Introduction to Proof Theory

Lectures 5 & 6 - Some applications of proof theory

Anupam Das

University of Copenhagen

Logic Summer School

Australian National University

7^{th} December 2018

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

Outline

If something exists, can we find it?

Suppose that we are working in some first-order theory S, and we have a proof

$$\vdash \exists x.A(x)$$

We have established that there exists *some* object satisfying A. But can we actually exhibit one?

If something exists, can we find it?

Suppose that we are working in some first-order theory S, and we have a proof

$$\vdash \exists x.A(x)$$

We have established that there exists *some* object satisfying A. But can we actually exhibit one?

In other words, we want to find a term t in our language such that

$$\vdash A(t)$$

We call t a **witness** or a **realizer** for $\exists x.A(x)$.

If something exists, can we find it?

Suppose that we are working in some first-order theory S, and we have a proof

$$\vdash \exists x.A(x)$$

We have established that there exists *some* object satisfying A. But can we actually exhibit one?

In other words, we want to find a term t in our language such that

$$\vdash A(t)$$

We call t a **witness** or a **realizer** for $\exists x.A(x)$.

The search for witnesses for existential statements is theme which lies at the heart of proof theory.

$\exists x.A(x)$ vs. $A(t)$

It may seem at first glance that a concrete witness should always exist, and that it should be easy to find it. Let's first think about this informally.

$\exists x.A(x)$ vs. $A(t)$

It may seem at first glance that a concrete witness should always exist, and that it should be easy to find it. Let's first think about this informally.

Example

There exists a person who is at least as old as all other people on Earth.

$\exists x.A(x)$ vs. $A(t)$

It may seem at first glance that a concrete witness should always exist, and that it should be easy to find it. Let's first think about this informally.

Example

There exists a person who is at least as old as all other people on Earth.

For simplicity let's round this to the nearest year.

$\exists x.A(x)$ vs. $A(t)$

It may seem at first glance that a concrete witness should always exist, and that it should be easy to find it. Let's first think about this informally.

Example

There exists a person who is at least as old as all other people on Earth.

For simplicity let's round this to the nearest year.

- There is a person P_0 who is 100 years old.

$\exists x.A(x)$ vs. $A(t)$

It may seem at first glance that a concrete witness should always exist, and that it should be easy to find it. Let's first think about this informally.

Example

There exists a person who is at least as old as all other people on Earth.

For simplicity let's round this to the nearest year.

- There is a person P_0 who is 100 years old.
- Either they are at least as old as all other people, or there is a person P_1 who is 101 years old.

$\exists x.A(x)$ vs. $A(t)$

It may seem at first glance that a concrete witness should always exist, and that it should be easy to find it. Let's first think about this informally.

Example

There exists a person who is at least as old as all other people on Earth.

For simplicity let's round this to the nearest year.

- There is a person P_0 who is 100 years old.
- Either they are at least as old as all other people, or there is a person P_1 who is 101 years old.
- Either they are at least as old as all other people, or there is a person P_2 who is 102 years old.

It may seem at first glance that a concrete witness should always exist, and that it should be easy to find it. Let's first think about this informally.

Example

There exists a person who is at least as old as all other people on Earth.

For simplicity let's round this to the nearest year.

- There is a person P_0 who is 100 years old.
- Either they are at least as old as all other people, or there is a person P_1 who is 101 years old.
- Either they are at least as old as all other people, or there is a person P_2 who is 102 years old.

$$\vdots$$

$\exists x.A(x)$ vs. $A(t)$

It may seem at first glance that a concrete witness should always exist, and that it should be easy to find it. Let's first think about this informally.

Example

There exists a person who is at least as old as all other people on Earth.

For simplicity let's round this to the nearest year.

- There is a person P_0 who is 100 years old.
- Either they are at least as old as all other people, or there is a person P_1 who is 101 years old.
- Either they are at least as old as all other people, or there is a person P_2 who is 102 years old.

$$\vdots$$

This process will certainly stop for some $i < 200$.

It may seem at first glance that a concrete witness should always exist, and that it should be easy to find it. Let's first think about this informally.

Example

There exists a person who is at least as old as all other people on Earth.

For simplicity let's round this to the nearest year.

- There is a person P_0 who is 100 years old.
- Either they are at least as old as all other people, or there is a person P_1 who is 101 years old.
- Either they are at least as old as all other people, or there is a person P_2 who is 102 years old.

$$\vdots$$

This process will certainly stop for some $i < 200$.

But how do we actually find our oldest person?

It gets harder! Each of the following existential statements are certainly true:

It gets harder! Each of the following existential statements are certainly true:

- In exactly 10 years time, there will be a person who is at least as old as all other people on Earth.

It gets harder! Each of the following existential statements are certainly true:

- In exactly 10 years time, there will be a person who is at least as old as all other people on Earth.
- There once lived a person who was at least as old as all other people who ever lived.

It gets harder! Each of the following existential statements are certainly true:

- In exactly 10 years time, there will be a person who is at least as old as all other people on Earth.
- There once lived a person who was at least as old as all other people who ever lived.
- There will be a person who will be at least as old as all other people who have or will ever live.

It gets harder! Each of the following existential statements are certainly true:

- In exactly 10 years time, there will be a person who is at least as old as all other people on Earth.
- There once lived a person who was at least as old as all other people who ever lived.
- There will be a person who will be at least as old as all other people who have or will ever live.

Moreover, each of them are proven using very simple reasoning - and taking as an axiom some reasonable upper bound on the age of humans!

It gets harder! Each of the following existential statements are certainly true:

- In exactly 10 years time, there will be a person who is at least as old as all other people on Earth.
- There once lived a person who was at least as old as all other people who ever lived.
- There will be a person who will be at least as old as all other people who have or will ever live.

Moreover, each of them are proven using very simple reasoning - and taking as an axiom some reasonable upper bound on the age of humans!

Key point. Existential statements are very strong! It can be very difficult to find an actual witness.

Can we make this idea more formal?

Which reasoning principle is the culprit?

The difficulty in producing witnesses for existential statements is primarily due to the negation axiom:

$$\neg\neg A \rightarrow A$$

which is equivalent to the statement

$$\neg A \vee A$$

This is known as the **law of excluded-middle**. It is problematic because we can't always decide which of A or $\neg A$ holds.

Which reasoning principle is the culprit?

The difficulty in producing witnesses for existential statements is primarily due to the negation axiom:

$$\neg\neg A \rightarrow A$$

which is equivalent to the statement

$$\neg A \vee A$$

This is known as the **law of excluded-middle**. It is problematic because we can't always decide which of A or $\neg A$ holds.

A typical use of excluded-middle in the proof of an existential statement would be

- If A then $P(t_1)$,
- If $\neg A$ then $P(t_2)$,
- Therefore since $\neg A \vee A$ then $\exists x.P(x)$.

But we don't know which of t_1 or t_2 works!

Rational powers

Theorem

There exists a pair of irrational numbers x, y such that x^y is rational.

Theorem

There exists a pair of irrational numbers x, y such that x^y is rational.

Proof.

Suppose that $\sqrt{2}^{\sqrt{2}}$ is rational. Then we can just set $x = y = \sqrt{2}$.

Theorem

There exists a pair of irrational numbers x, y such that x^y is rational.

Proof.

Suppose that $\sqrt{2}^{\sqrt{2}}$ is rational. Then we can just set $x = y = \sqrt{2}$.

