Proof Theory, Logic, and Category Theory

Raheleh Jalali

Utrecht University

TACL Summer School
Praia de Mira

14-18 June, 2022

Hilbert's Program

Modern proof theory: established by David Hilbert.
He proposed a solution to the foundational crisis of mathematics:

Hilbert's program

- Main goal: provide secure foundations for mathematics (within a finite, complete and consistent set of axioms).
- Hilbert's proposal: prove the consistency of more complicated systems, such as real analysis, via simpler systems.
  Ultimately, the consistency of all of mathematics could be reduced to basic arithmetic.

Consistency

- To prove the consistency of a system, we can provide a model for it.
  Example: geometry and real analysis.
  The proof of this relative consistency often makes use of a more powerful system! Which system should we map set theory to?
- Alternative natural candidate: syntactic study.
  Assuming a system is inconsistent: there is a finite proof for contradiction.
  By a syntactical analysis we may be able to show that such a proof cannot exist for some theories.
  This is safe as our usual tool for this analysis is a finite combinatorics.
  This leads to his concern for finite mathematics.

Gödel's role

Gödel's incompleteness theorems (1931): Hilbert's program is impossible to achieve.
Suppose a consistent "strong enough" system is given.

1. First theorem: such a system can never be complete.

   Corollary: It is not possible to formalize all mathematical true statements within a formal system.

2. Second theorem: such a system cannot prove its own consistency.

   Corollary: Hilbert's assumption that a finitistic system can be used to prove the consistency of itself and of more powerful theories, such as set theory, is refuted.

Gentzen enters

Gentzen was Hilbert's student. He did not believe Gödel's results put an end to Hilbert's program. His goal was to prove the (relative) consistency of PA.
He started with propositional logic and his goal was to prove its consistency. He did not want to use model theoretic methods, as here the model is very easy. He wanted instead to provide a method by analyzing proofs and generalize this method to analysis or arithmetic to prove consistency.

Why Proof Theory?

Proof theory: syntactic study of proofs represented as formal mathematical objects.
We focus here on one of its major areas: structural proof theory.

Advantages of proof theory:

- proving consistency (originally);
- proof mining: extracting information from a proof.
  Example: $\forall x \exists y A(x, y)$.
- decidability;
- proving logical properties: disjunction property, admissible rules, interpolation.

Outline

1. Propositional Logic
2. Hilbert System
3. Natural Deduction
4. Sequent Calculus
5. Cut Elimination
6. Applications of Cut Elimination

1 Propositional Logic

2 Hilbert System

3 Natural Deduction

4 Sequent Calculus

5 Cut Elimination

6 Applications of Cut Elimination

Propositional Logic

Language:

$$A := \bot \mid p \mid A \wedge A \mid A \vee A \mid A \to A \quad \text{where } p \in Prop = \{p, q, \ldots\}$$

$\neg A$ is defined as $A \to \bot$ and $\top$ as $\bot \to \bot$.

Semantics:

A valuation function is a mapping $v : Prop \to \{0, 1\}$ which can be extended to all formulas:

- $v(\bot) := 0$;
- $v(A \wedge B) = 1$ iff $v(A) = 1$ and $v(B) = 1$;
- $v(A \vee B) = 1$ iff $v(A) = 1$ or $v(B) = 1$;
- $v(A \to B) = 1$ iff $v(A) = 0$ or $v(B) = 1$.

Classical propositional logic (CPC): the set of all valid formulas.

Constructive Reasoning

To prove the existence of a mathematical object, we have to "construct" a specific example of it ("proof by contradiction" not acceptable).

Example

Theorem. There exist two irrational numbers x, y such that x^y is rational.

Proof (*nonconstructive*). Consider $\sqrt{2}$. Either $\sqrt{2}^{\sqrt{2}}$ is rational or irrational.

1. If $\sqrt{2}^{\sqrt{2}}$ is rational, take $x = y = \sqrt{2}$.
2. If $\sqrt{2}^{\sqrt{2}}$ is irrational, take $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$, because $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = 2$.

Proof (*constructive*). Take $x = e$ and $y = \ln 2$. Both of them are irrational and we have $e^{\ln 2} = 2$.

BHK-interpretation

Intuitionistic propositional logic (IPC): the logic of constructive reasoning.

An interpretation of the logical connectives in intuitionistic logic: the proof-interpretation, called the Brouwer-Heyting-Kolmogorov (BHK)-interpretation.

- $\bot$ has no proof.
- A proof of $A \wedge B$ is a pair such that the first element is a proof of A and the second one is a proof of B.
- A proof of $A \vee B$ is either a proof of A or a proof of B.
- A proof of $A \rightarrow B$ is a construction that transforms any proof of A to a proof of B.
  (special case: a proof of $\neg A$ is a construction that transforms any hypothetical proof of A to a proof of $\bot$.)

Formalism of Proofs

We are concerned with formalizing the notion of proof. Considering propositional classical and intuitionistic logics, there are three well-known kinds of formalism:

- Hilbert system (Hilbert calculus)
- natural deduction
- sequent calculus (or Gentzen's calculus)

1. Propositional Logic
2. Hilbert System
3. Natural Deduction
4. Sequent Calculus
5. Cut Elimination
6. Applications of Cut Elimination

Hilbert Proof System

Hilbert system: an axiomatization with axioms and rules of inference. The Hilbert system **HJ** for IPC has the following axioms:

1. $A \to (B \to A)$
2. $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$
3. $A \to A \vee B$
4. $B \to A \vee B$
5. $(A \to C) \to ((B \to C) \to (A \vee B \to C))$
6. $A \wedge B \to A$
7. $A \wedge B \to B$
8. $A \to (B \to (A \wedge B))$
9. $\bot \to A$

and the modus ponens rule:

$$\frac{A \qquad A \to B}{B}\,(MP)$$

Proof in Hilbert System

Hilbert system **HK** for CPC: **HJ** plus an addition axiom

$$\neg\neg A \to A \qquad \text{(law of double negation)}$$

Equivalently, we could take the law of excluded middle: $A \vee \neg A$.

