Complétude en logiques

Habilitation à diriger des recherches

Olivier Hermant

MINES ParisTech, PSL Research University

2017, April 20th

Key Questions in Logics

- What is true?
- What is provable?

Key Questions in Logics

- What is true?
  - What is truth?
- What is provable?
  - What is a proof?

Key Questions in Logics

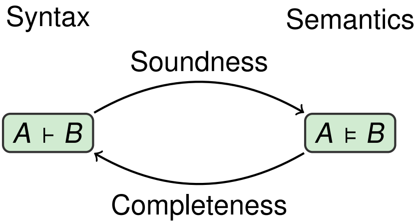
- What is true?
  - What is truth?
- What is provable?
  - What is a proof?
- Are they links between truth (semantics) and provability (syntax) ?

Logical Systems in Computer Science

- automated theorem proving [P. Halmagrand]
- proof checking [R. Saillard]
- application domain: formal methods
  - ⋆ large (mathematical) proofs
  - ⋆ safe, *bug-free*, system conception
- theory of programming languages (type systems, semantics, static analysis)
- and others: model checking, realizability, proof theory, ...

Key Properties of Logical Systems

- assume a semantics (truth notion) and a syntax (proof notion)



Theorem (Soundness)

If a statement is provable, it is (universally) true.

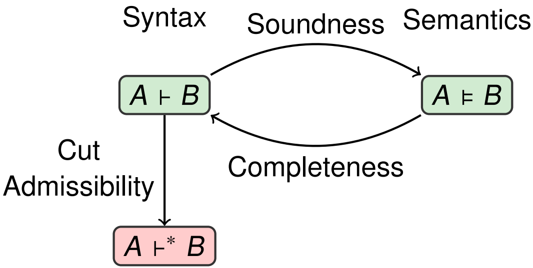
Corollary (Consistency)

Absurd statements have no proofs.

Theorem (Completeness)

If a statement is (universally) true, it is provable.

Key Properties of Logical Systems



Theorem (Cut Admissibility)

If a statement is provable, then it is provable without detour.

- consistency
- automated proof-search
- focus on computation (CS point of view):
  - proof terms
  - normalization (termination of proof-term reduction)

Outline

1. Intro
2. Playing Around (Classical Tableaux for Propositional Logic)
3. Sequent Calculus and Cut Admissibility
4. Extensions
5. Getting Rid of Tableaux
6. Opening the Box
7. Conclusion

2. Playing Around

Propositional Logic

- atomic formulas A, B, C
- connectives $\wedge, \vee, \Rightarrow, \neg, \bot, \top$
- semantics:
  - truth tables

A	B	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$\neg A$	$\bot$	$\top$
0	0	0	0	1	1	0	1
0	1	0	1	1	1	0	1
1	0	0	1	0	0	0	1
1	1	1	1	1	0	0	1

  - valuation $[\![F]\!]$ for any formula F
- syntax: a proof-search method called *the tableaux method*.

Tableaux Method in Classical Logic

- refutation-based method: to show F, derive a contradiction from $\neg F$.
- immediate contradictions (closure rule)

$$\frac{\bot}{\odot}\,\bot \qquad \frac{\neg\top}{\odot}\,\neg_\top \qquad \frac{F, \neg F}{\odot}\,\text{cl}$$

Tableaux Method in Classical Logic

- refutation-based method: to show F, derive a contradiction from $\neg F$.
- immediate contradictions (closure rule)
- conjunctive forms

$$\frac{\bot}{\odot}\ \bot \qquad \frac{\neg\top}{\odot}\ \neg_\top \qquad \frac{F, \neg F}{\odot}\ \text{cl}$$

$$\frac{A \wedge B}{A, B}\ \wedge \qquad \frac{\neg(A \vee B)}{\neg A, \neg B}\ \neg_\vee \qquad \frac{\neg(A \Rightarrow B)}{A, \neg B}\ \neg_\Rightarrow$$

Tableaux Method in Classical Logic

- refutation-based method: to show F, derive a contradiction from $\neg F$.
- immediate contradictions (closure rule)
- conjunctive forms
- disjunctive forms

$$\frac{\bot}{\odot}\,\bot \qquad \frac{\neg\top}{\odot}\,\neg_\top \qquad \frac{F, \neg F}{\odot}\,\text{cl}$$

$$\frac{A \wedge B}{A, B}\,\wedge \qquad \frac{\neg(A \vee B)}{\neg A, \neg B}\,\neg_\vee \qquad \frac{\neg(A \Rightarrow B)}{A, \neg B}\,\neg_\Rightarrow$$

$$\frac{\neg(A \wedge B)}{\neg A \quad\quad \neg B}\,\neg_\wedge \qquad \frac{A \vee B}{A \quad\quad B}\,\vee \qquad \frac{A \Rightarrow B}{A \quad\quad \neg B}\,\Rightarrow$$

Example

- prove $(B \vee A) \Rightarrow (A \vee B)$

$$\neg((B \vee A) \Rightarrow (A \vee B))$$

- tableau as a tree
- choice for rule application
- proof iff each branch is closed
- notation $F_1, \cdots, F_n \hookrightarrow \odot$