Otherwise, $\sqrt{2}^{\sqrt{2}}$ must be irrational, and we can set $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$, since

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{2} = 2.$$

Theorem

There exists a pair of irrational numbers x, y such that x^y is rational.

Proof.

Suppose that $\sqrt{2}^{\sqrt{2}}$ is rational. Then we can just set $x = y = \sqrt{2}$.

Otherwise, $\sqrt{2}^{\sqrt{2}}$ must be irrational, and we can set $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$, since

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{2} = 2.$$

Done.

Theorem

There exists a pair of irrational numbers x, y such that x^y is rational.

Proof.

Suppose that $\sqrt{2}^{\sqrt{2}}$ is rational. Then we can just set $x = y = \sqrt{2}$.

Otherwise, $\sqrt{2}^{\sqrt{2}}$ must be irrational, and we can set $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$, since

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^2 = 2.$$

Done. □

While the above proof gives us two *candidates* for x and y, namely

$$(x, y) = (\sqrt{2}, \sqrt{2}) \text{ or } (\sqrt{2}^{\sqrt{2}}, \sqrt{2})$$

we don't know which one works, since we have no procedure for deciding whether or not $\sqrt{2}^{\sqrt{2}}$ is irrational.

Theorem

There exists a pair of irrational numbers x, y such that x^y is rational.

Proof.

Suppose that $\sqrt{2}^{\sqrt{2}}$ is rational. Then we can just set $x = y = \sqrt{2}$.

Otherwise, $\sqrt{2}^{\sqrt{2}}$ must be irrational, and we can set $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$, since

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{2} = 2.$$

Done. □

While the above proof gives us two *candidates* for x and y, namely

$$(x, y) = (\sqrt{2}, \sqrt{2}) \text{ or } (\sqrt{2}^{\sqrt{2}}, \sqrt{2})$$

we don't know which one works, since we have no procedure for deciding whether or not $\sqrt{2}^{\sqrt{2}}$ is irrational.

Remark. Actually, it is known that $\sqrt{2}^{\sqrt{2}}$ is irrational, but this is a deep result in its own right.

A constructive proof: the infinitude of primes

A constructive proof: the infinitude of primes

Proposition

There are infinitely many prime numbers.

A constructive proof: the infinitude of primes

Proposition

There are infinitely many prime numbers.

FUNDAMENTAL THEOREM OF ARITHMETIC: every number has a prime factorisation.

Proof (Aristotle, Euclid).

Suppose there are only finitely many primes and label them $p_1, \ldots, p_k$. Apply the fundamental theorem to $p_1 \cdot \cdots \cdot p_k + 1$ to find a prime factor. This cannot be any of the p_i. □

What constructive information can we extract from this proof?

- The fundamental theorem of arithmetic gives us a factoring algorithm.
- Given primes $p_1, \ldots, p_k$, we simply factor $p_1 \cdots p_k + 1$ to find a new prime.

A constructive proof: the infinitude of primes

Proposition

There are infinitely many prime numbers.

Fundamental theorem of arithmetic: every number has a prime factorisation.

Proof (Aristotle, Euclid).

Suppose there are only finitely many primes and label them $p_1, \ldots, p_k$. Apply the fundamental theorem to $p_1 \cdot \cdots \cdot p_k + 1$ to find a prime factor. This cannot be any of the p_i. □

What constructive information can we extract from this proof?

- The fundamental theorem of arithmetic gives us a factoring algorithm.
- Given primes $p_1, \ldots, p_k$, we simply factor $p_1 \cdots p_k + 1$ to find a new prime.

In other words, the proof comes equipped with an algorithm for finding the next prime.

A constructive proof: the infinitude of primes

Proposition

There are infinitely many prime numbers.

FUNDAMENTAL THEOREM OF ARITHMETIC: every number has a prime factorisation.

Proof (Aristotle, Euclid).

Suppose there are only finitely many primes and label them $p_1, \dots, p_k$. Apply the fundamental theorem to $p_1 \cdot \dots \cdot p_k + 1$ to find a prime factor. This cannot be any of the p_i. □

What constructive information can we extract from this proof?

- The fundamental theorem of arithmetic gives us a factoring algorithm.
- Given primes $p_1, \dots, p_k$, we simply factor $p_1 \cdots p_k + 1$ to find a new prime.

In other words, the proof comes equipped with an algorithm for finding the next prime.

We also derive a bound: for any number n there is a prime p with $n < p \leq n! + 1$.

Outline

1. What does it mean to exist?
2. A less basic witnessing theorem
3. ‘Intuitionistic’ reasoning
4. From semantics to syntax: the scalability of Gentzen
5. From richer semantics to a newer proof theory
6. Personal perspectives: a revolution in proof theory
7. References

Peano Arithmetic, in sequent style

Recall that **Peano Arithmetic** (PA) is a FO theory over the language $\{\mathtt{0}, \mathtt{s}, +, \times\}$.

Recall that **Peano Arithmetic** (PA) is a FO theory over the language $\{0, \mathsf{s}, +, \times\}$.

We give a sequent-style system for it by adding to LK the following initial sequents,

- $0 = s(a) \vdash$
- $\mathsf{s}(a) = \mathsf{s}(b) \vdash a = b$
- $\vdash a + 0 = a$
- $\vdash a + \mathsf{s}(b) = \mathsf{s}(a + b)$
- $\vdash a \times 0 = 0$
- $\vdash a \times \mathsf{s}(b) = (a \times b) + a$

Recall that **Peano Arithmetic** (PA) is a FO theory over the language $\{0, \mathsf{s}, +, \times\}$.

We give a sequent-style system for it by adding to LK the following initial sequents,

- $0 = s(a) \vdash$
- $\mathsf{s}(a) = \mathsf{s}(b) \vdash a = b$
- $\vdash a + 0 = a$
- $\vdash a + \mathsf{s}(b) = \mathsf{s}(a + b)$
- $\vdash a \times 0 = 0$
- $\vdash a \times \mathsf{s}(b) = (a \times b) + a$

and, for each formula A, a corresponding induction rule:

$$\frac{\Gamma \vdash \Delta, A(0) \quad \Gamma, A(a) \vdash \Delta, A(\mathsf{s}a)}{\Gamma \vdash \Delta, A(t)}\ ind \quad (a \notin \mathsf{FV}(\Gamma, \Delta, A))$$

Existential proofs and a normal form

Convention: all formulae are over $\{\neg, \vee, \wedge\}$ in De Morgan Normal form (i.e. negation only on atoms). We also close all rules by De Morgan duality, so that there is no changing of sides in a proof.

Existential proofs and a normal form

Convention: all formulae are over $\{\neg, \vee, \wedge\}$ in De Morgan Normal form (i.e. negation only on atoms). We also close all rules by De Morgan duality, so that there is no changing of sides in a proof.

Definition

We call a formula **existential** if is of the form $\exists \vec{x}.A$ where A is quantifier-free. The theory $I\Sigma_1'$ is PA with induction restricted to existential formulae.

NB: this is non-standard terminology, bespoke to this lecture!

Existential proofs and a normal form

Convention: all formulae are over $\{\neg, \vee, \wedge\}$ in De Morgan Normal form (i.e. negation only on atoms). We also close all rules by De Morgan duality, so that there is no changing of sides in a proof.

Definition

We call a formula **existential** if is of the form $\exists \vec{x}.A$ where A is quantifier-free. The theory $I\Sigma_1'$ is PA with induction restricted to existential formulae.

NB: this is non-standard terminology, bespoke to this lecture!

