Formal proof systems for propositional logic

Chiara Ghidini – Maurizio Lenzerini

FBK-IRST, Trento, Italy – Sapienza Università di Roma

A.Y. 2021/22

Deciding logical implication

Problem

Is there an algorithm to determine whether a formula A is logically implied by a set of formulas Γ?

Naïve solution

- If Γ is finite, transform Γ into the conjunction of its elements, apply the deduction theorem ($\Gamma \models A$ if and only if $\Gamma \rightarrow A$ is valid), and then apply directly the definition of validity i.e., for all possible interpretations $\mathcal{I}$ determine if $\mathcal{I} \models \Gamma \rightarrow A$ is true.
- This solution can be used when Γ is finite, and therefore there is a finite number of relevant interpretations to consider.

Complexity of logical implication

The truth table method is exponential

The problem of determining if a formula A containing n propositional letters 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 a polynomial time algorithm in n, to determine the validity of A? This is an unsolved problem, related to "satisfiabiity".

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

The existence of a polynomial time algorithm for checking validity (i.e., unsatisfiability) is still an open problem, even it there are a lot of evidences in favor of non-existence.

Deciding logical implication by truth tables not always the best choice

Propositional Logics

The truth table method enumerates all the possible interpretations of a formula and, for each interpretation, it checks whether it is a model of the formula.

Other scenarios

When dealing with infinite sets of propositional formulas, or formulas in other logics (first order logic or modal logics) there is no general algorithm to perform deduction based on truth tables.

Also, the method is not suitable for example, for explaining deduction.

Deciding logical implication by truth tables not always the best choice

Propositional Logics

The truth table method enumerates all the possible interpretations of a formula and, for each interpretation, it checks whether it is a model of the formula.

Other scenarios

When dealing with infinite sets of propositional formulas, or formulas in other logics (first order logic or modal logics) there is no general algorithm to perform deduction based on truth tables.

Also, the method is not suitable for example, for explaining deduction.

Alternative approach: deduction via formal proof systems.

Proofs are the core of logic

- For centuries, mathematical proof has been the hallmark of logical validity (no formal semantics until recently).
- Most proofs were, however, expressed in natural languages.
- By using natural language, the process is open to **flaws**: e.g. the flawed Kempe's proof of the Four Colour Theorem.
- To address these problems, the modern formulation of logic requires that proofs are formal (based on the "form") and be broken down to their simplest steps, with all hidden premises uncovered.

Formal proofs are at the core of modern logic

- 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 symbolic formal proofs is that they are based on pure syntax, i.e., symbolic manipulation: *a precisely defined symbolic formalism with procedures for transforming 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 formulas.

The notion of formal system

Intuitively, a formal system consists of a language over some alphabet of symbols together with initial strings and production rules that are used to generate some of the strings in the language. More precisely,

Formal system

A formal system has the following components:

- An alphabet of symbols.
- A syntax that defines which sequence of symbols (each sequence of symbol also called string) are in the language of our formal system.
- A decidable set of initial strings.
- A finite set of production rules by which the set of conclusions of the system (each conclusion being again a string) is generated; each conclusion is generated through a finite set of application of the production rules on both the initial strings and the already generated conclusions.

Proof system: a special case of formal system

Formal proof system

A symbolic formal proof system (or simply proof system) Σ for propositional logic is constituted by:

- The set of axioms of Σ, i.e., a set of propositional formulas such that there is an effective procedure to decide if a given formula is an axiom.
- The (finite) set $R_1, \ldots, R_n$ of inference rules of Σ, where each inference rule R_i is a relation that associates to a set of j_i formulas $A_1, \ldots, A_{j_i}$, one formula A that is called the direct consequences of $A_1, \ldots, A_{j_i}$ through R_i.

A formula A that is a direct consequences of $A_1, \ldots, A_j$ through R is said to be derived $A_1, \ldots, A_j$ by R. When we want to describe an inference rule R applied to $A_1, \ldots, A_j$ to derive A, we write:

$$R \quad \frac{A_1, \ldots, A_j}{A}$$

Proof, provability, theorem

Proof

A proof in Σ is a finite sequence of formulas $\phi_1, \ldots, \phi_n$ such that each ϕ_k is either

- an axiom of Σ, or
- a direct consequence of a set of previous formulas in the sequence through an inference rule of Σ.