Example

- prove $(B \vee A) \Rightarrow (A \vee B)$

$$\frac{\neg((B \vee A) \Rightarrow (A \vee B))}{B \vee A, \neg(A \vee B)} \neg\Rightarrow$$

- tableau as a tree
- choice for rule application
- proof iff each branch is closed
- notation $F_1, \cdots, F_n \hookrightarrow \odot$

Example

- prove $(B \vee A) \Rightarrow (A \vee B)$

$$\dfrac{\neg((B \vee A) \Rightarrow (A \vee B))}{\dfrac{{\color{red}B \vee A}, \neg(A \vee B)}{B \qquad\qquad A}\ {\color{red}\vee}}\ \neg\Rightarrow$$

- tableau as a tree
- choice for rule application
- proof iff each branch is closed
- notation $F_1, \cdots, F_n \hookrightarrow \odot$

Example

- prove $(B \vee A) \Rightarrow (A \vee B)$

$$\cfrac{\neg((B \vee A) \Rightarrow (A \vee B))}{\cfrac{B \vee A, \neg(A \vee B)}{\cfrac{B}{\neg A, \neg B}\ \neg\vee \qquad\qquad A}\ \vee}\ \neg\Rightarrow$$

- tableau as a tree
- choice for rule application
- proof iff each branch is closed
- notation $F_1, \cdots, F_n \hookrightarrow \odot$

Example

- prove $(B \vee A) \Rightarrow (A \vee B)$

$$\cfrac{\neg((B \vee A) \Rightarrow (A \vee B))}{\cfrac{B \vee A, \neg(A \vee B)}{\cfrac{\cfrac{B}{\neg A, \neg B}\ \neg\vee}{\odot} \qquad\qquad A}\ \vee}\ \neg\Rightarrow$$

- tableau as a tree
- choice for rule application
- proof iff each branch is closed
- notation $F_1, \cdots, F_n \hookrightarrow \odot$

Example

- prove $(B \vee A) \Rightarrow (A \vee B)$

$$\dfrac{\neg((B \vee A) \Rightarrow (A \vee B))}{\dfrac{B \vee A, \neg(A \vee B)}{\dfrac{\dfrac{B}{\neg A, \neg B}\;\neg\vee}{\odot} \qquad \dfrac{A}{\neg A, \neg B}\;\neg\vee}\;\vee}\;\neg\Rightarrow$$

- tableau as a tree
- choice for rule application
- proof iff each branch is closed
- notation $F_1, \cdots, F_n \hookrightarrow \odot$

Example

- prove $(B \vee A) \Rightarrow (A \vee B)$

$$\dfrac{\neg((B \vee A) \Rightarrow (A \vee B))}{\dfrac{B \vee A, \neg(A \vee B)}{\dfrac{B}{\dfrac{\neg A, \neg B}{\odot}}\,\neg\vee \qquad \dfrac{A}{\dfrac{\neg A, \neg B}{\odot}}\,\neg\vee}\,\vee}\,\neg\Rightarrow$$

- tableau as a tree
- choice for rule application
- proof iff each branch is closed
- notation $F_1, \cdots, F_n \hookrightarrow \odot$

Soundness and Completeness

Soundness of the Tableaux Method

If there exists a closed tableau containing the formulas $F_1, \cdots, F_n$, the formula $F_1 \wedge \cdots \wedge F_n$ is unsatisfiable.

- no atomic truth value assignment makes $[\![F_1 \wedge \cdots \wedge F_n]\!] = 1$
- no model of $F_1, \cdots, F_n$
- induction on the tableau proof and case analysis
- basic concept: each rule is sound.
  Example on the $\vee$ rule. If $[\![F]\!] = 0$ and $[\![G]\!] = 0$, then $[\![F \vee G]\!] = 0$.

$$\frac{A \vee B}{A \qquad B}\ \vee$$

Completeness of Tableaux Method

- another view of tableaux rules:
  - exhaustively searching for a countermodel of F
  - refutation of F ~ a model of $\neg F$ ~ an interpretation with $[\![\neg F]\!] = 1$
- if search fails, all interpretations respect $[\![F]\!] = 1$.

$$\frac{\bot}{\odot}\ \bot \qquad \frac{\neg\top}{\odot}\ \neg_\top \qquad \frac{F, \neg F}{\odot}\ \mathrm{cl}$$

$$\frac{A \wedge B}{A, B}\ \wedge \qquad \frac{\neg(A \vee B)}{\neg A, \neg B}\ \neg_\vee \qquad \frac{\neg(A \Rightarrow B)}{A, \neg B}\ \neg_\Rightarrow$$

$$\frac{\neg(A \wedge B)}{\neg A \qquad \neg B}\ \neg_\wedge \qquad \frac{A \vee B}{A \qquad B}\ \vee \qquad \frac{A \Rightarrow B}{A \qquad \neg B}\ \Rightarrow$$

Example: Countermodel from Exhaustion

- try to prove $A \Rightarrow (A \wedge B)$

$$\cfrac{\neg(A \Rightarrow (A \wedge B))}{\cfrac{A, \neg(A \wedge B)}{\cfrac{\neg A}{\odot} \qquad \neg B}}$$

- right branch *open* and *complete*

Complete Branch

A branch of a tableau is complete if all applicable rules have been applied.