The MRDP theorem (aka Hilbert's 10^{th} problem, Matiyasevich '70)

Existential formulae are complete for semi-recursive predicates: they can encode the halting problem.

Convention: all formulae are over $\{\neg, \vee, \wedge\}$ in De Morgan Normal form (i.e. negation only on atoms). We also close all rules by De Morgan duality, so that there is no changing of sides in a proof.

Definition

We call a formula **existential** if is of the form $\exists \vec{x}.A$ where A is quantifier-free. The theory $I\Sigma_1'$ is PA with induction restricted to existential formulae.

NB: this is non-standard terminology, bespoke to this lecture!

The MRDP theorem (aka Hilbert's 10th problem, Matiyasevich '70)

Existential formulae are complete for semi-recursive predicates: they can encode the halting problem.

NB: The MRDP theorem *might* be overkill here!

Convention: all formulae are over $\{\neg, \vee, \wedge\}$ in De Morgan Normal form (i.e. negation only on atoms). We also close all rules by De Morgan duality, so that there is no changing of sides in a proof.

Definition

We call a formula **existential** if is of the form $\exists \vec{x}.A$ where A is quantifier-free. The theory $I\Sigma_1'$ is PA with induction restricted to existential formulae.

NB: this is non-standard terminology, bespoke to this lecture!

The MRDP theorem (aka Hilbert's 10th problem, Matiyasevich '70)

Existential formulae are complete for semi-recursive predicates: they can encode the halting problem.

NB: The MRDP theorem *might* be overkill here!

Proposition ('Free-cut' elimination)

Any $I\Sigma_1'$-provable sequent of only existential formulae can be proved using only existential formulae.

Existential proofs and primitive recursion

Existential proofs and primitive recursion

Recall the primitive recursive functions that Michael showed:

Definition

The **primitive recursive** functions is the smallest class of functions containing $\mathsf{0}, \mathsf{s}, +, \times$, projections and closed under composition and primitive recursion: if g, h are primitive recursive then so is f defined as follows:

$$\begin{array}{rcl} f(\mathsf{0}, \vec{x}) & = & g(\vec{x}) \\ f(\mathsf{s}x, \vec{x}) & = & h(x, \vec{x}, f(x, \vec{x})) \end{array}$$

Recall the primitive recursive functions that Michael showed:

Definition

The **primitive recursive** functions is the smallest class of functions containing $\mathsf{0}, \mathsf{s}, +, \times$, projections and closed under composition and primitive recursion: if g, h are primitive recursive then so is f defined as follows:

$$\begin{array}{rcl} f(\mathsf{0}, \vec{x}) & = & g(\vec{x}) \\ f(\mathsf{s}x, \vec{x}) & = & h(x, \vec{x}, f(x, \vec{x})) \end{array}$$

The main result we will show is:

Theorem (Parsons '72)

If $I\Sigma_1' \vdash \forall \vec{x}. \exists ! y. A(x, y)$, where A is quantifier-free, then $A(\vec{x}, y)$ is the graph of a primitive recursive function.

Recall the primitive recursive functions that Michael showed:

Definition

The **primitive recursive** functions is the smallest class of functions containing $0, \mathsf{s}, +, \times$, projections and closed under composition and primitive recursion: if g, h are primitive recursive then so is f defined as follows:

$$\begin{array}{rcl} f(0, \vec{x}) & = & g(\vec{x}) \\ f(\mathsf{s}x, \vec{x}) & = & h(x, \vec{x}, f(x, \vec{x})) \end{array}$$

The main result we will show is:

Theorem (Parsons '72)

If $I\Sigma_1' \vdash \forall \vec{x}. \exists ! y. A(x, y)$, where A is quantifier-free, then $A(\vec{x}, y)$ is the graph of a primitive recursive function.

NB: Parsons actually proved this for a slightly stronger theory, $I\Sigma_1$, which gives a converse result too.

Motto: *induction on semi-recursive predicates captures precisely primitive recursion.*

Existential proofs and primitive recursion

Recall the primitive recursive functions that Michael showed:

Definition

The **primitive recursive** functions is the smallest class of functions containing $0, \mathsf{s}, +, \times$, projections and closed under composition and primitive recursion: if g, h are primitive recursive then so is f defined as follows:

$$\begin{aligned} f(0, \vec{x}) &= g(\vec{x}) \\ f(\mathsf{s}x, \vec{x}) &= h(x, \vec{x}, f(x, \vec{x})) \end{aligned}$$

The main result we will show is:

Theorem (Parsons '72)

If $I\Sigma_1' \vdash \forall \vec{x}.\exists! y.A(x, y)$, where A is quantifier-free, then $A(\vec{x}, y)$ is the graph of a primitive recursive function.

NB: Parsons actually proved this for a slightly stronger theory, $I\Sigma_1$, which gives a converse result too.

MOTTO: *induction on semi-recursive predicates captures precisely primitive recursion.*

(Dirk will say much more about this kind of stuff next week!)

Some bootstrapping

The following functions are primitive recursive:

<u>CONDITIONAL</u>

The function:

$$\mathsf{cond}(x, y, z) := \begin{cases} y & x = 0 \\ z & \text{otherwise} \end{cases}$$

NB: think of this as a $\texttt{if} - \texttt{then} - \texttt{else}$ construction.

The following functions are primitive recursive:

CONDITIONAL

The function:

$$\mathsf{cond}(x,y,z) := \begin{cases} y & x = 0 \\ z & \text{otherwise} \end{cases}$$

NB: think of this as a `if` $-$ `then` $-$ `else` construction.

CHARACTERISTIC FUNCTIONS OF QUANTIFIER-FREE FORMULAE

For each quantifier-free formula $A(\vec{a})$ (with all free variables displayed), the function:

$$f_A(\vec{x}) := \begin{cases} 1 & \mathbb{N} \vDash A(\vec{x}) \\ 0 & \text{otherwise} \end{cases}$$

The following functions are primitive recursive:

CONDITIONAL

The function:

$$\mathsf{cond}(x, y, z) := \begin{cases} y & x = 0 \\ z & \text{otherwise} \end{cases}$$

NB: think of this as a `if` $-$ `then` $-$ `else` construction.

CHARACTERISTIC FUNCTIONS OF QUANTIFIER-FREE FORMULAE

For each quantifier-free formula $A(\vec{a})$ (with all free variables displayed), the function:

$$f_A(\vec{x}) := \begin{cases} 1 & \mathbb{N} \vDash A(\vec{x}) \\ 0 & \text{otherwise} \end{cases}$$

EXERCISE: Prove that these functions are primitive recursive for yourself.

Proof idea

Proof idea

Remark: Notice that, if $I\Sigma_1' \vdash \forall \vec{x}.\exists y.A(\vec{x}, y)$ then there is an existential proof of $\exists y.A(\vec{a}, y)$, by invertibility of $\forall$-r and the free-cut free normal form theorem.

Proof idea

Remark: Notice that, if $I\Sigma_1' \vdash \forall \vec{x}.\exists y.A(\vec{x}, y)$ then there is an existential proof of $\exists y.A(\vec{a}, y)$, by invertibility of $\forall$-r and the free-cut free normal form theorem.

We will show that, for any provable existential sequent,

$$\exists x_1.A_1, \ldots, \exists x_m.A_m \vdash \exists y_1.B_1, \ldots, \exists y_n.B_n$$

with free variables $\vec{a}$

Proof idea

Remark: Notice that, if $I\Sigma_1' \vdash \forall \vec{x}.\exists y.A(\vec{x}, y)$ then there is an existential proof of $\exists y.A(\vec{a}, y)$, by invertibility of $\forall$-r and the free-cut free normal form theorem.