Deduction from assumptions

By a *proof (deduction)* of A from a set of assumptions Γ, denoted by $\Gamma \vdash_{\mathbf{HJ}} A$, we mean a sequence of formulas $A_1, \ldots, A_n$ such that: $A_n = A$ and each A_i is either an element of Γ, or is an instance of an axiom, or is derived from A_j and A_k for $j, k < i$ by the modus ponens rule. Similarly we define $\Gamma \vdash_{\mathbf{HK}} A$.

Example

The example presents a proof of $A \to A$ in **HJ**, using the following axioms:

$$A \to (B \to A) \quad (H1)$$

$$(A \to (B \to C)) \to ((A \to B) \to (A \to C)) \quad (H2)$$

Example

1	$A \to ((A \to A) \to A)$	$(H1)$
2	$A \to ((A \to A) \to A) \to ((A \to (A \to A)) \to (A \to A))$	$(H2)$
3	$(A \to (A \to A)) \to (A \to A)$	$1, 2, MP$
4	$A \to (A \to A)$	$(H1)$
5	$A \to A$	$3, 4, MP$

Drawbacks of Hilbert System

Hilbert systems are not useful for proof search.

Example: Show that $\perp$ cannot be derived in **HJ**, i.e., it is consistent. (Hilbert's program in a toy model)

- Suppose $\perp$ is provable and $A_1, \ldots, A_n$ is its proof. Therefore, $A_n = \perp$.
- As $\perp$ is not an axiom, the last step of the proof is MP. It means that there is a formula A such that both A and $A \to \perp$ are proved.
- Now, either A is an axiom and we analyze the proof of $A \to \perp$, or A is derived from B and $B \to A$ using MP. Either B is an axiom or it is derived via MP ...
- In a backward proof search, each time that we reach MP, a new formula appears.

Remarks on Hilbert Systems

▸ Weakness of Hilbert system is not on the positive side, i.e., in the sense of proving theorems. After proving some (and not many) metatheorems (this is the hard part), we can prove theorems rather quickly.

Some common metatheorems:

- The deduction theorem: $\Gamma, A \vdash B$ if and only if $\Gamma \vdash A \rightarrow B$
- Contraposition: If $\Gamma, A \vdash B$ then $\Gamma, \neg B \vdash \neg A$

▸ The problem appears when you want to prove a formula is not provable. Then you have to consider all the proofs, and as we observed, guessing the structure of the proof is a very combinatorially complicated task.

Gentzen designs other systems

Hilbert systems help us to understand the notion of proof. However, Gentzen observed that Hilbert systems are not useful in achieving the goal of proving consistency.
Therefore, he introduced two other proof systems to study proofs systematically. Being in a transparent context, they are regarded as elegant systems.
These two systems are natural deduction and sequent calculi.

1. Propositional Logic
2. Hilbert System
3. **Natural Deduction**
4. Sequent Calculus
5. Cut Elimination
6. Applications of Cut Elimination

Natural Deduction

Proof trees in a natural deduction system have the following properties:

- nodes are labelled by formulas;
- leaf nodes are *assumptions* and the root node is the *conclusion*;
- assumptions are either *open* or *closed*; we use the notation $[A]$ for a closed assumption. Intuitively it means ...

Inductively define ND proof trees:

- a single node tree labelled by A is a proof tree, and
- new trees are constructed using the rules of ND.

Natural Deduction for IPC, **NJ**

$$\frac{\begin{array}{c}\mathcal{D}_1\\ A\end{array}\qquad\begin{array}{c}\mathcal{D}_2\\ B\end{array}}{A \wedge B}\,(I\wedge)\qquad \frac{\begin{array}{c}\mathcal{D}\\ A \wedge B\end{array}}{A}\,(E\wedge_1)\qquad \frac{\begin{array}{c}\mathcal{D}\\ A \wedge B\end{array}}{B}\,(E\wedge_2)$$

$$\frac{\begin{array}{c}[A]^i\\ \mathcal{D}\\ B\end{array}}{A \rightarrow B}\,i\;(I\rightarrow)\qquad \frac{\begin{array}{c}\mathcal{D}_1\\ A\end{array}\qquad\begin{array}{c}\mathcal{D}_2\\ A \rightarrow B\end{array}}{B}\,(E\rightarrow)$$

$$\frac{\begin{array}{c}\mathcal{D}\\ A\end{array}}{A \vee B}\,(I\vee_1)\qquad \frac{\begin{array}{c}\mathcal{D}\\ B\end{array}}{A \vee B}\,(I\vee_2)\qquad \frac{\begin{array}{c}\mathcal{D}\\ A \vee B\end{array}\qquad\begin{array}{c}[A]^i\\ \mathcal{D}_1\\ C\end{array}\qquad\begin{array}{c}[B]^j\\ \mathcal{D}_2\\ C\end{array}}{C}\,i,j\;(E\vee)$$

