{id}\,\dfrac{}{C \vdash C}}{C, B, A \vdash C}}{B \to C, B, A \vdash C}}{A \to (B \to C), B, A \vdash C}}{A \to (B \to C), A \to B, A \vdash C}}{\vdash (A \to (B \to C)) \to ((A \to B) \to (A \to C))}$$

Solutions to Exercise 2

$$
\dfrac{\dfrac{\dfrac{}{A[t/x] \vdash A[t/x]}\ \textsf{id}}{\forall x.A \vdash A[t/x]}\ \forall\text{-}l}{\vdash \forall x.A \to A[t/x]}\ \to\text{-}r
$$

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash A}\ \textsf{id}}{A \vdash B, A}\ w\text{-}r \qquad \dfrac{\dfrac{}{B \vdash B}\ \textsf{id}}{B, A \vdash B}\ w\text{-}l}{A \to B, A \vdash B}\ \to\text{-}l}{\forall x.(A \to B), A \vdash B}\ \forall\text{-}l}{\forall x.(A \to B), A \vdash \forall x.B}\ \forall\text{-}r \quad x \notin \mathsf{FV}(\forall x.(A \to B), A)}{\forall x.(A \to B) \vdash A \to \forall x.B}\ \to\text{-}r}{\vdash \forall x.(A \to B) \to (A \to \forall x.B)}\ \to\text{-}r
$$

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.