We will show that, for any provable existential sequent,

$$\exists x_1.A_1, \ldots, \exists x_m.A_m \vdash \exists y_1.B_1, \ldots, \exists y_n.B_n$$

with free variables $\vec{a}$:

- for $j \leq n$, there are primitive recursive functions $f_j(\vec{a}, \vec{x})$; such that,
- if for all $i \leq m$, $\mathbb{N} \vDash A_i[b_i/x_i]$, there is $j \leq n$ such that $\mathbb{N} \vDash B_j[f_j(\vec{a}, \vec{b})/y]$.

Proof idea

REMARK: Notice that, if $I\Sigma_1' \vdash \forall \vec{x}.\exists y.A(\vec{x}, y)$ then there is an existential proof of $\exists y.A(\vec{a}, y)$, by invertibility of $\forall$-r and the free-cut free normal form theorem.

We will show that, for any provable existential sequent,

$$\exists x_1.A_1, \ldots, \exists x_m.A_m \vdash \exists y_1.B_1, \ldots, \exists y_n.B_n$$

with free variables $\vec{a}$:

- for $j \leq n$, there are primitive recursive functions $f_j(\vec{a}, \vec{x})$; such that,
- if for all $i \leq m$, $\mathbb{N} \vDash A_i[b_i/x_i]$, there is $j \leq n$ such that $\mathbb{N} \vDash B_j[f_j(\vec{a}, \vec{b})/y]$.

How should we prove this?

Proof idea

Remark: Notice that, if $I\Sigma_1' \vdash \forall \vec{x}.\exists y.A(\vec{x}, y)$ then there is an existential proof of $\exists y.A(\vec{a}, y)$, by invertibility of $\forall$-r and the free-cut free normal form theorem.

We will show that, for any provable existential sequent,

$$\exists x_1.A_1, \ldots, \exists x_m.A_m \vdash \exists y_1.B_1, \ldots, \exists y_n.B_n$$

with free variables $\vec{a}$:

- for $j \leq n$, there are primitive recursive functions $f_j(\vec{a}, \vec{x})$; such that,
- if for all $i \leq m$, $\mathbb{N} \vDash A_i[b_i/x_i]$, there is $j \leq n$ such that $\mathbb{N} \vDash B_j[f_j(\vec{a}, \vec{b})/y]$.

How should we prove this? Let us proceed by structural induction…

Existential cases

Let us look at some of the ways a proof might end:

Existential cases

Let us look at some of the ways a proof might end:

(Throughout, we assume $|\Gamma| = m$ and $|\Delta| = n$)

$$\exists\text{-}l\ \frac{\Gamma, A[a/x] \vdash \Delta}{\Gamma, \exists x.A \vdash \Delta}$$

Define $f_j(\vec{a}, \vec{x}, x) := f_j'(x, \vec{a}, \vec{x})$.

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

Define $f_{n+1}(\vec{a}, \vec{x}) := t$.

Let us look at some of the ways a proof might end:

(Throughout, we assume $|\Gamma| = m$ and $|\Delta| = n$)

$$\exists\text{-}l \, \frac{\Gamma, A[a/x] \vdash \Delta}{\Gamma, \exists x.A \vdash \Delta}$$

Define $f_j(\vec{a}, \vec{x}, x) := f_j'(x, \vec{a}, \vec{x})$.

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

Define $f_{n+1}(\vec{a}, \vec{x}) := t$.

What about the universal quantifier or negation cases, which could be non-constructive?

Existential cases

Let us look at some of the ways a proof might end:

(Throughout, we assume $|\Gamma| = m$ and $|\Delta| = n$)

$$\exists\text{-}l \; \frac{\Gamma, A[a/x] \vdash \Delta}{\Gamma, \exists x.A \vdash \Delta}$$

Define $f_j(\vec{a}, \vec{x}, x) := f_j'(x, \vec{a}, \vec{x})$.

$$\exists\text{-}r \; \frac{\Gamma \vdash \Delta, \exists y.B[t/x]}{\Gamma \vdash \Delta, \exists x, y.B}$$

Define $f_{n+1}(\vec{a}, \vec{x}) := t$.

What about the universal quantifier or negation cases, which could be non-constructive? There are none by our normal form!

Structural rules and induction

$$\textit{c-l}\ \frac{\Gamma, \exists x.A, \exists x.A \vdash \Delta}{\Gamma, \exists x.A \vdash \Delta}$$

Structural rules and induction

$$\text{c-l}\ \frac{\Gamma, \exists x.A, \exists x.A \vdash \Delta}{\Gamma, \exists x.A \vdash \Delta}$$

Define $f_j(\vec{a}, \vec{x}, x) := f_j'(\vec{a}, \vec{x}, x, x)$.

$$\text{c-l}\ \frac{\Gamma, \exists x.A, \exists x.A \vdash \Delta}{\Gamma, \exists x.A \vdash \Delta}$$

Define $f_j(\vec{a}, \vec{x}, x) := f_j'(\vec{a}, \vec{x}, x, x)$.

$$\text{c-r}\ \frac{\Gamma \vdash \Delta, \exists x.B, \exists x.B}{\Gamma \vdash \Delta, \exists x.B}$$

Structural rules and induction

$$\text{c-l}\ \frac{\Gamma, \exists x.A, \exists x.A \vdash \Delta}{\Gamma, \exists x.A \vdash \Delta}$$

Define $f_j(\vec{a}, \vec{x}, x) := f_j'(\vec{a}, \vec{x}, x, x)$.

$$\text{c-r}\ \frac{\Gamma \vdash \Delta, \exists x.B, \exists x.B}{\Gamma \vdash \Delta, \exists x.B}$$

Then define:

$$f_{n+1}(\vec{a}, \vec{x}) := \begin{cases} f_{n+1}'(\vec{a}, \vec{x}) & \mathbb{N} \models A[f_{n+1}'(\vec{a}, \vec{x})/x] \\ f_{n+2}'(\vec{a}, \vec{x}) & \text{otherwise} \end{cases}$$

The induction case

The most interesting case is induction:

$$\text{ind}\ \frac{\Gamma \vdash \Delta, \exists x.A(\mathsf{0}) \quad \Gamma, \exists x.A(a) \vdash \Delta, \exists x.A(\mathsf{s}a)}{\Gamma \vdash \Delta, \exists x.A(t)}$$

The induction case

The most interesting case is induction:

$$\textit{ind}\ \frac{\Gamma \vdash \Delta, \exists x.A(\mathsf{0}) \quad \Gamma, \exists x.A(a) \vdash \Delta, \exists x.A(\mathsf{s}a)}{\Gamma \vdash \Delta, \exists x.A(t)}$$

Unsurprisingly, this is where primitive recursion shows up. Let g and h be functions obtained from the left and right subproofs, by inductive hypothesis.

The induction case

The most interesting case is induction:

$$\text{ind}\ \frac{\Gamma \vdash \Delta, \exists x.A(0) \quad \Gamma, \exists x.A(a) \vdash \Delta, \exists x.A(\mathsf{s}a)}{\Gamma \vdash \Delta, \exists x.A(t)}$$

Unsurprisingly, this is where primitive recursion shows up. Let g and h be functions obtained from the left and right subproofs, by inductive hypothesis.