- Countermodel construction:
  - ★ collect the litterals (plain and negated atoms), A and $\neg B$,
  - ★ assign the truth values accordingly, $[\![A]\!] = 1$ and $[\![B]\!] = 0$,
  - ★ yields $[\![A \Rightarrow (A \wedge B)]\!] = 0$.
  - ★ Interpretation that falsifies $A \Rightarrow (A \wedge B)$.

Completeness Proof Sketch

Theorem (Completeness)

If a tableau with formulas $F_1, \cdots, F_n$ cannot be closed, there is an interpretation such that $[\![F_i]\!] = 1$.

- complete branch mandatory to collect the litterals
- need for a systematic proof-search algorithm

3. Sequent Calculus and Cut Admissibility

Sequent Calculus

- Sequent Calculus: a framework for reasoning [Gentzen]
- hypotheses Γ, conclusions Δ, notation $\Gamma \vdash \Delta$

$$\frac{}{\Gamma, A \vdash A, \Delta}\ \text{axiom} \qquad \frac{\Gamma \vdash A, \Delta \qquad \Gamma, A \vdash \Delta}{\Gamma \vdash \Delta}\ \text{cut}$$

$$\frac{\Gamma A, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta}\ \wedge_L \qquad \frac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \vee B, \Delta}\ \vee_R \qquad \frac{\Gamma, A \vdash \neg B, \Delta}{\Gamma \vdash A \Rightarrow B, \Delta}\ \Rightarrow_R$$

$$\frac{\Gamma \vdash A, \Delta \qquad \Gamma \vdash B, \Delta}{\Gamma \vdash A \wedge B, \Delta}\ \wedge_R \qquad \frac{\Gamma, A \vdash \Delta \qquad \Gamma, B \vdash \Delta}{\Gamma, A \vee B \vdash \Delta}\ \vee_L \qquad \frac{\Gamma, A \vdash \Delta \qquad \Gamma \vdash B, \Delta}{\Gamma, A \Rightarrow B \vdash \Delta}\ \Rightarrow_L$$

- example proof.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{B \vdash A, B}}{B \vdash A \vee B} \qquad \dfrac{\dfrac{}{A \vdash A, B}}{A \vdash A \vee B}}{B \vee A \vdash A \vee B}}{\vdash (B \vee A) \Rightarrow (A \vee B)}$$

The Cut Rule

- the cut rule: a necessary detour

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

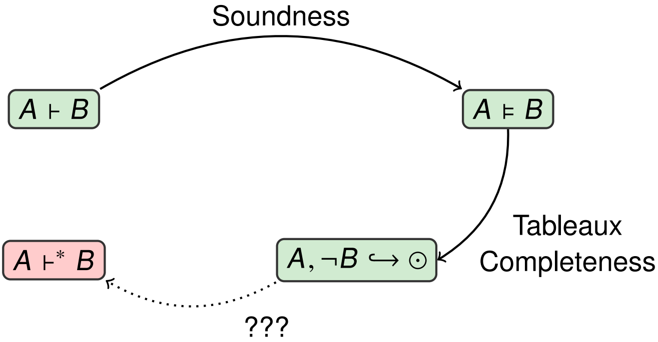
- used by human beings, *interaction*
- at the heart of logic and Computer Science
  - elimination. Proof transformation mechanisms.
  - admissibility. Show the follwing result

Cut Admissibility

If $\Gamma \vdash A, \Delta$ and $\Gamma, A \vdash \Delta$ provable, then $\Gamma \vdash \Delta$ is provable.

  - of course, in s calculus without the cut rule.

Completeness and Cut Admissilibity



Can We Translate Tableaux to Sequents?

- A tableau is a reversed cut-free sequent
  - ⋆ $\neg_X$ tableau rule $\sim$ X_R rule
  - ⋆ X tableau rule $\sim$ X_L rule

$$
\dfrac{\dfrac{\neg((B \vee A) \Rightarrow (A \vee B))}{B \vee A, \neg(A \vee B)}\ \neg_{\Rightarrow}}{\dfrac{\dfrac{B, \neg(A \vee B)}{B, \neg A, \neg B}\ \neg_{\vee}}{\odot} \qquad \dfrac{\dfrac{A, \neg(A \vee B)}{A, \neg A, \neg B}\ \neg_{\vee}}{\odot}}\ \vee
$$

$$
\Rightarrow_L \dfrac{\vee_L \dfrac{\vee_R \dfrac{\overline{B \vdash A, B}}{B \vdash A \vee B} \qquad \vee_R \dfrac{\overline{A \vdash A, B}}{A \vdash A \vee B}}{B \vee A \vdash A \vee B}}{\vdash (B \vee A) \Rightarrow (A \vee B)}
$$

- We just proved cut elimination

4. Extensions

Switching to First-Order

- we add variables, terms and quantifiers

$$\forall x(P(x) \Rightarrow Q(x))$$

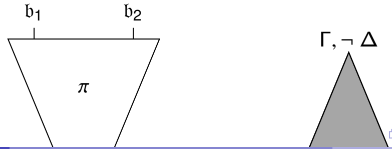
- first-order tableaux, first-order sequent calculus
- cut admissibility by the previous method
- but the complete exhaustive proof-search is highly inefficient
  - ★ enumerates all the terms of the language $t_0, t_1, \cdots$
  - ★ complete branch with $\forall x F$ must have $F[t_0/x], F[t_1/x], \cdots$
  - ★ some sweat to keep proof-search fair

