Mathematical Logic

Introduction to Reasoning and Automated Reasoning. Hilbert-style Propositional Reasoning.

Chiara Ghidini

FBK-IRST, Trento, Italy

Deciding logical consequence

Problem

Is there an algorithm to determine whether a formula ϕ is the logical consequence of a set of formulas Γ?

Naïve solution

- Apply directly the definition of logical consequence i.e., for all possible interpretations $\mathcal{I}$ determine if $\mathcal{I} \models \Gamma$, if this is the case then check if $\mathcal{I} \models A$ too.
- This solution can be used when Γ is finite, and there is a finite number of relevant interpretations.

Complexity of deciding logical consequence in Propositional Logic

The truth table method is Exponential

The problem of determining if a formula A containing n primitive propositions, is a logical consequence of the empty set, i.e., the problem of determining if A is valid, ($\models A$), takes an n-exponential number of steps. To check if A is a tautology, we have to consider 2^n interpretations in the truth table, corresponding to 2^n lines.

More efficient algorithms?

Are there more efficient algorithms? I.e. Is it possible to define an algorithm which takes a polinomial number of steps in n, to determine the validity of A? This is an unsolved problem

$P \stackrel{?}{=} NP$

The existence of a polinomial algorithm for checking validity is still an open problem, even it there are a lot of evidences in favor of non-existence

Deciding logical consequence is not always possible

Propositional Logics

The truth table method enumerates all the possible interpretations of a formula and, for each formula, it computes the relation $\models$.

Other logics

For first order logic and modal logics there is no general algorithm to compute the logical consequence. There are some algorithms computing the logical consequence for first order logic sub-languages and for sub-classes of structures (as we will see further on).

Alternative approach: decide logical consequence via reasoning.

Reasoning

What the dictionaries say:

- **reasoning**: the process by which one judgement is deduced from another or others which are given (Oxford English Dictionary)
- **reasoning**: the drawing of inferences or conclusions through the use of *reason*
  reason: the power of comprehending, inferring, or thinking, esp. in orderly rational ways (cf. *intelligence*) (Merriam-Webster)

What is it to Reason?

- Reasoning is a process of deriving new statements (conclusions) from other statements (premises) by argument.
- For reasoning to be correct, this process should generally **preserve truth**. That is, the arguments should be **valid**.
- How can we be sure our arguments are valid?
- Reasoning takes place in many different ways in everyday life:
  - **Word of Authority**: we derive conclusions from a source that we trust; e.g. religion.
  - **Experimental science**: we formulate hypotheses and try to confirm them with experimental evidence.
  - **Sampling**: we analyse many pieces of evidence statistically and identify patterns.
  - **Mathematics**: we derive conclusions based on mathematical *proof*.
- Are any of the above methods **valid**?

What is a Proof? (I)

- For centuries, mathematical proof has been the hallmark of logical validity.
- But there is still a **social aspect** as peers have to be convinced by argument.
- This process is open to **flaws**: e.g. Kempes proof of the Four Colour Theorem.
- To avoid this, we require that all proofs be broken down to their simplest steps and all hidden premises uncovered.

What is a Formal Proof?

We can be sure there are no hidden premises by reasoning according to logical form alone.

Example

Suppose all men are mortal. Suppose Socrates is a man. Therefore, Socrates is mortal.

- The validity of this proof is independent of the meaning of "men", "mortal" and "Socrates".
- Indeed, even a nonsense substitution gives a valid sentence:
    - Suppose all borogroves are mimsy. Suppose a mome rath is a borogrove. Therefore, a mome rath is mimsy.
- General pattern:
    - Suppose all Ps are Q. Suppose x is a P. Therefore, x is a Q.

Symbolic Proof

- The modern notion of symbolic formal proof was developed in the 20th century by logicians and mathematicians such as Russell, Frege and Hilbert.
- The benefit of formal logic is that it is based on a pure syntax: *a precisely defined symbolic language with procedures for transforming symbolic statements into other statements, based solely on their form*.
- **No intuition or interpretation is needed**, merely applications of agreed upon rules to a set of agreed upon formulae.

Propositional reasoning: Proofs and deductions (or derivations)

proof

A proof of a formula ϕ is a sequence of formulas $\phi_1, \ldots, \phi_n$, with $\phi_n = \phi$, such that each ϕ_k is either

- an axiom or
- it is derived from previous formulas by reasoning rules

ϕ is provable, in symbols $\vdash \phi$, if there is a proof for ϕ.

Deduction of ϕ from Γ

A deduction of a formula ϕ from a set of formulas Γ is a sequence of formulas $\phi_1, \ldots, \phi_n$, with $\phi_n = \phi$, such that ϕ_k

- is an axiom or
- it is in Γ (an assumption)
- it is derived form previous formulas bhy reasoning rules

ϕ is derivable from Γ, in symbols $\Gamma \vdash \phi$, if there is a proof for ϕ from formulas in Γ.