We can define an auxiliary function by primitive recursion as follows:

$$\begin{array}{rcl} f'(0, \vec{a}, \vec{x}) & = & g(\vec{x}, \vec{a}) \\ f'(\mathsf{s}a, \vec{a}, \vec{x}) & = & h(f(a, \vec{a}, \vec{x}), \vec{a}, \vec{x}) \end{array}$$

The induction case

The most interesting case is induction:

$$\textit{ind}\ \frac{\Gamma \vdash \Delta, \exists x.A(0) \quad \Gamma, \exists x.A(a) \vdash \Delta, \exists x.A(\mathsf{s}a)}{\Gamma \vdash \Delta, \exists x.A(t)}$$

Unsurprisingly, this is where primitive recursion shows up. Let g and h be functions obtained from the left and right subproofs, by inductive hypothesis.

We can define an auxiliary function by primitive recursion as follows:

$$\begin{array}{rcl} f'(0, \vec{a}, \vec{x}) & = & g(\vec{x}, \vec{a}) \\ f'(\mathsf{s}a, \vec{a}, \vec{x}) & = & h(f(a, \vec{a}, \vec{x}), \vec{a}, \vec{x}) \end{array}$$

Now we may simply set $f(\vec{a}, \vec{x}) := f'(t, \vec{a}, \vec{x})$.

Outline

A problem with pure reasoning

We are in a strange situation: Perfectly valid reasoning allows us to conclude

$$\exists x, y \notin \mathbb{Q}.\ x^y \in \mathbb{Q}$$

but we cannot explicitly witness this...

A problem with pure reasoning

We are in a strange situation: Perfectly valid reasoning allows us to conclude

$$\exists x, y \notin \mathbb{Q}.\ x^y \in \mathbb{Q}$$

but we cannot explicitly witness this...

so do such x, y really exist?

A problem with pure reasoning

We are in a strange situation: Perfectly valid reasoning allows us to conclude

$$\exists x, y \notin \mathbb{Q}.\ x^y \in \mathbb{Q}$$

but we cannot explicitly witness this...

so do such x, y really exist?

The question of what it means for an object to exist, or for a statement to be true, created a famous divide in the logical community, and led to the development of **intuitionism**.

Formalism vs Intuitionism

<u>Formalism</u> (led by D. Hilbert, see [Weir, 2015])

- Based on *syntax*.
- Mathematics is a game of symbols: something 'exists' if it can be derived from mathematical axioms by logical inference rules.
- In particular, if we can show the nonexistence of an object is false, then the object must exist.

<u>Intuitionism</u> (led by L. E. J. Brouwer, see [Iemhoff, 2016])

- Based on *semantics*.
- Mathematics is a mental construction: Something exists only if it can be exhibited.
- In particular, if we can show the nonexistence of an object is false, that doesn't necessarily mean that the object exists!

Combining intuitionism with formalism

So far in this course we have broadly taken the formalist approach. However, we can adapt our deductive systems so that they aligns with the principle of intuitionism. As we already mentioned, the problem lies with the negation axiom, so why not just remove it?

So far in this course we have broadly taken the formalist approach. However, we can adapt our deductive systems so that they aligns with the principle of intuitionism. As we already mentioned, the problem lies with the negation axiom, so why not just remove it?

Definition (A Hilbert-Frege system for intuitionistic first-order logic)

Take the system we defined in Lecture 1, but replace the axiom schema

$$\neg\neg A \to A$$

with the axiom **ex falso quodlibet**:

$$\bot \to A$$

We write $\Gamma \vdash_i A$ is A is derivable from Γ *intuitionistically*.

Combining intuitionism with formalism

So far in this course we have broadly taken the formalist approach. However, we can adapt our deductive systems so that they aligns with the principle of intuitionism. As we already mentioned, the problem lies with the negation axiom, so why not just remove it?

Definition (A Hilbert-Frege system for intuitionistic first-order logic)

Take the system we defined in Lecture 1, but replace the axiom schema

$$\neg\neg A \to A$$

with the axiom **ex falso quodlibet**:

$$\bot \to A$$

We write $\Gamma \vdash_i A$ is A is derivable from Γ *intuitionistically*.

We have $\Gamma \vdash_i A \Rightarrow \Gamma \vdash A$, but not conversely. For example,

$$\nvdash_i A \vee \neg A$$
$$\nvdash_i \neg(A \wedge B) \leftrightarrow \neg A \vee \neg B$$
$$\nvdash_i \exists x(P(x) \to \forall y.P(y))$$

An intuitionistic sequent calculus

The formulation of intuitionistic logic in the sequent calculus turns out to be incredibly simple, which highlights once again the elegance of this system.

An intuitionistic sequent calculus

The formulation of intuitionistic logic in the sequent calculus turns out to be incredibly simple, which highlights once again the elegance of this system.

Theorem (Gentzen, '34)

Let LJ *denote the restriction of the system* LK *in which we are only allowed to have one formula on the right, i.e. only contains sequents of the form* $\Gamma \vdash A$*. Then* LJ *is sound and complete for intuitionistic logic.*

The formulation of intuitionistic logic in the sequent calculus turns out to be incredibly simple, which highlights once again the elegance of this system.

Theorem (Gentzen, '34)

Let LJ *denote the restriction of the system* LK *in which we are only allowed to have one formula on the right, i.e. only contains sequents of the form* $\Gamma \vdash A$*. Then* LJ *is sound and complete for intuitionistic logic.*

This is a quite remarkable result: a fundamentally semantic and philosophical notion is reflected by a purely syntactic criterion.

The formulation of intuitionistic logic in the sequent calculus turns out to be incredibly simple, which highlights once again the elegance of this system.

Theorem (Gentzen, '34)

Let LJ *denote the restriction of the system* LK *in which we are only allowed to have one formula on the right, i.e. only contains sequents of the form* $\Gamma \vdash A$*. Then* LJ *is sound and complete for intuitionistic logic.*

This is a quite remarkable result: a fundamentally semantic and philosophical notion is reflected by a purely syntactic criterion.

We also get cut-elimination for free:

Observation

Cut-elimination for LK *applied to* LJ *proofs yields cut-free* LJ *proofs.*

Corollary

Intuitionistic propositional logic is decidable.

Observe how the single-formula-on-the-right condition is broken by LK proofs of fundamentally classical theorems:

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

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

Intuitionistic logic, while being more restrictive than classical logic, enjoys two important properties:

Intuitionistic logic, while being more restrictive than classical logic, enjoys two important properties:

Theorem (Disjunction property)

If $\vdash_i A \vee B$ *then either* $\vdash_i A$ *or* $\vdash_i B$.

Intuitionistic logic, while being more restrictive than classical logic, enjoys two important properties:

Theorem (Disjunction property)

If $\vdash_i A \vee B$ *then either* $\vdash_i A$ *or* $\vdash_i B$.

Theorem (Existence property)

If $\vdash_i \exists x.A(x)$ *where* $A(x)$ *has only* x *free, then there is a closed term* t *such that* $\vdash_i A(t)$.

Intuitionistic logic, while being more restrictive than classical logic, enjoys two important properties:

Theorem (Disjunction property)

If $\vdash_i A \vee B$ *then either* $\vdash_i A$ *or* $\vdash_i B$*.*

Theorem (Existence property)

If $\vdash_i \exists x.A(x)$ *where* $A(x)$ *has only* x *free, then there is a closed term* t *such that* $\vdash_i A(t)$*.*

The existence property demonstrates that for intuitionistic logic, an object exists if and only if it can be constructed!