$$\frac{\begin{array}{c}\mathcal{D}\\ \bot\end{array}}{A}\,(\bot)$$

Natural Deduction for CPC, **NK**

$$\dfrac{\begin{matrix}\mathcal{D}_1 & \qquad & \mathcal{D}_2\\ A & & B\end{matrix}}{A \wedge B}\,(I\wedge) \qquad \dfrac{\begin{matrix}\mathcal{D}\\ A \wedge B\end{matrix}}{A}\,(E\wedge_1) \qquad \dfrac{\begin{matrix}\mathcal{D}\\ A \wedge B\end{matrix}}{B}\,(E\wedge_2)$$

$$\dfrac{\begin{matrix}[A]^i\\ \mathcal{D}\\ B\end{matrix}}{A \rightarrow B}\,i\;(I\rightarrow) \qquad \dfrac{\begin{matrix}\mathcal{D}_1 & \qquad & \mathcal{D}_2\\ A & & A \rightarrow B\end{matrix}}{B}\,(E\rightarrow)$$

$$\dfrac{\begin{matrix}\mathcal{D}\\ A\end{matrix}}{A \vee B}\,(I\vee_1) \qquad \dfrac{\begin{matrix}\mathcal{D}\\ B\end{matrix}}{A \vee B}\,(I\vee_2) \qquad \dfrac{\begin{matrix} & \qquad & [A]^i & \qquad & [B]^j\\ \mathcal{D} & & \mathcal{D}_1 & & \mathcal{D}_2\\ A \vee B & & C & & C\end{matrix}}{C}\,i,j\;(E\vee)$$

$$\dfrac{\begin{matrix}\mathcal{D}\\ \bot\end{matrix}}{A}\,(\bot) \qquad \dfrac{\begin{matrix}[\neg A]^i\\ \mathcal{D}\\ \bot\end{matrix}}{A}\,i\;(RAA)$$

Notes on **NJ** and **NK**

- The rule $(\bot)$ is called the *intuitionistic absurdity* rule.
- The rule (RAA) is called the *classic absurdity* rule (reductio ad absurdum). This rule embodies proofs by contradiction. It says that if by assuming that A is false we can derive a contradiction, then A must be true.
- Natural deduction systems **NJ** and **NK** that Gentzen introduced are a bit different. They are the same as the ones introduced here except that $\neg$ is treated as a primitive and there are two additional rules:

$$\dfrac{\begin{array}{c}[A]^i\\ \mathcal{D}\\ \bot\end{array}}{\neg A}\,i\ (I\neg) \qquad \dfrac{\begin{array}{c}\mathcal{D}_1\\ A\end{array}\qquad\begin{array}{c}\mathcal{D}_2\\ \neg A\end{array}}{\bot}\ (E\neg)$$

They reduce to $(I \rightarrow)$ and $(E \rightarrow)$ if $\neg A$ is defined.

Proofs in Natural Deduction

Definition

Derivation $\Gamma \vdash_{\mathbf{NK}} A$ means that there is a proof tree whose open assumptions are among Γ and the root is A.

Theorem

H[**JK**] *and* **N**[**JK**] *are equivalent, i.e.,*

$$\Gamma \vdash_{\mathbf{H}[\mathbf{JK}]} A \qquad \textit{if and only if} \qquad \Gamma \vdash_{\mathbf{N}[\mathbf{JK}]} A.$$

Proof.

Left to right: we have to show all axioms of **HJ** and the modus ponens rule are provable in **NJ**. □

Proof of the equivalence of **HJ** and **NJ**

Proof.

As an example, we will prove $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[A \to (B \to C)]^1 \qquad [A]^2}{B \to C}\,{\scriptstyle (E\to)} \qquad \dfrac{[A]^2 \qquad [A \to B]^3}{B}\,{\scriptstyle (E\to)}}{C}\,{\scriptstyle (E\to)}}{A \to C}\,{\scriptstyle 2\ (I\to)}}{(A \to B) \to (A \to C)}\,{\scriptstyle 3\ (I\to)}}{(A \to (B \to C)) \to ((A \to B) \to (A \to C))}\,{\scriptstyle 1\ (I\to)}$$

□

Proof of the equivalence of **HJ** and **NJ**

Proof.

As an example, we will prove $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[(A \to (B \to C))]^1 \qquad [A]^2}{B \to C}\,(E \to) \qquad \dfrac{[A]^2 \qquad [(A \to B)]^3}{B}\,(E \to)}{C}\,(E \to)}{A \to C}\,2\ (I \to)}{(A \to B) \to (A \to C)}\,3\ (I \to)}{(A \to (B \to C)) \to ((A \to B) \to (A \to C))}\,1\ (I \to)$$

As for the other direction, to prove every proof π in **NJ** is a proof in **HJ**, we use induction on the height of π. □

Example

Example

A proof tree in **NJ** for $(\neg A \vee B) \rightarrow (A \rightarrow B)$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[A]^1 \qquad [\neg A]^2}{\bot}\,(E \rightarrow)}{B}\,(\bot) \qquad [B]^3 \qquad [\neg A \vee B]^4}{B}\,2,3\ (E \vee)}{A \rightarrow B}\,1\ (I \rightarrow)}{(\neg A \vee B) \rightarrow (A \rightarrow B)}\,4\ (I \rightarrow)$$

Example

Example

A proof trees in **NK** for $\neg\neg A \to A$:

$$\dfrac{\dfrac{\dfrac{[\neg\neg A]^1 \qquad [\neg A]^2}{\bot}\,(E \to)}{A}\,2\ (RAA)}{\neg\neg A \to A}\,1\ (I \to)$$

Exercise

Prove the following formulas in **NK**:

- $A \vee \neg A$
- $((A \to B) \to A) \to A$ (Peirce law)

Hilbert System vs. Natural Deduction

- Hilbert systems:
  - not useful for proof search;
  - it is difficult to use them for reasoning about reasoning;
  - they do not tell us much about the meaning of the logical symbols.
- Natural deduction:
  - the introduction and elimination rules are in harmony;
  - the rules convey the meaning of the logical symbols;
  - proof search is still difficult because too many proofs are allowed.