Efficiency in First-Order Tableaux

- unefficient naive enumeration, maybe was $F[t_{2017}/x]$ the right choice ?
- do not know: wait to instantiate!
- free variable tableaux

$$\cfrac{\neg(\exists x(D(x) \Rightarrow \forall y D(y)))}{\cfrac{\neg(D(X) \Rightarrow \forall y D(y))}{\cfrac{D(X), \neg\forall y D(y)}{\cfrac{\neg D(c)}{\odot \ \{X \approx c\}}\ \odot}\ \forall}\ \neg\Rightarrow}\ \neg\exists$$

- FV tableaux: exponential speedups
- sequent calculus connection lost
  - ⋆ freshness condition *globally* ensured, not *locally*
  - ⋆ re-expand, double inverted induction, duplication



Switching to Deduction Modulo Theory

Rewrite Rule

A term (resp. proposition) rewrite rule is a pair of terms (resp. formulæ) $l \rightarrow r$, where $\mathcal{FV}(l) \subseteq \mathcal{FV}(r)$ and, in the propositiona case, l is atomic.

Examples:

- term rewrite rule:

$$A \cup \emptyset \rightarrow A$$

- proposition rewrite rule:

$$A \subseteq B \rightarrow \forall x\ x \in A \Rightarrow x \in B$$

Conversion modulo a Rewrite System

We consider the congruence $\equiv$ generated by a set of proposition rewrite rules $\mathcal{R}$ and a set of term rewrite rules $\mathcal{E}$ (often implicit)

Example:

$$A \cup \emptyset \subseteq A \quad \equiv \quad \forall x\ x \in A \Rightarrow x \in A$$

(Classical) Sequent Calculus modulo

We add two conversion rules:

$$\frac{\Gamma \vdash A, \Delta}{\Gamma \vdash B, \Delta}\ \mathrm{conv}_R, [A \equiv B] \qquad \frac{\Gamma, A \vdash \Delta}{\Gamma, B \vdash \Delta}\ \mathrm{conv}_L, [A \equiv B]$$

Or embed conversions modulo $\mathcal{RE}$ directly inside the rules (next slide).

(Classical) Sequent Calculus

$$\frac{}{A \vdash A}\ \text{ax} \qquad \frac{\Gamma \vdash A, \Delta \qquad \Gamma, A \vdash \Delta}{\Gamma \vdash \Delta}\ \text{cut}$$

$$\frac{\Gamma, A, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta}\ \wedge_L \qquad \frac{\Gamma \vdash A, \Delta \qquad \Gamma \vdash B, \Delta}{\Gamma \vdash A \wedge B, \Delta}\ \wedge_R$$

$$\frac{\Gamma, A \vdash \Delta \qquad \Gamma, B \vdash \Delta}{\Gamma, A \vee B \vdash \Delta}\ \vee_L \qquad \frac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \vee B, \Delta}\ \vee_R$$

$$\frac{\Gamma, B \vdash \Delta \qquad \Gamma \vdash A, \Delta}{\Gamma, A \Rightarrow B \vdash \Delta}\ \Rightarrow_L \qquad \frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \Rightarrow B, \Delta}\ \Rightarrow_R$$

(Classical) Sequent Calculus Modulo

$$\frac{}{A \vdash B}\ \text{ax},\ [A \equiv B] \qquad \frac{\Gamma \vdash A, \Delta \qquad \Gamma, B \vdash \Delta}{\Gamma \vdash \Delta}\ \text{cut},\ [A \equiv B]$$

$$\frac{\Gamma, A, B \vdash \Delta}{\Gamma, C \vdash \Delta}\ \wedge_L,\ [C \equiv A \wedge B] \qquad \frac{\Gamma \vdash A, \Delta \qquad \Gamma \vdash B, \Delta}{\Gamma \vdash C, \Delta}\ \wedge_R,\ [C \equiv A \wedge B]$$

$$\frac{\Gamma, A \vdash \Delta \qquad \Gamma, B \vdash \Delta}{\Gamma, C \vdash \Delta}\ \vee_L,\ [C \equiv A \vee B] \qquad \frac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash C, \Delta}\ \vee_R,\ [C \equiv A \vee B]$$

$$\frac{\Gamma, B \vdash \Delta \qquad \Gamma \vdash A, \Delta}{\Gamma, C \vdash \Delta}\ \Rightarrow_L,\ [C \equiv A \Rightarrow B] \qquad \frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash C, \Delta}\ \Rightarrow_R,\ [C \equiv A \Rightarrow B]$$