Hilbert axioms for classical propositional logic

Axioms

A1 $\phi \supset (\psi \supset \phi)$

A2 $(\phi \supset (\psi \supset \theta)) \supset ((\phi \supset \psi) \supset (\phi \supset \theta))$

A3 $(\neg\psi \supset \neg\phi) \supset ((\neg\psi \supset \phi) \supset \psi)$

Inference rule(s)

MP $\dfrac{\phi \quad \phi \supset \psi}{\psi}$

Why there are no axioms for $\wedge$ and $\vee$ and $\equiv$?

The connectives $\wedge$ and $\vee$ are rewritten into equivalent formulas containing only $\supset$ and $\neg$.

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

Proofs and deductions (or derivations)

proof

A proof of a formula ϕ is a sequence of formulas $\phi_1, \ldots, \phi_n$, with $\phi_n = \phi$, such that each ϕ_k is either

- an axiom or
- it is derived from previous formulas by MP

ϕ is provable, in symbols $\vdash \phi$, if there is a proof for ϕ.

Deduction of ϕ from Γ

A deduction of a formula ϕ from a set of formulas Γ is a sequence of formulas $\phi_1, \ldots, \phi_n$, with $\phi_n = \phi$, such that ϕ_k

- is an axiom or
- it is in Γ (an assumption)
- it is derived form previous formulas by MP

ϕ is derivable from Γ in symbols $\Gamma \vdash \phi$ if there is a proof for ϕ.

Deduction and proof - example

Example (Proof of $A \supset A$)

1.	$A1$	$A \supset ((A \supset A) \supset A)$
2.	$A2$	$(A \supset ((A \supset A) \supset A)) \supset ((A \supset (A \supset A)) \supset (A \supset A))$
3.	$MP(1,2)$	$(A \supset (A \supset A)) \supset (A \supset A)$
4.	$A1$	$(A \supset (A \supset A))$
5.	$MP(4,3)$	$A \supset A$

Deduction and proof - other examples

Example (proof of $\neg A \supset (A \supset B)$)

We prove that $A, \neg A \vdash B$ and by deduction theorem we have that $\neg A \vdash A \supset B$ and that $\vdash \neg A \supset (A \supset B)$

We label with Hypothesis the formula on the left of the $\vdash$ sign.

1.	*hypothesis*	A
2.	$A1$	$A \supset (\neg B \supset A)$
3.	$MP(1,2)$	$\neg B \supset A$
4.	*hypothesis*	$\neg A$
5.	$A1$	$\neg A \supset (\neg B \supset \neg A)$
6.	$MP(4,5)$	$\neg B \supset \neg A$
7.	$A3$	$(\neg B \supset \neg A) \supset ((\neg B \supset A) \supset B)$
8.	$MP(6,7)$	$(\neg B \supset A) \supset B$
9.	$MP(3,8)$	B

Hilbert axiomatization

Minimality

The main objective of Hilbert was to find the smallest set of axioms and inference rules from which it was possible to derive all the tautologies.

Unnatural

Proofs and deductions in Hilbert axiomatization are awkward and unnatural. Other proof styles, such as Natural Deductions, are more intuitive. As a matter of facts, nobody is practically using Hilbert calculus for deduction.

Why it is so important

Providing an Hilbert style axiomatization of a logic describes with simple axioms the entire properties of the logic. Hilbert axiomatization is the "identity card" of the logic.

The deduction theorem

Theorem

$\Gamma, A \vdash B$ *if and only if* $\Gamma \vdash A \supset B$

Proof.

$\Longrightarrow$ direction ($\Longleftarrow$ is easy)
If A and B are equal, then we know that $\vdash A \supset B$ (see previous example), and by monotonicity $\Gamma \vdash A \supset B$.
Suppose that A and B are distinct formulas. Let $\pi = (A_1, \ldots, A_n = B)$ be a deduction of $\Gamma, A \vdash B$, we proceed by induction on the length of π.

Base case $n = 1$ If $\pi = (B)$, then either $B \in \Gamma$ or B is an axiom. Then

Axiom **A1**	$B \supset (A \supset B)$
$B \in \Gamma$ or B is an axiom	B
by **MP**	$A \supset B$

is a deduction of $A \supset B$ from Γ or from the empty set, and therefore $\Gamma \vdash A \supset B$.

$\square$

The deduction theorem

Proof.

Step case If $A_n = B$ is either an axiom or an element of Γ, then we can reason as the previous case.