  Example:

$$\dfrac{\dfrac{\dfrac{[A]^1 \qquad [A]^1}{A \wedge A}}{A}}{A \to A}\,{}^{1} \qquad\qquad \dfrac{[A]^1}{A \to A}\,{}^{1}$$

Consistency via ND

The goal of introducing natural deduction was to prove the consistency of propositional logic. Does it help?

- Suppose $\bot$ is proved in **NJ**.
- Looking at the last rule of the proof, here are several possibilities: it is possible that the last rule is $(E\rightarrow)$ and A and $A \rightarrow \bot$ are proved. Or the last rule can be $(E\wedge)$ and $A \wedge \bot$ is proved, and so on.

This is more complex than Hilbert system! The situation has become worse, as in Hilbert system we had to only deal with MP, while in natural deduction there are several possibilities. Gentzen had some ideas...

Redundancies

Gentzen's idea: Avoid redundancies in a proof.

- β-reduction: introducing a connective and immediately in the next step eliminating it.

$$\dfrac{\dfrac{\begin{matrix}\mathcal{D}_1\\ A\end{matrix} \qquad \begin{matrix}\mathcal{D}_2\\ B\end{matrix}}{A \wedge B}}{A} \qquad \rightsquigarrow \qquad \begin{matrix}\mathcal{D}_1\\ A\end{matrix}$$

$$\dfrac{\dfrac{\begin{matrix}[A]^1\\ \mathcal{D}\\ B\end{matrix}}{A \to B}{\scriptstyle 1} \qquad \begin{matrix}\mathcal{D}'\\ A\end{matrix}}{B} \qquad \rightsquigarrow \qquad \begin{matrix}\mathcal{D}'\\ A\\ \mathcal{D}\\ B\end{matrix}$$

Redundancies

$$\dfrac{\dfrac{\begin{matrix}\mathcal{D}\\ A\end{matrix}}{A \vee B} \qquad \begin{matrix}[A]^1\\ \mathcal{D}_1\\ C\end{matrix} \qquad \begin{matrix}[B]^2\\ \mathcal{D}_2\\ C\end{matrix}}{C}\,{\scriptstyle 1,2} \qquad \rightsquigarrow \qquad \begin{matrix}\mathcal{D}\\ A\\ \mathcal{D}_1\\ C\end{matrix}$$

$$\dfrac{\dfrac{\begin{matrix}\mathcal{D}\\ B\end{matrix}}{A \vee B} \qquad \begin{matrix}[A]^1\\ \mathcal{D}_1\\ C\end{matrix} \qquad \begin{matrix}[B]^2\\ \mathcal{D}_2\\ C\end{matrix}}{C}\,{\scriptstyle 1,2} \qquad \rightsquigarrow \qquad \begin{matrix}\mathcal{D}\\ B\\ \mathcal{D}_2\\ C\end{matrix}$$

Normalization

Normalization is omitting all the redundancies in a proof. The resulting proof is a *normal* proof.
It is not trivial to see that this task is possible for any given proof (it may be the case that two introduction elimination rules are not after each other, but in the steps of omitting the redundancies, these two rules become after one another. So, new redundancies may appear.)

η-equivalence

β-reduction gives rise to an equivalence between proofs called β-equivalence. There is another notion of equivalence, called η-equivalence.

$$\eta : \quad \dfrac{\dfrac{\begin{matrix}\mathcal{D}\\ A \wedge B\end{matrix}}{A} \qquad \dfrac{\begin{matrix}\mathcal{D}\\ A \wedge B\end{matrix}}{B}}{A \wedge B} \qquad\qquad \dfrac{\dfrac{\begin{matrix}\mathcal{D}\\ A \to B\end{matrix} \qquad [A]^1}{B}}{A \to B}\,1$$

- η-equivalence is complicated in some cases and not useful for our purposes.
- An example of η-reduction: first eliminating and immediately introducing.
- η-equivalence for $\perp$: any two derivations of a formula A from $\perp$ are considered to be equivalent.

Does normalization solve our problem?

Suppose we have proved the normalization theorem, i.e., it is possible to make any proof normal. So, we are sure that if a formula is provable, there exists a finite and algorithmic process that takes a proof and makes it normal such that it does not contain any β-redex. Now, can we prove the consistency?

Theorem

Every normal proof, without any open assumptions, ends with an introduction rule.

Proof of consistency via normalization

Proof.

Suppose on the contrary that there are normal proofs ending with an elimination rule. Take the shortest such proof. We investigate all the possibilities of elimination rules in the last step. For instance, if it is $E\wedge$, then as the proof above it is shorter, then it must end with an introduction rule. This is not possible: (introduction, elimination), as our proof was normal. □

Proof of consistency is immediate after the above theorem. Also proof of DP in intuitionistic logic.

Moving to Sequent Calculi

Recall that Gentzen's goal was to efficiently study the form of the proof and ND is one such system, up to normalization. We will define the next system that Gentzen introduced, sequent calculi.

1. Propositional Logic
2. Hilbert System
3. Natural Deduction
4. **Sequent Calculus**
5. Cut Elimination
6. Applications of Cut Elimination

Sequents

Sequents are expressions of the form

$$\Gamma \Rightarrow \Delta$$

where Γ and Δ are finite multisets of formulas called the *antecedent* and the *succedent* of the sequent, respectively. The formula interpretation, I, corresponding to the above sequent is $\bigwedge \Gamma \to \bigvee \Delta$.
Convention: $\bigwedge \varnothing = \top$ and $\bigvee \varnothing = \bot$.

