Chapter 3: Deductive Systems

Definition 3.1

A *deductive system* – or *proof system* – consists of a set of formulas called *axioms* and a set of (formal) *inference rules*.

A *proof* in such a system is a sequence of formulas $A_1, A_2, \ldots, A_n$, each of which either is an axiom or can be inferred from previous formulas in the sequence by means of an inference rule.

The last formula A in a proof is a *theorem*, written $\vdash A$, and the sequence is a proof *of* that theorem. ∎

- If the axioms are all valid, and the inference rules preserve validity, then all theorems are valid, and the deductive system is *sound* ($\vdash A$ implies $\models A$).
- If all valid formulas are theorems, the proof system is *complete* ($\models A$ implies $\vdash A$).
- Deductive systems are particularly useful for logics where validity is undecidable.
- Historically, logics were all about deductive systems, and semantics were neglected (often leading to confusion).
- But a deductive system may offer greater insight than a decision procedure into logical interrelationships …
- for instance, it distinguishes between 'immediate' consequences of axioms and 'deeper' theorems.

Overview

- Two common types of logical deductive systems, or proof systems, are *Hilbert* and *Gentzen* systems.
- Hilbert systems have many axioms and a single inference rule. Gentzen systems feature fewer axioms but many inference rules. While Gentzen systems figure in the computing literature, Hilbert systems are arguably of more fundamental importance, being the basis of mathematical logic.
- We'll study a Hilbert system for propositional logic.
- This deduction system will later be incorporated into a proof system for predicate (first-order) logic.

Hilbert system $\mathscr{H}$

- As usual, capital letters $A,\ B,\ C,\ \ldots$ will be used to represent arbitrary formulas of propositional logic.
- Only the operators $\implies$ and $\neg$ will be used; others will be introduced only as abbreviations.

Definition 3.9 (Deductive system $\mathscr{H}$) The *axioms* of $\mathscr{H}$ are:

Axiom 1 $\vdash (A \implies (B \implies A))$,
Axiom 2 $\vdash (A \implies (B \implies C)) \implies ((A \implies B) \implies (A \implies C))$,
Axiom 3 $\vdash (\neg B \implies \neg A) \implies (A \implies B)$.

The *inference rule* is **modus ponens**:

$$\frac{\vdash A \qquad \vdash A \implies B}{B}$$

– 'method of affirming' (MP for short). ∎

Here,

Theorem 3.10

$$\vdash A \implies A \qquad\qquad (\text{in } \mathscr{H}).$$

Proof:

1. $\vdash (A \Rightarrow ((A \Rightarrow A) \Rightarrow A)) \Rightarrow ((A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A))$ Axiom 2
2. $\vdash A \implies ((A \implies A) \implies A)$ Axiom 1
3. $\vdash (A \implies (A \implies A)) \implies (A \implies A)$ MP, 1, 2
4. $\vdash A \implies (A \implies A)$ Axiom 1
5. $\vdash A \implies A$ MP, 3, 4

$\square$

Strictly speaking, the three 'axioms' given above are really *axiom schemes* or *schemas*: a substitution of any propositional formulas for A, B, and C yields one of infinitely many axioms. Likewise, the 'theorem' is really a *theorem scheme* or *schema*.

At this stage, the proving of theorems of $\mathscr{H}$ is like solving brainteasers, even in the case of formulas that are obviously valid, like that of Theorem 3.10: with few other theorems to help you out, you have to work largely from the axioms and the inference rule themselves. But as the catalogue of proved theorems grows, it becomes easier to formalize arguments on the basis of your logical intuition.

This process is also made easier by the establishment of *derived rules*, which, once proven, can be used as additional inference rules.

3.4 Derived rules in $\mathscr{H}$

- We can derive additional rules of inference.
- For this, extend the definition of a proof:

Definition 3.12 Let $U \subseteq \mathscr{F}$ and $A \in \mathscr{F}$.

- The notation $U \vdash A$ means that the formulas in U are assumptions that may have been used in the proof of A (in addition to the axioms). In other words, A can be deduced from the assumptions U by treating the formulas in U as if they were axioms.
- A proof of A from the set of assumptions U is a sequence of lines $U_i \vdash \phi_i$, where ϕ_i is an axiom or a previously proved theorem, or an assumption in the set U_i, ...

- or, the line $U_i \vdash \phi_i$ is derived from previous lines of the proof via an inference rule or a *derived* rule; and
- the last line of the proof is $U \vdash A$.