Outline

Adapting LK

Adapting LK

Recall something Tom said about proofs for intuitionistic logic:

Observation

Restricting LK *to have only one formula on the right results in a calculus sound and complete for intuitionistic logic.*

Recall something Tom said about proofs for intuitionistic logic:

Observation

Restricting LK *to have only one formula on the right results in a calculus sound and complete for intuitionistic logic.*

This may be reformulated as:

"LJ does not allow structural rules on the right (*i.e. w-r*, *c-r*)"

Adapting LK

Recall something Tom said about proofs for intuitionistic logic:

Observation

Restricting LK *to have only one formula on the right results in a calculus sound and complete for intuitionistic logic.*

This may be reformulated as:

"LJ does not allow structural rules on the right (*i.e. w-r*, *c-r*)"

Remarkably, similar structural constraints suffice to elegantly capture other important logics in the wild.

Recall something Tom said about proofs for intuitionistic logic:

Observation

Restricting LK *to have only one formula on the right results in a calculus sound and complete for intuitionistic logic.*

This may be reformulated as:

"LJ does not allow structural rules on the right (*i.e. w-r*, *c-r*)"

Remarkably, similar structural constraints suffice to elegantly capture other important logics in the wild.

Let us consider a few case studies that you might have heard of…

Relevan(t+ce) logic

Relevan(t+ce) logic

Remember theorems like *Pierce's law* or the *Drinker's paradox*:

$$((A \to B) \to A) \to A$$
$$\exists x.(D(x) \to \forall y.D(y))$$

Relevan(t+ce) logic

Remember theorems like *Pierce's law* or the *Drinker's paradox*:

$$((A \to B) \to A) \to A$$
$$\exists x.(D(x) \to \forall y.D(y))$$

These were counterintuitive since their implications did not reflect any causality from premiss to conclusion. They were material.

Remember theorems like *Pierce's law* or the *Drinker's paradox*:

$$((A \to B) \to A) \to A$$
$$\exists x.(D(x) \to \forall y.D(y))$$

These were counterintuitive since their implications did not reflect any causality from premiss to conclusion. They were material.

Relevant logic (or Relevance logic) arose in the early 20$^{\text{th}}$ century. It is an attempt to remedy this by rejecting the law of *ex falso quod libet*.

Relevan(t+ce) logic

Remember theorems like *Pierce's law* or the *Drinker's paradox*:

$$((A \to B) \to A) \to A$$
$$\exists x.(D(x) \to \forall y.D(y))$$

These were counterintuitive since their implications did not reflect any causality from premiss to conclusion. They were material.

Relevant logic (or Relevance logic) arose in the early 20$^{\text{th}}$ century. It is an attempt to remedy this by rejecting the law of *ex falso quod libet*.

Initially proposed in a Hilbert-Frege setting, relevant logic lacked a rigorous proof-theoretic treatment.

Remember theorems like *Pierce's law* or the *Drinker's paradox*:

$$((A \to B) \to A) \to A$$
$$\exists x.(D(x) \to \forall y.D(y))$$

These were counterintuitive since their implications did not reflect any causality from premiss to conclusion. They were material.

Relevant logic (or Relevance logic) arose in the early 20[th] century. It is an attempt to remedy this by rejecting the law of *ex falso quod libet*.

Initially proposed in a Hilbert-Frege setting, relevant logic lacked a rigorous proof-theoretic treatment. However, in the sequent calculus, we again have a remarkably simple characterisation:

Theorem (folklore)

- LK, *without w rules, is sound and complete for* ***basic relevant logic****.*
- *Cut-elimination still holds.*

Remember theorems like *Pierce's law* or the *Drinker's paradox*:

$$((A \to B) \to A) \to A$$
$$\exists x.(D(x) \to \forall y.D(y))$$

These were counterintuitive since their implications did not reflect any causality from premiss to conclusion. They were material.

Relevant logic (or Relevance logic) arose in the early 20$^{\text{th}}$ century. It is an attempt to remedy this by rejecting the law of *ex falso quod libet*.

Initially proposed in a Hilbert-Frege setting, relevant logic lacked a rigorous proof-theoretic treatment. However, in the sequent calculus, we again have a remarkably simple characterisation:

Theorem (folklore)

- LK, *without w rules, is sound and complete for* ***basic relevant logic****.*
- *Cut-elimination still holds.*

For a concise introduction, consult:

- [Mares, 2014]

Linear logic

Linear logic

Jean-Yves Girard proposed **linear logic** in the ’80s, to model resource-sensitive computation.

Jean-Yves Girard proposed **linear logic** in the '80s, to model resource-sensitive computation.

Linear logic goes further than relevant logic in terms of restricting the structural rules, rejecting:

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

Instead, we recover different versions of the connectives based on their usually equivalent rules.

Linear logic

Jean-Yves Girard proposed **linear logic** in the '80s, to model resource-sensitive computation.

Linear logic goes further than relevant logic in terms of restricting the structural rules, rejecting:

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

Instead, we recover different versions of the connectives based on their usually equivalent rules.

Theorem (Girard '87)

Linear logic (LL) enjoys cut-elimination.

This means that *LL* is meaningful since, in particular, it must be consistent: if the empty sequent were derivable, what would be the last step in a cut-free proof?

Linear logic

Jean-Yves Girard proposed **linear logic** in the '80s, to model resource-sensitive computation.

Linear logic goes further than relevant logic in terms of restricting the structural rules, rejecting:

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

Instead, we recover different versions of the connectives based on their usually equivalent rules.

Theorem (Girard '87)

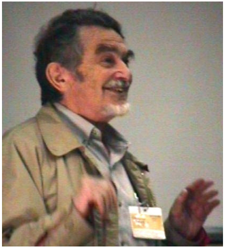
Linear logic (LL) enjoys cut-elimination.

This means that *LL* is meaningful since, in particular, it must be consistent: if the empty sequent were derivable, what would be the last step in a cut-free proof?

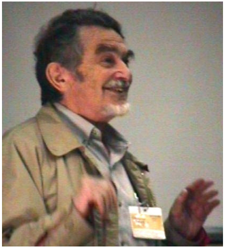
There is a lot more to say about *LL*. Here is a concise introduction:

- [Di Cosmo and Miller, 2016]

Lambek calculus



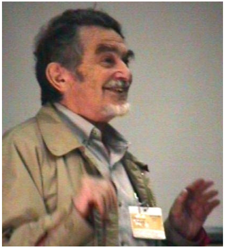
The **Lambek calculus** is a substructural logic obtained by combining resource-sensitivity with intuitionism.



The **Lambek calculus** is a substructural logic obtained by combining resource-sensitivity with intuitionism.

Furthermore, it restricts sequents to lists where order matters. I.e., it rejects:

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



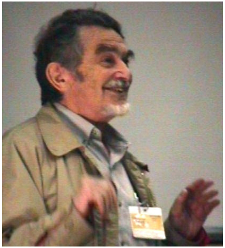
The **Lambek calculus** is a substructural logic obtained by combining resource-sensitivity with intuitionism.

Furthermore, it restricts sequents to lists where order matters. I.e., it rejects:

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

This calculus is incredibly important in *mathematics* and *linguistics*:

- In mathematics, it is modelled by **residuated lattices**.
- In linguistics, it is modelled by **categorical grammars**.



The **Lambek calculus** is a substructural logic obtained by combining resource-sensitivity with intuitionism.