Example

The formula interpretation of the sequent $p, q \to r, q \to r \Rightarrow s, \neg q$ is $(p \wedge (q \to r) \wedge (q \to r)) \to (s \vee \neg q)$.
Moreover, $I(A \Rightarrow) = A \to \bot = \neg A$ and $I(\Rightarrow A) = \top \to A$, which is equivalent to A.

Sequent calculus

A rule is an expression of the form

$$\frac{S_1 \qquad \dots \qquad S_n}{S}$$

where $S_1, \dots, S_n$ and S are sequents called the *premises* and the *conclusion* of the rule, respectively.

A *sequent Calculus* (also called a Gentzen system or a Gentzen calculus) is a set of rules.

Sequent Calculus **G3c** for CPC

Axioms

$$\Gamma, A \Rightarrow A, \Delta \qquad \Gamma, \bot \Rightarrow \Delta$$

Logical rules

$$\frac{\Gamma, A, B \Rightarrow \Delta}{\Gamma, A \wedge B \Rightarrow \Delta}\,(L\wedge) \qquad \frac{\Gamma \Rightarrow A, \Delta \qquad \Gamma \Rightarrow B, \Delta}{\Gamma \Rightarrow A \wedge B, \Delta}\,(R\wedge)$$

$$\frac{\Gamma, A \Rightarrow \Delta \qquad \Gamma, B \Rightarrow \Delta}{\Gamma, A \vee B \Rightarrow \Delta}\,(L\vee) \qquad \frac{\Gamma \Rightarrow A, B, \Delta}{\Gamma \Rightarrow A \vee B, \Delta}\,(R\vee)$$

$$\frac{\Gamma \Rightarrow A, \Delta \qquad \Gamma, B \Rightarrow \Delta}{\Gamma, A \rightarrow B \Rightarrow \Delta}\,(L \rightarrow) \qquad \frac{\Gamma, A \Rightarrow B, \Delta}{\Gamma \Rightarrow A \rightarrow B, \Delta}\,(R \rightarrow)$$

The cut rule

$$\frac{\Gamma \Rightarrow A, \Delta \qquad \Gamma', A \Rightarrow \Delta'}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'}\,(cut)$$

Sequent Calculus for CPC

Axioms

$$\Gamma, A \Rightarrow A, \Delta \qquad \Gamma, \bot \Rightarrow \Delta$$

Logical rules

$$\frac{\Gamma, A, B \Rightarrow \Delta}{\Gamma, A \wedge B \Rightarrow \Delta}\ (L\wedge) \qquad \frac{\Gamma \Rightarrow A, \Delta \qquad \Gamma \Rightarrow B, \Delta}{\Gamma \Rightarrow A \wedge B, \Delta}\ (R\wedge)$$

$$\frac{\Gamma, A \Rightarrow \Delta \qquad \Gamma, B \Rightarrow \Delta}{\Gamma, A \vee B \Rightarrow \Delta}\ (L\vee) \qquad \frac{\Gamma \Rightarrow A, B, \Delta}{\Gamma \Rightarrow A \vee B, \Delta}\ (R\vee_1)$$

$$\frac{\Gamma \Rightarrow A, \Delta \qquad \Gamma, B \Rightarrow \Delta}{\Gamma, A \rightarrow B \Rightarrow \Delta}\ (L \rightarrow) \qquad \frac{\Gamma, A \Rightarrow B, \Delta}{\Gamma \Rightarrow A \rightarrow B, \Delta}\ (R \rightarrow)$$

The cut rule

$$\frac{\Gamma \Rightarrow A, \Delta \qquad \Gamma', A \Rightarrow \Delta'}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'}\ (cut)$$

Sequent Calculus **G3i** for IPC

Axioms

$$\Gamma, A \Rightarrow A \qquad \Gamma, \bot \Rightarrow \Delta$$

Logical rules

$$\frac{\Gamma, A, B \Rightarrow \Delta}{\Gamma, A \wedge B \Rightarrow \Delta}\,(L\wedge) \qquad \frac{\Gamma \Rightarrow A \qquad \Gamma \Rightarrow B}{\Gamma \Rightarrow A \wedge B}\,(R\wedge)$$

$$\frac{\Gamma, A \Rightarrow \Delta \qquad \Gamma, B \Rightarrow \Delta}{\Gamma, A \vee B \Rightarrow \Delta}\,(L\vee) \qquad \frac{\Gamma \Rightarrow A}{\Gamma \Rightarrow A \vee B}\,(R\vee) \qquad \frac{\Gamma \Rightarrow B}{\Gamma \Rightarrow A \vee B}\,(R\vee)$$

$$\frac{\Gamma, A \rightarrow B \Rightarrow A \qquad \Gamma, B \Rightarrow \Delta}{\Gamma, A \rightarrow B \Rightarrow \Delta}\,(L\rightarrow) \qquad \frac{\Gamma, A \Rightarrow B}{\Gamma \Rightarrow A \rightarrow B}\,(R\rightarrow)$$

The cut rule

$$\frac{\Gamma \Rightarrow A \qquad \Gamma', A \Rightarrow \Delta'}{\Gamma, \Gamma' \Rightarrow \Delta'}\,(cut)$$

Notes on Sequent Calculi

- Original sequent calculi for CPC and IPC introduced by Gentzen, denoted by **LK** and **LJ**, respectively, (also called **G1** calculi) were defined using sequences of formulas instead of multisets. In these systems roles of structural rules and logical rules are kept distinct. In **G3** style, the structural rules are absorbed into the logical rules. (**G2** calculi are intermediate ones, where the weakening rules are built in.)