Proof of $A \subseteq A$ with and without DM

- without:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \subseteq A \Rightarrow [\cdots], x \in A \vdash x \in A, A \subseteq A}}{A \subseteq A \Rightarrow [\cdots] \vdash x \in A \Rightarrow x \in A, A \subseteq A}}{A \subseteq A \Rightarrow [\cdots] \vdash \forall x(x \in A \Rightarrow x \in A), A \subseteq A} \quad \dfrac{}{A \subseteq A \Rightarrow [\cdots], A \subseteq A \vdash A \subseteq A}}{\dfrac{A \subseteq A \Rightarrow \forall x(x \in A \Rightarrow x \in A), \forall x(x \in A \Rightarrow x \in A) \Rightarrow A \subseteq A \vdash A \subseteq A}{\dfrac{A \subseteq A \Leftrightarrow \forall x(x \in A \Rightarrow x \in A) \vdash A \subseteq A}{\dfrac{\forall Y(A \subseteq Y \Leftrightarrow \forall x(x \in A \Rightarrow x \in Y)) \vdash A \subseteq A}{\forall X \forall Y(X \subseteq Y \Leftrightarrow \forall x(x \in X \Rightarrow x \in Y)) \vdash A \subseteq A}}}}$$

- with:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{x \in A \vdash x \in A}}{\vdash x \in A \Rightarrow x \in A}}{\vdash \forall x(x \in A \Rightarrow x \in A)}}{\vdash A \subseteq A}$$

Proof of $A \subseteq A$ with and without DM

- without:

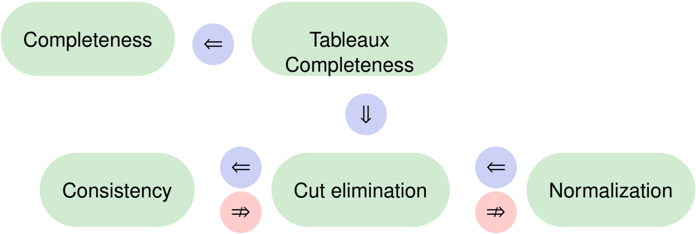
$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \subseteq A \Rightarrow [\cdots], x \in A \vdash x \in A, A \subseteq A}}{A \subseteq A \Rightarrow [\cdots] \vdash x \in A \Rightarrow x \in A, A \subseteq A}}{A \subseteq A \Rightarrow [\cdots] \vdash \forall x(x \in A \Rightarrow x \in A), A \subseteq A} \quad \dfrac{}{A \subseteq A \Rightarrow [\cdots], A \subseteq A \vdash A \subseteq A}}{\dfrac{A \subseteq A \Rightarrow \forall x(x \in A \Rightarrow x \in A), \forall x(x \in A \Rightarrow x \in A) \Rightarrow A \subseteq A \vdash A \subseteq A}{\dfrac{A \subseteq A \Leftrightarrow \forall x(x \in A \Rightarrow x \in A) \vdash A \subseteq A}{\dfrac{\forall Y(A \subseteq Y \Leftrightarrow \forall x(x \in A \Rightarrow x \in Y)) \vdash A \subseteq A}{\forall X \forall Y(X \subseteq Y \Leftrightarrow \forall x(x \in X \Rightarrow x \in Y)) \vdash A \subseteq A}}}}$$

- with:

$$\dfrac{\dfrac{\dfrac{}{x \in A \vdash x \in A}}{\vdash x \in A \Rightarrow x \in A}}{\vdash A \subseteq A}$$

Tableaux and Cuts in Deduction Modulo Theory

- beyond first order (axiomless higher-order logic, arithmetic, ...)
- everything depends on $\mathcal{RE}$.
  - ★ consistency ($A \longrightarrow \neg A$)
  - ★ cut elimination ($A \longrightarrow (A \Rightarrow A)$)
  - ★ cut admissibility
  - ★ undecidable, even if $\mathcal{RE}$ confluent terminating.



Semantics for Deduction Modulo Theory

- your favorite semantics
- add one constraint

Model of $\mathcal{RE}$

An interpretation $[\![]\!]$ is a model of $\mathcal{RE}$ if for any F, F', such that $F \equiv F'$, we have $[\![F]\!] = [\![F']\!]$.

- straightforward Soundness Theorem

Generic Approach for Tableaux

- as far as possible
  - needs only confluence
  - everything except countermodel construction
- difficulties (besides models)
  - fair and exhausting proof-search design (STEP)
  - interleave quantifier instantiation and rewriting
  - add free-variables
- optimized proof-seach, holes on the branch
  - fill the gaps to get a (semi-)valuation
  - not forgetting rewriting

Specific Countermodel Constructions

Completeness of tableaux, hence cut admissibility for

- positive rewrite systems

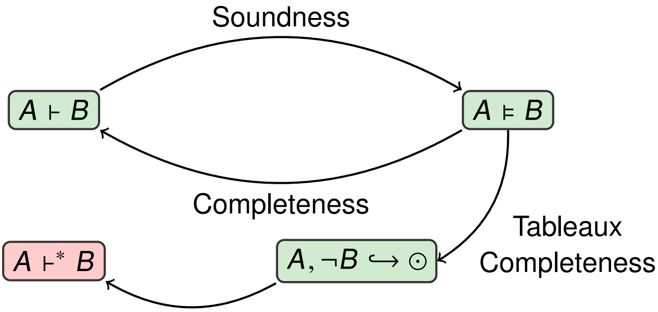
$$\begin{array}{lcl} \text{even}(0) & \rightarrow & \top \\ \text{even}(S(x)) & \rightarrow & \neg\text{odd}(x) \\ \text{odd}(S(x)) & \rightarrow & \neg\text{even}(x) \end{array}$$