Furthermore, it restricts sequents to lists where order matters. I.e., it rejects:

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

This calculus is incredibly important in *mathematics* and *linguistics*:

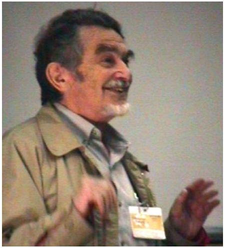
- In mathematics, it is modelled by **residuated lattices**.
- In linguistics, it is modelled by **categorical grammars**.

Once again…

Theorem

The Lambek calculus enjoys cut-elimination, and many of the usual corollaries.

Lambek calculus



The **Lambek calculus** is a substructural logic obtained by combining resource-sensitivity with intuitionism.

Furthermore, it restricts sequents to lists where order matters. I.e., it rejects:

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

This calculus is incredibly important in *mathematics* and *linguistics*:

- In mathematics, it is modelled by **residuated lattices**.
- In linguistics, it is modelled by **categorical grammars**.

Once again…

Theorem

The Lambek calculus enjoys cut-elimination, and many of the usual corollaries.

For more information, consult:

- [Moortgat, 2014].

Outline

A richer semantics

Classical propositional logic had a very simple Boolean semantics.

A richer semantics

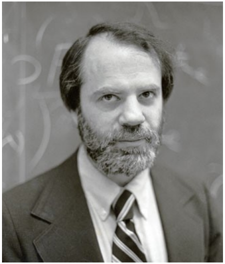
Classical propositional logic had a very simple Boolean semantics.

For richer logics such as *intuitionistic logic*, one must do some more work. As we already saw, we may arrive at semantics via realisers or proof interpretations.

Classical propositional logic had a very simple Boolean semantics.

For richer logics such as *intuitionistic logic*, one must do some more work. As we already saw, we may arrive at semantics via realisers or proof interpretations.

Saul Kripke and André Joyal proposed in the ’50s and ’60s a semantics based on **relational structures**.

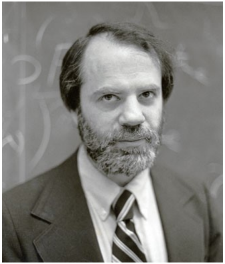


A richer semantics

Classical propositional logic had a very simple Boolean semantics.

For richer logics such as *intuitionistic logic*, one must do some more work. As we already saw, we may arrive at semantics via realisers or proof interpretations.

Saul Kripke and André Joyal proposed in the '50s and '60s a semantics based on **relational structures**.



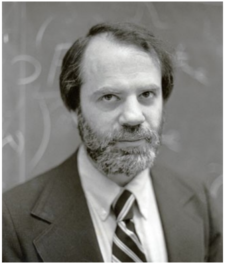
Theorem (informally)

LJ *is sound and complete over preorder structures with a Boolean valuation.*

Classical propositional logic had a very simple Boolean semantics.

For richer logics such as *intuitionistic logic*, one must do some more work. As we already saw, we may arrive at semantics via realisers or proof interpretations.

Saul Kripke and André Joyal proposed in the '50s and '60s a semantics based on **relational structures**.



Theorem (informally)

LJ *is sound and complete over preorder structures with a Boolean valuation.*

This has lead to fundamental advances in *philosophy*, *mathematics* and *computer science*.

Modal logics

Modal logics

Modal logic emerged in the early 20th century and constituted a competing approach to constructivism.

Modal logics

Modal logic emerged in the early 20$^{\text{th}}$ century and constituted a competing approach to constructivism.

They add to classical propositional logic two dual modalities $\Box$ and $\Diamond$:

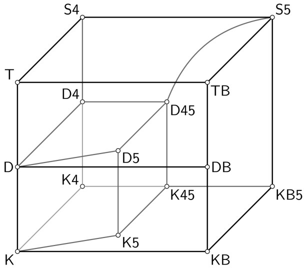
$$\begin{array}{lcl} \Box A & : & \text{“It is necessary that } A\text{”} \\ \Diamond A & : & \text{“It is possible that } A\text{”} \end{array}$$

Modal logic emerged in the early 20th century and constituted a competing approach to constructivism.

They add to classical propositional logic two dual modalities $\Box$ and $\Diamond$:

$$\begin{array}{lcl} \Box A & : & \text{"It is necessary that } A\text{"} \\ \Diamond A & : & \text{"It is possible that } A\text{"} \end{array}$$

Due to motivations from *philosophy* and *computer science* there are now countless different versions of modal logic that are widely studied:

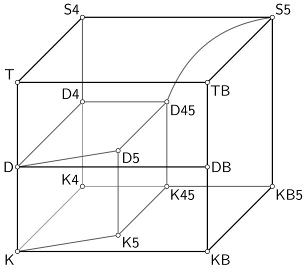


Modal logic emerged in the early 20th century and constituted a competing approach to constructivism.

They add to classical propositional logic two dual modalities $\Box$ and $\Diamond$:

$$\Box A \quad : \quad \text{"It is necessary that } A\text{"}$$
$$\Diamond A \quad : \quad \text{"It is possible that } A\text{"}$$

Due to motivations from *philosophy* and *computer science* there are now countless different versions of modal logic that are widely studied:



For a concise introduction, see:

- [Garson, 2016].

For a historical perspective, in particular contrasting the syntactic tradition, à la Lewis, and the semantic tradition, à la Kripke-Joyal, see:

- [Ballarin, 2017].

Gentzen calculi for modal logics

The Gentzen approach has been remarkably successful.

The Gentzen approach has been remarkably successful. A calculus for K is obtained by adding a single rule to LK (by De Morgan duality of $\Box$ and $\Diamond$):

$$k\ \frac{\Gamma \vdash A}{\Box\Gamma \vdash \Box A}$$

The Gentzen approach has been remarkably successful. A calculus for *K* is obtained by adding a single rule to LK (by De Morgan duality of □ and ◊):

$$k\,\frac{\Gamma \vdash A}{\Box\Gamma \vdash \Box A}$$

Extensions such as *S*4 are similarly handled by adding:

$$t\,\frac{\Gamma, A \vdash \Delta}{\Gamma, \Box A \vdash \Delta} \qquad 4\,\frac{\Box\Gamma \vdash A}{\Box\Gamma \vdash \Box A}$$

The Gentzen approach has been remarkably successful. A calculus for K is obtained by adding a single rule to LK (by De Morgan duality of $\Box$ and $\Diamond$):

$$k\,\frac{\Gamma \vdash A}{\Box\Gamma \vdash \Box A}$$

Extensions such as $S4$ are similarly handled by adding:

$$t\,\frac{\Gamma, A \vdash \Delta}{\Gamma, \Box A \vdash \Delta} \qquad 4\,\frac{\Box\Gamma \vdash A}{\Box\Gamma \vdash \Box A}$$

Remarkably, these calculi again enjoy cut-elimination:

Theorem

Cut-elimination holds for the sequent calculi for K and $S4$.

The Gentzen approach has been remarkably successful. A calculus for K is obtained by adding a single rule to LK (by De Morgan duality of $\Box$ and $\Diamond$):

$$k\,\frac{\Gamma \vdash A}{\Box\Gamma \vdash \Box A}$$

Extensions such as $S4$ are similarly handled by adding:

$$t\,\frac{\Gamma, A \vdash \Delta}{\Gamma, \Box A \vdash \Delta} \qquad 4\,\frac{\Box\Gamma \vdash A}{\Box\Gamma \vdash \Box A}$$

Remarkably, these calculi again enjoy cut-elimination:

Theorem

Cut-elimination holds for the sequent calculi for K and $S4$.