Structural rules:

$$\frac{\Gamma \Rightarrow \Delta}{\Gamma, A \Rightarrow \Delta}\,(Lw) \qquad \frac{\Gamma \Rightarrow \Delta}{\Gamma \Rightarrow A, \Delta}\,(Rw)$$

$$\frac{\Gamma, A, A \Rightarrow \Delta}{\Gamma, A \Rightarrow \Delta}\,(Lc) \qquad \frac{\Gamma \Rightarrow A, A\Delta}{\Gamma \Rightarrow A\Delta}\,(Rc)$$

$$\frac{\Gamma, A, B, \Sigma \Rightarrow \Delta}{\Gamma, B, A, \Sigma \Rightarrow \Delta}\,(Le) \qquad \frac{\Gamma, \Rightarrow \Delta, A, B, \Pi}{\Gamma \Rightarrow \Delta, B, A, \Pi}\,(Re)$$

Notes on Sequent Calculi (Cont.)

- There are several variants of sequent calculi, no variants preferable over others; choose one suitable for your purpose.
- There are three types of formulas in the rules of the sequent calculus:
  - *Principal*: The formula introduced in conclusion
  - *Auxiliary*: The formula(s) mentioned in the premise(s)
  - *Side*: The formulas in Γ and Δ

Proofs in Sequent Calculi

Proofs in sequent calculi are finite trees labelled with sequents such that:

- there is one root, labelled with the result of the proof (called endsequent or conclusion of the proof);
- labels of the leaves are axioms;
- all the other nodes are labelled and connected to the immediate successors with respect to one of the rules of the sequent calculus.

Example I

Example

Sequent $(\Rightarrow A \to ((A \to B) \to B))$ is derivable in both **G3c** and **G3i**:

$$\dfrac{\dfrac{\dfrac{A \Rightarrow A \qquad B \Rightarrow B}{A, A \to B \Rightarrow B}\,(L \to)}{A \Rightarrow (A \to B) \to B}\,(R \to)}{\Rightarrow A \to ((A \to B) \to B)}\,(R \to)$$

Exercise

Provide proofs for the sequents $(\Rightarrow A \vee \neg A)$ and $(\Rightarrow \neg\neg A \to A)$ and $(\neg A \vee B \Rightarrow A \to B)$ in **G3c**.

Example II

Example

Peirce's law is provable in **G3c**:

$$\dfrac{\dfrac{\dfrac{A \Rightarrow A, B}{\Rightarrow A, A \to B}\,(R \to) \qquad A \Rightarrow A}{(A \to B) \to A \Rightarrow A}\,(L \to)}{\Rightarrow ((A \to B) \to A) \to A}\,(R \to)$$

Exercise

Show that if we allow sequents in the sequent calculus to have at most one formula in the succedent, Peirce's law cannot be provable.

The importance of the cut rule

- We have included the cut rule in the sequent calculi, and we will show it can be eliminated from the calculi. Why include it in the first place?
- The cut rule is useful to prove the soundness and completeness of the sequent calculi (i.e., every formula true in the logic must be provable in the system and vice versa).

Equivalence of Sequent Calculi and Hilbert Systems

Theorem

$\mathbf{H}[\mathbf{JK}]$ and $\mathbf{G3}[\mathbf{ic}]$ are equivalent, i.e.,

$$\Gamma \vdash_{\mathbf{H}[\mathbf{JK}]} A \qquad \textit{if and only if} \qquad \vdash_{\mathbf{G3}[\mathbf{ic}]} \Gamma \Rightarrow A.$$

Proof.

We will sketch the proof for the intuitionistic case.
Left to right: by induction. Hilbert axioms are provable in **G3i**. To show the provability of MP in **G3i**, suppose both $\Rightarrow A$ and $\Rightarrow A \to B$ are provable in **G3i**. □

Proof of the equivalence

Proof (continued).

The following proof serves our goal:

$$\dfrac{\dfrac{\Rightarrow A \qquad \dfrac{A \Rightarrow A \qquad B \Rightarrow B}{A, A \to B \Rightarrow B}\,(L \to)}{A \to B \Rightarrow B}\,(\mathrm{cut}) \qquad \Rightarrow A \to B}{\Rightarrow B}\,(\mathrm{cut})$$

Therefore, the cut rule is practically useful to simulate Hilbert system in the sequent calculus. The converse, that is **HJ** simulates **G3i** is easy. □

1. Propositional Logic
2. Hilbert System
3. Natural Deduction
4. Sequent Calculus
5. Cut Elimination
6. Applications of Cut Elimination

Cut is problematic

Gentzen provided this system to prove the consistency. However, we face the same problem as the one for natural deduction:

- Suppose $\Rightarrow \bot$ is proved.
- It is not an axiom. What rule can be above this sequent?
- Not a left rule, as the antecedent is empty; and not a right rule as there is no connective so that it can be introduced. The only possible rule is cut.
- The rest is similar as the investigation of the case where MP above $\bot$ in natural deduction.

Cut makes the discussion for consistency problematic. Can we eliminate this rule from the sequent calculus? Yes.

Cut elimination

Theorem

Cut elimination holds for **G3**[**ci**]*, i.e., every sequent derivable in* **G3**[**ci**] *has a derivation in* **G3**[**ci**]$-$ *Cut.*

Idea of the proof: permute cut upward until there exist no more cuts.