- ordered rewrite systems
- higher-order logic as a rewrite system

5. Getting Rid of Tableaux

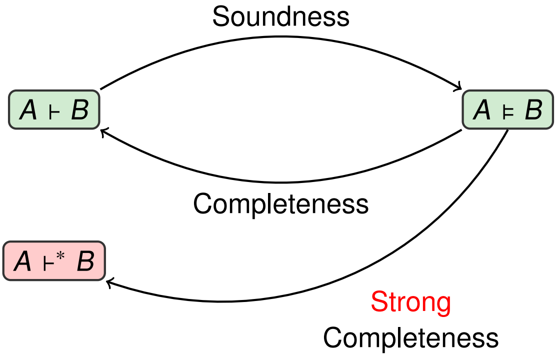
Direct Completeness

- most difficulties in Tableaux Completeness



Direct Completeness

- most difficulties in Tableaux Completeness
- most difficulties in Strong Completeness
  - more flexibility in the semantics
  - 0/1 Boolean algebra imposed by tableaux (intuitionistic case, Kripke structures).



More Flexible Semantics: Algebraic Structures

- propositional intuitionistic logic here (first-order, higher-order possible)
- Heyting algebras
- a universe Ω, operators $\wedge, \vee, \Rightarrow$
- an order $\leq$: Ω is a lattice.
- lowest upper bound (join: $\wedge$), greatest lower bound (meet: $\vee$)

$$a \wedge b \leq a \quad a \wedge b \leq b \quad c \leq a \text{ and } c \leq b \text{ implies } c \leq a \wedge b$$

$$a \leq a \vee b \quad b \leq a \vee b \quad a \leq c \text{ and } b \leq c \text{ implies } a \vee b \leq c$$

- like Boolean algebras (classical case), but
- weak complement (aka implication property):

$$a \wedge b \leq c \;\text{ iff }\; a \leq b \Rightarrow c$$

- example: $\mathbb{R}$ and open sets:

$$b \Rightarrow c := \text{ the interior of } b \cup \overline{a}$$

Cut Admissibility: Algebraic Way

Base Elements of the Lindenbaum Algebra

$\lceil A \rceil = \{B \mid A \vdash B \text{ and } B \vdash A\}$

Lidenbaum algebra:

- interpretation of formulas
  - ★ $[\![A]\!] = \lceil A \rceil$ on atoms, then induction
  - ★ $\lceil A \rceil \leq \lceil B \rceil$ iff $A \vdash B$

Fundamental Lemma

For *any* formula A, $[\![A]\!] = \lceil A \rceil$

- what do we have ?

Completeness

if $[\![A]\!] \leq [\![B]\!]$ in all models, then $A \vdash B$.

  - ★ this is the definition of $\leq$ in the Lindenbaum algebra.

- need the cut rule

Cut Admissibility: Algebraic Way

Base Elements of the Lindenbaum Algebra

$\lceil A \rceil = \{B \mid A \vdash B \text{ and } B \vdash A\}$

Cut Admissibility: Algebraic Way

Base Elements of the Context Algebra

$\lceil A \rceil = \{\Gamma \mid \Gamma \vdash A\}$

- $\leq$ is $\subseteq$ and g.l.b. ($\wedge$) and l.u.b. ($\vee$) are "intersection" and "union"
- close Ω by arbitrary intersection:

The Algebra Ω

$$\Omega = \left\{ \bigcap_{C \in \mathcal{C}} \lceil C \rceil \mid \text{ for } \mathcal{C} \text{ set of formulas} \right\}$$

Ω is composed of arbitrary intersections of base elements

- Ω not closed by union
  - ⋆ there are other ways to compute a least upper bound ...

Cut Admissibility: Algebraic Way

- set the interpretation of the atoms to be: $[\![A]\!] = \lceil A \rceil$

Key Theorem

For *any* formula A, $[\![A]\!] = \lceil A \rceil$.

Cut Admissibility: Algebraic Way

- set the interpretation of the atoms to be: $[\![A]\!] = \lceil A \rceil$

Key Theorem

For *any* formula A, $[\![A]\!] = \lceil A \rceil$.

- what do we have ?

Completeness

if $[\![A]\!] \leq [\![B]\!]$ in all models, then $A \vdash B$.

- ★ (trivial) $A \in \lceil A \rceil$
- ★ $\lceil A \rceil = [\![A]\!]$ (Key Theorem)
- ★ $[\![A]\!] \subseteq [\![B]\!]$ (Hypothesis)
- ★ $[\![B]\!] = \lceil B \rceil$ (Key Theorem)
- ★ means $A \vdash B$

Cut Admissibility: Algebraic Way

- set the interpretation of the atoms to be: $[\![A]\!] = \lceil A \rceil$

Key Theorem

For *any* formula A, $[\![A]\!] = \lceil A \rceil$.

- what do we really need ?

Completeness

if $[\![A]\!] \leq [\![B]\!]$ in all models, then $A \vdash B$.

- ★
- ★ $A \in [\![A]\!]$ (Key Theorem)
- ★ $[\![A]\!] \subseteq [\![B]\!]$ (Hypothesis)
- ★ $[\![B]\!] \subseteq \lceil B \rceil$ (Key Theorem)
- ★ means $A \vdash B$

Cut Admissibility: Algebraic Way

- Ω contains arbitrary intersections of base elements.