Corollary

- ***Interpolation*** *for modal logics.*
- ***Satisfiability solving*** *for modal logics.*

Every dream must end

However, this is where the story becomes difficult.

Every dream must end

However, this is where the story becomes difficult.

For the logic *S*5, we searched for a long time to find a cut-free calculus. We failed.

Every dream must end

However, this is where the story becomes difficult.

For the logic *S*5, we searched for a long time to find a cut-free calculus. We failed.

But out of that effort rose a new methodology for proof systems, that is currently still in its formative stages.

Theorem (Mints, Pottinger, Avron, informally)

*There is a cut-free calculus that manipulates 'lists of lists' which is sound and complete for S*5*.*

However, this is where the story becomes difficult.

For the logic *S*5, we searched for a long time to find a cut-free calculus. We failed.

But out of that effort rose a new methodology for proof systems, that is currently still in its formative stages.

Theorem (Mints, Pottinger, Avron, informally)

*There is a cut-free calculus that manipulates 'lists of lists' which is sound and complete for S*5*.*

Since this work, uniform and modular treatments have been found for all logics in the modal cube (and beyond!) in several other variations of sequent:

- Sequents are lists.
- Hypersequents are lists of lists.
- Nested sequents are trees.
- Labelled sequents are graphs.
- ...

Outline

Where is structural proof theory today

Where is structural proof theory today

As we speak, there is a revolution under way towards a proof theory:

- with more structure. (*e.g.* (hyper + labelled + nested) sequents, cyclic proofs)
- that is more compositional. (*e.g.* deep inference, categorical logic, natural deduction, proof nets)
- that is more symmetric. (*e.g.*display calculus, deep inference)

Where is structural proof theory today

As we speak, there is a revolution under way towards a proof theory:

- with more structure. (*e.g.* (hyper + labelled + nested) sequents, cyclic proofs)
- that is more compositional. (*e.g.* deep inference, categorical logic, natural deduction, proof nets)
- that is more symmetric. (*e.g.*display calculus, deep inference)

In the same way that Gentzen broke away from Hilbert-Frege systems to obtain powerful results, these advances have further extended the scope of proof theory.

Where is structural proof theory today

As we speak, there is a revolution under way towards a proof theory:

- with more structure. (*e.g.* (hyper + labelled + nested) sequents, cyclic proofs)
- that is more compositional. (*e.g.* deep inference, categorical logic, natural deduction, proof nets)
- that is more symmetric. (*e.g.*display calculus, deep inference)

In the same way that Gentzen broke away from Hilbert-Frege systems to obtain powerful results, these advances have further extended the scope of proof theory.

Let us look at two recent (very personally biased) developments…

Deep inference

Deep inference is a methodology underlying several of the developments we have seen.

Deep inference

Deep inference is a methodology underlying several of the developments we have seen.

It was first proposed by Guglielmi in the late '90s:

1. *"inference rules should operate on any connective in a formula"*
2. *"there should be no distinction between object level and meta level"*

Deep inference

Deep inference is a methodology underlying several of the developments we have seen.

It was first proposed by Guglielmi in the late '90s:

1. *"inference rules should operate on any connective in a formula"*
2. *"there should be no distinction between object level and meta level"*

It is the second point, that gives rise to compositionality and symmetry which is the most revolutionary.

Deep inference

Deep inference is a methodology underlying several of the developments we have seen.

It was first proposed by Guglielmi in the late '90s:

1. *"inference rules should operate on any connective in a formula"*
2. *"there should be no distinction between object level and meta level"*

It is the second point, that gives rise to compositionality and symmetry which is the most revolutionary.

<u>Achievements include:</u>

- Modular proof-theoretic treatments of substructural and modal logics.
- Cut-elimination proofs, including finer extraction of interpolants and witnesses.
- Much shorter proofs!

Structure at the level of a proof

Structure at the level of a proof

Changing the lines of a proof has yielded tremendous success, as we have seen.

Structure at the level of a proof

Changing the lines of a proof has yielded tremendous success, as we have seen.

If we want to reason inductively or over fixed points, we need to add some more structure, but this time at the level of a proof graph.

Changing the lines of a proof has yielded tremendous success, as we have seen.

If we want to reason inductively or over fixed points, we need to add some more structure, but this time at the level of a proof graph.

A **cyclic proof** is one that allows cyclic reasoning. This can sometimes be meaningful!

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\vdots}{b^2 = 2c^2 \vdash}\;\bullet}{c < a, 4c^2 = 2b^2 \vdash}}{\exists x < a. a = 2x, a^2 = 2b^2 \vdash}\;\bullet}{a^2 = 2b^2 \vdash}}{\vdash \forall x, y.\, x^2 \neq 2y^2}
$$

Structure at the level of a proof

Changing the lines of a proof has yielded tremendous success, as we have seen.

If we want to reason inductively or over fixed points, we need to add some more structure, but this time at the level of a proof graph.

A **cyclic proof** is one that allows cyclic reasoning. This can sometimes be meaningful!

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\vdots}{b^2 = 2c^2 \vdash}\bullet}{c < a, 4c^2 = 2b^2 \vdash}}{\exists x < a. a = 2x, a^2 = 2b^2 \vdash}}{a^2 = 2b^2 \vdash}\bullet}{\vdash \forall x, y.\, x^2 \neq 2y^2}$$

We now have proof theoretic treatments of:

- Fragments of the modal μ-calculus.
- Substructural logics with fixed points.
- First-order logic with inductive definitions
- Fragments of arithmetic.

Structure at the level of a proof

Changing the lines of a proof has yielded tremendous success, as we have seen.

If we want to reason inductively or over fixed points, we need to add some more structure, but this time at the level of a proof graph.

A **cyclic proof** is one that allows cyclic reasoning. This can sometimes be meaningful!

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\vdots}{b^2 = 2c^2 \vdash}\ \bullet}{c < a, 4c^2 = 2b^2 \vdash}}{\exists x < a . a = 2x, a^2 = 2b^2 \vdash}}{a^2 = 2b^2 \vdash}\ \bullet}{\vdash \forall x, y.\, x^2 \neq 2y^2}
$$

We now have proof theoretic treatments of:

- Fragments of the modal μ-calculus.
- Substructural logics with fixed points.
- First-order logic with inductive definitions
- Fragments of arithmetic.

There are an increasing number of emerging applications in *computer science* and *mathematics*.

Thank you all!

Outline

Ballarin, R. (2017).
Modern origins of modal logic.
In Zalta, E. N., editor, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, summer 2017 edition.

Di Cosmo, R. and Miller, D. (2016).
Linear logic.
In Zalta, E. N., editor, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, winter 2016 edition.

Garson, J. (2016).
Modal logic.
In Zalta, E. N., editor, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, spring 2016 edition.

Iemhoff, R. (2016).
Intuitionism in the philosophy of mathematics.
In Zalta, E. N., editor, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, winter 2016 edition.

References II

Kohlenbach, U. (2008).
Applied Proof Theory - Proof Interpretations and their Use in Mathematics.
Springer Monographs in Mathematics. Springer.

Mares, E. (2014).
Relevance logic.
In Zalta, E. N., editor, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, spring 2014 edition.

Moortgat, M. (2014).
Typelogical grammar.
In Zalta, E. N., editor, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, spring 2014 edition.

Weir, A. (2015).
Formalism in the philosophy of mathematics.
In Zalta, E. N., editor, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, spring 2015 edition.