Definition

- *level* of a cut: sum of the depths of the derivations of its premises;
- *rank* of a cut on A is $|A| + 1$ (number of symbols in A plus one);
- *cutrank* of a derivation $\mathcal{D}$, $cr(\mathcal{D})$: maximum of the ranks of the cut formulas occurring in it.

Proof of Cut Elimination

Proof.

We use induction on the cutrank of the derivation with a subinduction on the level. Throughout the proof, we use the fact that **G3c** is closed under weakening and contraction. Consider

$$\dfrac{\begin{array}{c}\mathcal{D}_1\\ \Gamma \Rightarrow \Delta, A\end{array} \qquad \begin{array}{c}\mathcal{D}_2\\ \Gamma', A \Rightarrow \Delta'\end{array}}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'}\,(\text{cut})$$

There are three possibilities:

- at least one of $\mathcal{D}_1$ and $\mathcal{D}_2$ is an axiom;
- none of $\mathcal{D}_1$ and $\mathcal{D}_2$ is an axiom, and at least in one of the premises A is auxiliary;
- A is principal in both premises.

□

Cut formula is auxiliary

Cut formula A is auxiliary in the left premise:

$$\dfrac{\dfrac{\begin{array}{c}\mathcal{D}_1\\ \Gamma, B \Rightarrow C, A, \Delta\end{array}}{\Gamma \Rightarrow B \to C, A, \Delta} \qquad \begin{array}{c}\mathcal{D}_2\\ \Gamma', A \Rightarrow \Delta'\end{array}}{\Gamma, \Gamma' \Rightarrow B \to C, \Delta, \Delta'}\ (\mathrm{cut})$$

then it reduces to

$$\dfrac{\dfrac{\begin{array}{c}\mathcal{D}_1\\ \Gamma, B \Rightarrow C, A, \Delta\end{array} \qquad \begin{array}{c}\mathcal{D}_2\\ \Gamma', A \Rightarrow \Delta'\end{array}}{\Gamma, \Gamma', B \Rightarrow C, \Delta, \Delta'}\ (\mathrm{cut})}{\Gamma, \Gamma' \Rightarrow B \to C, \Delta, \Delta'}$$

- Cutrank is the same; level of the cut is lower.
- We permute the cut upwards.

Cut formula is principal

Suppose the cut formula is $A \wedge B$ and it is principal in both premises:

$$\dfrac{\dfrac{\begin{matrix}\mathcal{D}_1\\ \Gamma \Rightarrow A, \Delta\end{matrix} \qquad \begin{matrix}\mathcal{D}_2\\ \Gamma \Rightarrow B, \Delta\end{matrix}}{\Gamma \Rightarrow A \wedge B, \Delta} \qquad \dfrac{\begin{matrix}\mathcal{D}_3\\ A, B, \Gamma' \Rightarrow \Delta'\end{matrix}}{A \wedge B, \Gamma' \Rightarrow \Delta'}}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'}\,(\text{cut})$$

will be replaced by

$$\dfrac{\begin{matrix}\mathcal{D}_1\\ \Gamma \Rightarrow A, \Delta\end{matrix} \qquad \dfrac{\begin{matrix}\mathcal{D}_2\\ \Gamma \Rightarrow B, \Delta\end{matrix} \qquad \begin{matrix}\mathcal{D}_3\\ A, B, \Gamma' \Rightarrow \Delta'\end{matrix}}{\Gamma, \Gamma', A \Rightarrow \Delta, \Delta'}\,(\text{cut})}{\Gamma, \Gamma, \Gamma' \Rightarrow \Delta, \Delta, \Delta'}\,(\text{cut})$$

- Cutrank of the second proof tree is lower.
- **G3c** is closed under contraction, so we get $\Gamma, \Gamma' \Rightarrow \Delta, \Delta'$.

On the importance of **G3**-style systems

Suppose the contraction rules are explicitly present in the system. Consider the case:

$$\dfrac{\dfrac{\Gamma, A, A \Rightarrow \Delta}{\Gamma, A \Rightarrow \Delta} \qquad \Gamma' \Rightarrow A}{\Gamma, \Gamma' \Rightarrow \Delta}\ (\text{cut})$$

How do we eliminate the cut in this case? Possibly:

$$\dfrac{\dfrac{\Gamma, A, A \Rightarrow \Delta \qquad \Gamma' \Rightarrow A}{\Gamma, \Gamma', A \Rightarrow \Delta}\ (\text{cut}) \qquad \Gamma' \Rightarrow A}{\Gamma, \Gamma', \Gamma' \Rightarrow \Delta}\ (\text{cut})$$

Neither the cutrank, nor the level of the cut is lower than the original derivation. (A derivable generalization of cut is introduced: multi-cut or mix, that allows eliminating several copies of the cut formula in one step.)

Complexity of Cut-elimination

Define $2_0^i := i$ and $2_{k+1}^i := 2^{2_k^i}$. Similarly define 4_k^i.

Theorem (Hyperexponential bounds on cut elimination)

For every derivation $\mathcal{D}$ in $G3c + cut$ or $G3i + cut$ with cutrank k, there exists a cut free derivation $\mathcal{D}^*$ with the same conclusion as the one in $\mathcal{D}$ such that

$$|\mathcal{D}^*| \leqslant 2_k^{|\mathcal{D}|} \quad \text{for } G3c \qquad \text{and} \qquad |\mathcal{D}^*| \leqslant 4_k^{|\mathcal{D}|} \quad \text{for } G3i$$

1. Propositional Logic

2. Hilbert System

3. Natural Deduction

4. Sequent Calculus

5. Cut Elimination

6. Applications of Cut Elimination

Applications of Cut Elimination

In fact, applications of a cut-free proof system.