Proof of ϕ

A proof of ϕ in Σ is a proof $\phi_1, \ldots, \phi_n$ in Σ such that $\phi_n = \phi$.

Theorem

A formula ϕ is provable in Σ if there is proof of ϕ in Σ, and in this case we write $\vdash_\Sigma \phi$ (or simply $\vdash \phi$ when Σ is understood), and we also say that ϕ is a theorem in (or of) Σ.

Proof from hypotheses

Proof from hypothesis

A proof of ϕ in Σ from a set of hypothesis (or assumptions) Γ is a sequence of formulas $\phi_1, \ldots, \phi_n$, with $\phi_n = \phi$, such that each ϕ_k is either

- an axiom of Σ, or
- an hypothesis in Γ, or
- a direct consequence of a set of previous formulas in the squence through an inference rule of Σ.

Inference or derivation

We say that ϕ is inferred (or provable, or derived) from Γ in Σ, written $\Gamma \vdash_\Sigma \phi$ (or simply $\Gamma \vdash \phi$ when Σ is understood), if there is a proof of ϕ in Σ from Γ.

Consistency

We say that a set Γ of formulas is Σ-consistent if no formula ϕ exists such that both $\Gamma \vdash_\Sigma \phi$ and $\Gamma \vdash_\Sigma \neg\phi$, otherwise is Σ-inconsistent.

Properties of a proof system

Analogously to logical implication, it is interesting to check whether the following property hold for a certain $\vdash_\Sigma$:

- Reflexivity (If $A \in \Gamma$, then $\Gamma \vdash_\Sigma A$)
- Ex falso sequitur quodlibet (If Γ is unsatisfiable, then $\Gamma \vdash_\Sigma A$ for all A)
- Monotonicity (If $\Gamma \vdash_\Sigma A$ then $\Gamma \cup \Delta \vdash_\Sigma A$)
- Cut (If $\Gamma \vdash_\Sigma A$ and $\Delta \cup \{A\} \vdash_\Sigma B$ then $\Gamma \cup \Delta \vdash_\Sigma B$)
- Compactness (If $\Gamma \vdash_\Sigma A$, then there is a finite subset $\Gamma_0 \subseteq \Gamma$, such that $\Gamma_0 \vdash_\Sigma A$)
- Deduction principle ($\Gamma \cup \{A\} \vdash_\Sigma B$ if and only if $\Gamma \vdash_\Sigma A \to B$)
- Refutation principle ($\Gamma \vdash_\Sigma A$ if and only if $\Gamma \cup \{\neg A\}$ is inconsistent)
- Consistency: $\vdash_\Sigma$ is consistent if there is no formula A such that both $\vdash_\Sigma A$ and $\vdash_\Sigma \neg A$

Hilbert formal proof system for propositional logic

We study the Hilbert proof system, denoted by $\mathcal{H}$. In what follows, ϕ and ψ denote formulas, and **MP** stands for "modus ponens".

Axioms of $\mathcal{H}$ (each ϕ, ψ, θ is any formula)

A1 $\phi \to (\psi \to \phi)$

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

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

Inference rule(s) of $\mathcal{H}$

MP $\dfrac{\phi,\ \phi \to \psi}{\psi}$

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

Formulas with connectives $\wedge$ and $\vee$ are rewritten into equivalent formulas containing only $\to$ and $\neg$.

$$A \wedge B \equiv \neg(A \to \neg B)$$
$$A \vee B \equiv \neg A \to B$$
$$A \equiv B \equiv \neg((A \to B) \to \neg(B \to A))$$

Example of proof in $\mathcal{H}$

Example (Proof of $A \to A$ in $\mathcal{H}$)

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

Example of inference in $\mathcal{H}$

Example (Inference of B from $\{A, \neg A\}$ in $\mathcal{H}$)

We show that $\{A, \neg A\} \vdash_{\mathcal{H}} B$.

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

Exercise on $\mathcal{H}$

Exercise on the Hilbert proof system

Prove that a set of formulas Γ is $\mathcal{H}$-inconsistent if and only if $\Gamma \vdash_{\mathcal{H}} A$ for all formulas A.