If B is derived by **MP** form A_i and $A_j = A_i \supset B$. Then, A_i and $A_j = A_i \supset B$, are provable in less then n steps and, by induction hypothesis, $\Gamma \vdash A \supset A_i$ and $\Gamma \vdash A \supset (A_i \supset B)$. Starting from the deductions of these two formulas from Γ, we can build a deduction of $A \supset B$ form Γ as follows:

By induction	$\vdots$ deduction of $A \supset (A_i \supset B)$ form Γ
	$A \supset (A_i \supset B)$
By induction	$\vdots$ deduction of $A \supset A_i$ form Γ
	$A \supset A_i$
A2	$(A \supset (A_i \supset B)) \supset ((A \supset A_i) \supset (A \supset B))$
MP	$(A \supset A_i) \supset (A \supset B)$
MP	$A \supset B$

□

Soundness of Hilbert axiomatization

Theorem

Soundness of Hilbert axiomatization If $\Gamma \vdash A$ *then* $\Gamma \models A$.

Proof.

Let $\pi = (A_1, \ldots, A_n = A)$ be a proof of A from Γ. We prove by induction on n that $\Gamma \models A$

Base case $n = 1$ If π is (A), then either $A \in \Gamma$ or A is an axiom, that is, an instance of **(**A1), **(**A2), or **(**A3).
If $A \in \Gamma$ then by reflexivity we have $A \models A$, and by monotonicity $A \in \Gamma$ implies $\Gamma \models A$.
If A is an axiom, then it is enough to prove that $\models$ **A1**, $\models$ **A2** and $\models$ **A3** (by exercise)

Step case Suppose that A_n is derived by the application of **MP** to A_i and A_j with $i, j < n$. Then A_j is of the form $A_i \supset A_n$. By induction we have $\Gamma \models A_i$ and $\Gamma \models A_i \supset A_n$. which implies (prove it by exercise) that $\Gamma \models A_n$.

□

Completeness of Hilbert axiomatization

Theorem

If $\Gamma \models A$ *then* $\Gamma \vdash A$.

Completeness proof - 1/5

Definition

- a set of formulas Γ is inconsistent if $\Gamma \vdash \phi$ for every ϕ
- Γ is consistent it is not inconsistent;
- Γ is maximally consistent if it is consistent and any other consistent set $\Sigma \supseteq \Gamma$ is equal to Γ.

Proposition

1. *if* Γ *is consistent and* $\Sigma = \{\phi | \Gamma \vdash \phi\}$ *then* Σ *is consistent.*
2. *if* Γ *is maximally consistent, then* $\Gamma \vdash \phi$ *implies that* $\phi \in \Gamma$
3. Γ *is inconsistent if* $\Gamma \vdash \phi$ *and* $\Gamma \vdash \neg\phi$

Completeness proof - 2/5

Theorem (Lindenbaum's Theorem)

Any consistent set of formulas Σ can be extended to a maximally consistent set of formulas Γ.

Proof.

- Let $\phi_1, \phi_2, \ldots$ an enumeration of all the formulas of the language
- Let $\Sigma = \Sigma_0 \subseteq \Sigma_1 \subseteq \Sigma_2 \subseteq \ldots$, with

$$\Sigma_{n+1} = \begin{cases} \Sigma_n \cup \{\phi_n\} & \text{If } \Sigma_n \cup \{\phi_n\} \text{ is consistent} \\ \Sigma_n & \text{otherwise} \end{cases}$$

  Let $\Gamma = \bigcup_{n \geq 1} \Sigma_n$
- Γ is consistent!
- Γ is maximally consistent!

□

Completeness proof - 3/5

Lemma

If Γ *is maximally consistent then for every formula* ϕ *and* ψ*;*

1. $\phi \in \Gamma$ *if and only if* $\neg\phi \notin \Gamma$*;*
2. $\phi \supset \psi \in \Gamma$ *if and only if* $\phi \in \Gamma$ *implies that* $\psi \in \Gamma$

Proof.