- *Consistency*: $(\Rightarrow \bot)$ is not derivable in either **G3**[**ci**]. immediate!
  Corollary: IPC and CPC are consistent.

Applications of Cut Elimination

- in an intuitionistic setting:
  Disjunction property: if $(\Rightarrow A \vee B)$ is provable, then either $(\Rightarrow A)$ or $(\Rightarrow B)$ is provable; or more generally:
  Visser's admissible rules: if **G3i** $\vdash \{A_i \to B_i\}_{i \in I} \Rightarrow B \vee C$ then one of the following is provable:
  - **G3i** $\vdash \{A_i \to B_i\}_{i \in I} \Rightarrow B$, or
  - **G3i** $\vdash \{A_i \to B_i\}_{i \in I} \Rightarrow C$, or
  - **G3i** $\vdash \{A_i \to B_i\}_{i \in I} \Rightarrow A_i$, for some $i \in I$.

  Corollary: IPC enjoys DP and admissibility of Visser's rules.

Applications of Cut Elimination

- **G3**[**ci**] are terminating; *proof search*. Termination implies the decidability of a logic. Not only it proves the decidability, but also if it is provable, it constructs the proof.
  Corollary: CPC and IPC are *decidable*, i.e., there is an algorithm that reads a formula A and determines whether A is logically valid or not. Moreover, using the cut-free systems, if A is valid the algorithm outputs a proof of it.

Applications of Cut Elimination

- *Subformula Property*: every derivable sequent has a derivation in which all the formulas throughout the proof are subformulas of formulas of the endsequent. Eliminating the cut rule gives us more control over the presence of formulas. (**G3**[**ci**] have subformula property, which is immediate by inspection of the rules.)

Applications of Cut Elimination (Interpolation)

- *Interpolation:*

Definition

Craig interpolation property for a logic L: if $L \vdash A \to B$, then there exists a formula $I(A, B)$, such that $var(I) \subseteq var(A) \cap var(B)$ and moreover $L \vdash A \to I$ and $L \vdash I \to B$.

Theorem

IPC *and* CPC *enjoy the Craig interpolation property.*

We will consider **G3c**. Main idea: split sequents, due to Maehara.

Definition

For a sequent $\Gamma \Rightarrow \Delta$ a *split sequent* (also called *partition*) is an expression $\Gamma_1; \Gamma_2 \Longrightarrow \Delta_1; \Delta_2$ such that $\Gamma_1, \Gamma_2 = \Gamma$ and $\Delta_1, \Delta_2 = \Delta$.

Definition

Let $\Gamma \Rightarrow \Delta$ be a provable sequent and $\Gamma_1; \Gamma_2 \Longrightarrow \Delta_1; \Delta_2$ be one of its split sequents. We say I is an *interpolant* for $\Gamma_1; \Gamma_2 \Longrightarrow \Delta_1; \Delta_2$ if

- $\Gamma_1 \Rightarrow \Delta_1, I$ and $\Gamma_2, I \Rightarrow \Delta_2$, and
- $var(I) \subseteq var(\Gamma_1 \cup \Delta_1) \cap var(\Gamma_2 \cup \Delta_2)$

In **G3c**:

Theorem

Let $\Gamma \Rightarrow \Delta$ *be provable. If* $\Gamma_1 ; \Gamma_2 \Longrightarrow \Delta_1 ; \Delta_2$ *is an split sequent for it, then there exists an interpolant for it.*

Proof.

By induction on the length of the cut-free proofs in **G3c**. We consider the last rule used in the proof and show how to construct an interpolant for a partition of the conclusion from the interpolants of suitable partitions of the premises. □

Corollary

CPC *enjoys Craig interpolation.*

Proof.

Last rule: $(L \rightarrow)$. Two cases based on the position of the principal formula:

$$\frac{\Gamma; \Gamma' \Longrightarrow \Delta A; \Delta' \qquad \Gamma'; B\Gamma \Longrightarrow \Delta'; \Delta}{\Gamma(A \rightarrow B); \Gamma' \Longrightarrow \Delta; \Delta'}$$

□

Proof.

Last rule: $(L \to)$. Two cases based on the position of the principal formula:

$$\frac{\Gamma; \Gamma' \overset{D}{\Longrightarrow} \Delta A; \Delta' \qquad \Gamma'; B\Gamma \overset{C}{\Longrightarrow} \Delta'; \Delta}{\Gamma(A \to B); \Gamma' \xRightarrow{C \to D} \Delta; \Delta'}$$

Proof.

Last rule: $(L \to)$. Two cases based on the position of the principal formula:

$$\frac{\Gamma; \Gamma' \xRightarrow{D} \Delta A; \Delta' \qquad \Gamma'; B\Gamma \xRightarrow{C} \Delta'; \Delta}{\Gamma(A \to B); \Gamma' \xRightarrow{C \to D} \Delta; \Delta'}$$

By IH:

- $\Gamma \Rightarrow D, A, \Delta \quad (1)$ and $\quad \Gamma', D \Rightarrow \Delta' \quad (2)$.
- $\Gamma' \Rightarrow C, \Delta' \quad (3)$ and $\quad \Gamma, C, B \Rightarrow \Delta \quad (4)$.

By (1) and (4) we get $\Gamma, A \to B \Rightarrow C \to D, \Delta$ and by (2) and (3) we get $\Gamma', C \to D \Rightarrow \Delta'$. Variable check is easy. □

Exercise

Show that this method does not work for **G3i** to prove the Craig interpolation property. (Hint: think about partitions of the axioms.)

Thank you!