Properties of $\mathcal{H}$

It is interesting to check whether the following property hold for $\vdash_{\mathcal{H}}$:

- Reflexivity (If $A \in \Gamma$, then $\Gamma \vdash_{\mathcal{H}} A$)
- Ex falso sequitur quodlibet (If Γ is unsatisfiable, then $\Gamma \vdash_{\Sigma} A$ for all A)
- Monotonicity (If $\Gamma \vdash_{\mathcal{H}} A$ then $\Gamma \cup \Delta \vdash_{\mathcal{H}} A$)
- Cut (If $\Gamma \vdash_{\mathcal{H}} A$ and $\Delta \cup \{A\} \vdash_{\mathcal{H}} B$ then $\Gamma \cup \Delta \vdash_{\mathcal{H}} B$)
- Compactness (If $\Gamma \vdash_{\mathcal{H}} A$, then there is a finite subset $\Gamma_0 \subseteq \Gamma$, such that $\Gamma_0 \vdash_{\mathcal{H}} A$)
- Deduction principle ($\Gamma \cup \{A\} \vdash_{\mathcal{H}} B$ if and only if $\Gamma \vdash_{\mathcal{H}} A \to B$)
- Refutation principle ($\Gamma \vdash_{\mathcal{H}} A$ if and only if $\Gamma \cup \{\neg A\}$ is $\mathcal{H}$-inconsistent)
- Consistency: $\vdash_{\mathcal{H}}$ is consistent (i.e., there is no formula A such that both $\vdash_{\mathcal{H}} A$ and $\vdash_{\mathcal{H}} \neg A$)

Exercises on $\mathcal{H}$

Exercise: deduction theorem in the Hilbert proof system

Prove that the deduction theorem holds for the Hilbert proof system.

Exercise: cut principle in the Hilbert proof system

Prove that the cut principle holds for the Hilbert proof system.

Difference between logical implication and inference

- Logical implication
  - Definition: a formula A is logically implied by a set of formulas Γ if every model of Γ is also a model of A
  - Notation: $\Gamma \models A$
  - Nature: based on semantics, it characterizes the model theoretic view of logic
- Inference
  - Definition: a formula A is inferred from a set of formulas Γ in the proof system Σ if there is a proof of A in Σ from Γ.
  - Notation: $\Gamma \vdash_\Sigma A$, or simply $\Gamma \vdash A$
  - Nature: based on syntax (Σ is concerned with the form of axioms and inference rules), it characterizes the proof theoretic view of logic

Which is the relationship between the two?

Difference between logical implication and inference

- Logical implication
  - Definition: a formula A is logically implied by a set of formulas Γ if every model of Γ is also a model of A
  - Notation: $\Gamma \models A$
  - Nature: based on semantics, it characterizes the model theoretic view of logic
- Inference
  - Definition: a formula A is inferred from a set of formulas Γ in the proof system Σ if there is a proof of A in Σ from Γ.
  - Notation: $\Gamma \vdash_{\Sigma} A$, or simply $\Gamma \vdash A$
  - Nature: based on syntax (Σ is concerned with the form of axioms and inference rules), it characterizes the proof theoretic view of logic

Which is the relationship between the two?

Soundness and completeness of a proof system

Two very important properties of a proof system derive from the relationship between $\vdash_\Sigma$ and $\models$

Soundness

A proof system Σ is sound if for every formula A and every set of formula Γ, we have that $\Gamma \vdash_\Sigma A$ implies $\Gamma \models A$.

Completeness

A proof system Σ is complete if for every formula A and every set of formula Γ, we have that $\Gamma \models A$ implies $\Gamma \vdash_\Sigma A$.

In other words,

- a sound Σ derives only logically implied formulas, and
- a complete Σ derives all logically implied formulas.

The Hilbert proof system is sound and complete

Theorem (Soundness of Hilbert proof system)

If $\Gamma \vdash_{\mathcal{H}} A$ *then* $\Gamma \models A$.

Theorem (Completeness of Hilbert proof system)

If $\Gamma \models A$ *then* $\Gamma \vdash_{\mathcal{H}} A$.

Exercise

Prove that $\mathcal{H}$ is a sound proof system.

Completeness is much more difficult to prove ...

Importance of the Hilbert proof system

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.

However, proofs and inferences in the Hilbert proof system are not very intuitive. Other proof systems are more intuitive (see later). As a matter of facts, nobody is practically using Hilbert system for deduction.

Why is it so important then?

The Hilbert proof systems was the first formal proof system formally defined and studied for any logic. At that time, proof systems were the only hope for mechanizing reasoning!