Base Elements

$\lceil A \rceil = \{\Gamma \mid \Gamma \vdash A\}$

- $\leq$ is $\subseteq$. Gives a lattice.
- it is also a Heyting algebra
- set the interpretation of the atoms to be: $[\![A]\!] = \lceil A \rceil$

Key Theorem

For *any* formula A, $[\![A]\!] = \lceil A \rceil$.

- what do we have ?

Completeness

if $[\![A]\!] \leq [\![B]\!]$ in all models, then $A \vdash B$.

Proof: $A \in \lceil A \rceil = [\![A]\!] \subseteq [\![B]\!] = \lceil B \rceil$.

Cut Admissibility: Algebraic Way

- Ω contains arbitrary intersections of base elements.

Base Elements

$\lceil A \rceil = \{\Gamma \mid \Gamma \vdash^* A\}$

- $\leq$ is $\subseteq$. Gives a lattice.
- it is also a Heyting algebra ($\Rightarrow$ property difficult)
- set the interpretation of the atoms to be: $[\![A]\!] = \lceil A \rceil$

Key Theorem

For *any* formula A, $A \in [\![A]\!] \subseteq \lceil A \rceil$

- Similarities with Reducibility Candidate-valued models (logical relations)

$$NE \subseteq \mathcal{R}_A \subseteq SN \quad \text{(simplified)}$$

Cut Admissibility, Second Order: Algebraic Way

- Ω contains arbitrary intersections of base elements.

Base Elements

$\lceil A \rceil = \{\Gamma \mid \Gamma \vdash^* A\}$

- $\leq$ is $\subseteq$. Gives a lattice.
- it is also a Heyting algebra ($\Rightarrow$ property difficult)
- set the interpretation of the atoms to be: $[\![A]\!] = \lceil A \rceil$

Key Theorem

For *any* formula A, $A\sigma \in [\![A]\!]_\phi \subseteq \lceil A\sigma \rceil$,
for any ϕ, σ such that $\sigma(X_i) \in \phi(X_i) \subseteq \lceil \sigma(X_i) \rceil$

- Similarities with Reducibility Candidate-valued models (logical relations)

$$NE \subseteq \mathcal{R}_A \subseteq SN \quad \text{(simplified)}$$
$$[\![A]\!]_\phi \in \mathcal{R}_{A\sigma}, \text{ for any } \phi, \sigma \text{ s.t. } \phi(X_i) \in R_{\sigma(X_i)}$$

Application to Higher-Order Logics

- does not apply directly to higher-order logic
- intensional logic
$$P(\top) \not\Leftrightarrow P(\top \wedge \top)$$
- $[\![\top]\!] \neq \top$
- V-complexes [Takahashi], [Prawitz], [Andrews]
- adapted to
    - intuitionnistic case,
    - linear case,
    - the Deduction modulo theory expression of HOL (classical and intuitionnistic),

6. Opening the Box

Constructivity of Proofs

- Tableaux: rebuild proof from scratch
- Henkin completeness ([Herbelin & Ilik])

Computational Content of Algebraic Proofs

- switch to Natural Deduction
- more work existing
  - Normalization by Evaluation
  - all Kripke (-like)
- easier to compare
  - and understand (at least, so did we thought)
  - no problem with disjunction in Heyting algebra

What Had to be Done

- from Sequent Calculus to Natural Deduction

What Had to be Done

- from Sequent Calculus to Natural Deduction
- notion of cut-free proof

Cut-Free Proofs

A proof is neutral it is an elimination with cut-free premises and neutral principal premiss. A proof is cut-free it is an introduction with cut-free premises.

$$\frac{\Gamma \vdash_{ne} A}{\Gamma \vdash^* A}\ coerce \qquad \frac{A \in \Gamma}{\Gamma \vdash_{ne} A}\ ax$$

$$\frac{\Gamma \vdash^* A \qquad \Gamma \vdash^* B}{\Gamma \vdash^* A \wedge B}\ \wedge_I \qquad \frac{\Gamma \vdash_{ne} A \wedge B}{\Gamma \vdash_{ne} A}\ \wedge_{E_l} \qquad \frac{\Gamma \vdash_{ne} A \wedge B}{\Gamma \vdash_{ne} B}\ \wedge_{E_r}$$

$$\frac{\Gamma \vdash^* A}{\Gamma \vdash^* A \vee B}\ \vee_{I_l} \qquad \frac{\Gamma \vdash^* B}{\Gamma \vdash^* A \vee B}\ \vee_{I_r} \qquad \frac{\Gamma \vdash_{ne} A \vee B \qquad A, \Gamma \vdash^* C \qquad B, \Gamma \vdash^* C}{\Gamma \vdash_{ne} C}\ \vee_E$$

$$\frac{\Gamma, A \vdash^* B}{\Gamma \vdash^* A \Rightarrow B}\ \Rightarrow_I \qquad \frac{\Gamma \vdash_{ne} A \Rightarrow B \qquad \Gamma \vdash^* A}{\Gamma \vdash_{ne} B}\ \Rightarrow_E$$

What Had to be Done

- from Sequent Calculus to Natural Deduction
- notion of cut-free proof

Cut-Free Proofs

A proof is neutral it is an elimination with cut-free premises and neutral principal premiss. A proof is cut-free it is an introduction with cut-free premises.