1. ($\Rightarrow$) If $\phi \in \Gamma$, then $\neg\phi \notin \Gamma$ since Γ is consistent
1. ($\Leftarrow$) if $\neg\phi \notin \Gamma$, $\Gamma \cup \phi$ is consistent. Indeed suppose that $\Gamma \cup \phi$ is inconsistent, then $\Gamma \cup \phi \vdash \neg\phi$. By the deduction theorem $\Gamma \vdash \phi \supset \neg\phi$, and since $(\phi \supset \neg\phi) \supset \neg\phi$ is provable, then $\Gamma \vdash \neg\phi$ (by **MP**). By maximality of Γ, $\Gamma \vdash \neg\phi$ implies that $\neg\phi \in \Gamma$, This contradicts the hypothesis that $\neg\phi \notin \Gamma$. The fact that $\Gamma \cup \{\phi\}$ is consistent and the maximality of Γ imply that $\phi \in \Gamma$.
2. ($\Rightarrow$) If $\phi \supset \psi \in \Gamma$ and $\phi \in \Gamma$, then $\Gamma \vdash \psi$, which implies that $\psi \in \Gamma$.
2. ($\Leftarrow$) If $\phi \supset \psi \notin \Gamma$. Then by property 1, $\neg(\phi \supset \psi) \in \Gamma$. Since $\neg(\phi \supset \psi) \supset \phi$ and $\neg(\phi \supset \psi) \supset \neg\psi$, can be proved by the Hilbert axiomatic system, then $\phi \in \Gamma$ and $\neg\psi \in \Gamma$, which implies $\psi \notin \Gamma$. This implies that it is not true that if $\phi \in \Gamma$ then $\psi \in \Gamma$.

□

Completeness proof - 4/5

Theorem (Extended Completeness)

If set of formulas Σ is consistent then it is satisfiable.

Proof.

We have to prove that there is an interpretation that satisfies all the formulas of Σ.

- By Lindenbaum's Theorem, there is maximally consistent set of formulas $\Gamma \supseteq \Sigma$
- Let $\mathcal{I}$ be the interpretation such that

$$\mathcal{I}(p) = \text{True if and only if } p \in \Gamma$$

- By induction $\mathcal{I}(\phi) = \text{True}$ if and only if $\phi \in \Gamma$
- Since $\Sigma \subseteq \Gamma$, then $\mathcal{I} \models \Gamma$.

$\square$

Completeness proof - 5/5

Theorem (Completeness)

If $\Gamma \models \phi$ *then* $\Gamma \vdash \phi$

Proof.

By contradiction:

- If $\Gamma \nvdash \phi$, then $\Gamma \cup \{\neg\phi\}$ is consistent
- By extended completeness theorem $\Gamma \cup \{\neg\phi\}$ is satisfiable
- there is an interpretation $\mathcal{I} \models \Gamma$ and $\mathcal{I} \not\models \phi$
- contradiction with the hypothesis that $\Gamma \models \phi$.

□

Observation about the completeness proof

- The underlying methodology for the proof of the completeness theorem, is to prove that a consistent set of formulas Γ has a model,
- The model for Γ is build by saturating Γ with formulas
- during the saturation, we have to be careful not to make Γ inconsistent, i.e., every time we add a formula we have to check if a pair of contraddicting formulas are derivable via the set of inference rules, if it is not, we can safely add the formula.
- When Γ is saturated, (but still consistent) it defines a single model for Γ (up to isomorphism) and we have to provide a way to extract such a model form Γ

Symbolic proof (II)

But... Formal proofs are bloated and over expanded!

> *I find nothing in [formal logic] but shackles. It does not help us at all in the direction of conciseness, far from it; and if it requires 27 equations to establish that 1 is a number, how many will it require to demonstrate a real theorem? (Poincaré)*

Can automation help?

Automated Reasoning

- Automated Reasoning (AR) refers to reasoning in a computer using **logic**.
- AR has been an active area of research since the 1950s.
- It uses deductive reasoning to tackle problems such as:
  - constructing formal mathematical proofs;
  - verifying programs meet their specifications;
  - modelling human reasoning.

Different Forms of Reasoning

- **Deduction**: Given a set of premises Γ and a conclusion ϕ show that indeed $\Gamma \models \phi$ (this includes Validity: $\Gamma = \emptyset$)
- **Abduction/Induction**: given a theory T and an observation ϕ, find an explanation Γ such that $T \cup \Gamma \models \phi$
- **Satisfiability Checking**: given a set of formulae Γ, check whether there exists a model $\mathcal{I}$ such that $\mathcal{I} \models \phi$ for all $\phi \in \Gamma$?
- **Model Checking**: given a model $\mathcal{I}$ and a formula ϕ, check whether $\mathcal{I} \models \phi$

Automated reasoning attempts to mechanise all of these forms of reasoning for different *logics*: propositional or first-order, classical, intuionistic, modal, temporal, non-monotonic, . . .

More efficient reasoning systems

Automate Hilbert style reasoning

Checking if $\Gamma \models \phi$ by searching for a Hilbert-style deduction of ϕ from Γ is not an easy task for computers. Indeed, in trying to generate a deduction of ϕ from Γ, there are to many possible actions a computer could take:

- adding an instance of one of the three axioms (infinite number of possibilities)
- applying **MP** to already deduced formulas,
- adding a formula in Γ

More efficient methods

Resolution	to check if a formula is *not satisfiable*
SAT	DP, DPLL to *search for an interpretation that satisfies a formula*
Tableaux	*search for a model of a formula* guided by its structure