$$\frac{\Gamma \vdash_{ne} A}{\Gamma \vdash^* A}\ coerce \qquad \frac{A \in \Gamma}{\Gamma \vdash_{ne} A}\ ax$$

$$\frac{\Gamma \vdash^* A \qquad \Gamma \vdash^* B}{\Gamma \vdash^* A \wedge B}\ \wedge_I \qquad \frac{\Gamma \vdash_{ne} A \wedge B}{\Gamma \vdash_{ne} A}\ \wedge_{E_l} \qquad \frac{\Gamma \vdash_{ne} A \wedge B}{\Gamma \vdash_{ne} B}\ \wedge_{E_r}$$

$$\frac{\Gamma \vdash^* A}{\Gamma \vdash^* A \vee B}\ \vee_{I_l} \qquad \frac{\Gamma \vdash^* B}{\Gamma \vdash^* A \vee B}\ \vee_{I_r} \qquad \frac{\Gamma \vdash_{ne} A \vee B \qquad A, \Gamma \vdash^* C \qquad B, \Gamma \vdash^* C}{\Gamma \vdash_{ne} C}\ \vee_E$$

$$\frac{\Gamma, A \vdash^* B}{\Gamma \vdash^* A \Rightarrow B}\ \Rightarrow_I \qquad \frac{\Gamma \vdash_{ne} A \Rightarrow B \qquad \Gamma \vdash^* A}{\Gamma \vdash_{ne} B}\ \Rightarrow_E$$

- show that constructions are still valid

What had to be Done - 2

- works for first-order logic (probably more)

What had to be Done - 2

- works for first-order logic (probably more)
- formalize in Coq (propositional logic)

What had to be Done - 2

- works for first-order logic (probably more)
- formalize in Coq (propositional logic)
- extract the algorithm:
  - limitations of Coq
  - either we face proof-irrelevance
  - or universe inconsistency

What had to be Done - 2

- works for first-order logic (probably more)
- formalize in Coq (propositional logic)
- extract the algorithm:
  - ★ limitations of Coq
  - ★ either we face proof-irrelevance
  - ★ or universe inconsistency
- we can at least observe inside Coq
- or have a potentially unsound algorithm

On Examples

- how a ⇒-cut is reduced

$$\dfrac{\dfrac{\dfrac{}{A, A \vdash A}\,ax}{A \vdash A \Rightarrow A}\Rightarrow_I \qquad \dfrac{}{A \vdash A}\,ax}{A \vdash A}\Rightarrow_E \quad \rhd \quad \dfrac{}{A \vdash A}\,ax$$

On Examples

- how a $\vee$-cut is reduced

$$\dfrac{\dfrac{\dfrac{}{A \vdash A}\,ax}{A \vdash A \vee A}\,\vee_{I_l} \qquad \dfrac{\dfrac{}{A, A \vdash A}\,ax}{A, A \vdash A \vee A}\,\vee_{I_r} \qquad \dfrac{\dfrac{}{A, A \vdash A}\,ax}{A, A \vdash A \vee A}\,\vee_{I_l}}{A \vdash A \vee A}\,\vee_E \quad \rhd \quad \dfrac{\dfrac{}{A \vdash A}\,ax}{A \vdash A \vee A}\,\vee_{I_r}$$

On Examples

- η-expansion

$$\dfrac{}{A \vee B \vdash A \vee B}\; ax$$

On Examples

- η-expansion

$$
\dfrac{
\dfrac{}{A \vee B \vdash A \vee B}\,ax
\qquad
\dfrac{\dfrac{}{A \vee B, A \vdash A}\,ax}{A \vee B, A \vdash A \vee B}\,\vee_{I_l}
\qquad
\dfrac{\dfrac{}{A \vee B, B \vdash B}\,ax}{A \vee B, B \vdash A \vee B}\,\vee_{I_r}
}{A \vee B \vdash A \vee B}\,\vee_E
$$

On Examples

- η-expansion, one more step

$$
\dfrac{
  \dfrac{
    \dfrac{}{A \vee B \vdash A \vee B}\,ax
    \qquad
    \dfrac{\dfrac{\dfrac{}{A \vee B, A, A \vee B \vdash A}\,ax}{A \vee B, A, A \vee B \vdash A \vee B}\,\vee_{I_l}}{A \vee B, A \vdash (A \vee B) \Rightarrow (A \vee B)}\,\Rightarrow_I
    \qquad
    \dfrac{\dfrac{\dfrac{}{A \vee B, B, A \vee B \vdash B}\,ax}{A \vee B, B, A \vee B \vdash A \vee B}\,\vee_{I_r}}{A \vee B, B \vdash (A \vee B) \Rightarrow (A \vee B)}\,\Rightarrow_I
  }{A \vee B \vdash (A \vee B) \Rightarrow (A \vee B)}\,\vee_E
  \qquad
  \dfrac{}{A \vee B \vdash A \vee B}\,ax
}{A \vee B \vdash A \vee B}\,\Rightarrow_E
$$

Conclusion

A lot of domains to which apply those techniques

- logics with constraints (higher order)
- polarized Deduction Modulo Theory
  - model theory
  - theoretical results
  - tools
- this is all first order, no dependent types
  - $\lambda\Pi$-calculus Modulo Theory
  - Dedukti