$\blacksquare$

Derived rules:

Deduction	$\dfrac{U \cup \{A\} \vdash B}{U \vdash A \rightarrow B}$
Contrapositive	$\dfrac{U \vdash \neg B \rightarrow \neg A}{U \vdash A \rightarrow B}$
Transitivity	$\dfrac{U \vdash A \rightarrow B \qquad U \vdash B \rightarrow C}{U \vdash A \rightarrow C}$
Exchange of antecedent	$\dfrac{U \vdash A \rightarrow (B \rightarrow C)}{U \vdash B \rightarrow (A \rightarrow C)}$
Double negation	$\dfrac{U \vdash \neg\neg A}{U \vdash A}$
Reductio ad absurdum	$\dfrac{U \vdash \neg A \rightarrow \mathit{false}}{U \vdash A}$

We shall prove the **Deduction Rule**. Note that this pattern of reasoning is standard in mathematical proofs: assume A, prove B, conclude that A implies B. In fact, we'll use similar reasoning in this proof.

Let $U \subseteq \mathscr{F}$ and $A \in \mathscr{F}$. We shall show by induction that if there is a deduction of length n of any formula $B \in \mathcal{F}$ from $U \cup \{A\}$, then there is a deduction of $A \Longrightarrow B$ from U.

For the base case, suppose that there is a deduction of length 1 of B from $U \cup \{A\}$. If B is an axiom, or $B \in U$, then $U \vdash B$, and hence, $U \vdash A \Longrightarrow B$, by Axiom 1 and MP. Otherwise, B is A, in which case the result follows from Theorem 3.10. This completes the base case.

For the induction step, suppose that the result holds for $n = m$, and that there is a deduction of length $m+1$ of B from $U \cup \{A\}$. If B is an axiom, or an element of $U \cup \{A\}$, then the result follows from the argument of the base case. Otherwise, two formulas C and $C \Longrightarrow B$ must have deductions from $U \cup \{A\}$ of length k or less. By inductive hypothesis, then, $U \vdash A \Longrightarrow C$ and

$U \vdash A \Longrightarrow (C \Longrightarrow B)$, so the result follows by Axiom 2, and two applications of MP.

The proofs of the other derived rules and theorems of $\mathscr{H}$ listed in the textbook are good exercises. This includes the proofs of the "theorems for other operators."

3.5 Theorems for other operators

– skipped.

3.6 Soundness of $\mathscr{H}$

It is naturally desirable to be able to deduce a formula A from a set of assumptions $U \subseteq \mathscr{F}$ only if A is a logical consequence of U. This property of a deductive system, relating the syntactic property of deducibility to the semantic property of logical consequence, is called *strong soundness*.

Theorem (Strong soundness) The Hilbert system $\mathscr{H}$ satisfies strong soundness: if $U \vdash A$, then $U \models A$.

(Soundness is the weaker property that every theorem of the deductive system is valid – the special case of strong soundness where $U = \emptyset$.)

Proof: Let $\mathscr{I}$ be an arbitrary interpretation for $U \cup \{A\}$ that is a model of U. Because the axioms of $\mathscr{H}$ are all valid, they too are satisfied by $\mathscr{I}$; and modus ponens preserves satisfaction by $\mathscr{I}$. Therefore, any formula deduced from U is also satisfied by $\mathscr{I}$. $\square$

Ideally, the converse – strong completeness – should also hold. Before discussing strong completeness, we should examine the important syntactical issue of *consistency*.

3.7 Consistency

Definition 3.42 Within a deductive system, a set of formulas U is *inconsistent* if both $U \vdash A$ and $U \vdash \neg A$. The set U is *consistent* if it is not inconsistent. The deductive system is inconsistent if its set of theorems is inconsistent.

Theorem 3.43 In $\mathscr{H}$, a set U of formulas is inconsistent iff for all formulas A, $U \vdash A$.

Proof: The 'if' part is immediate. For the converse, let U be inconsistent and suppose that $U \vdash B$ and $U \vdash \neg B$.

It can be shown that $\vdash B \implies (\neg B \implies A)$ (Theorem 3.21 of the textbook). The result follows by two applications of MP. $\square$

Corollary 3.44 The set U is consistent iff for some A, $U \nvdash A$.

By soundness, $\mathscr{H}$ is consistent.

Theorem 3.45 $U \vdash \neg A$ iff $U \cup \{A\}$ is inconsistent.

Proof: The 'only if' part is immediate. For 'if,' suppose that $U \cup \{A\}$ is inconsistent, and therefore $U \cup \{A\} \vdash \neg A$ (Theorem 3.43). Then, by the Deduction Rule, $U \vdash A \Longrightarrow \neg A$. The result follows by Theorem 3.30 of the textbook.

$\square$

(By a similar proof, the result also holds when A and $\neg A$ are interchanged.)

Corollary Let $U \subseteq \mathscr{F}$ be consistent and $A \in \mathscr{F}$. Then either $U \cup \{A\}$ or $U \cup \{\neg A\}$ is consistent.

Proof: If both sets are inconsistent, then by Theorem 3.45, U is inconsistent. $\square$

As a property of a formal deductive system, consistency is a purely syntactic concept. Yet it can be shown to be equivalent to the purely semantic concept of satisfiability. This link makes it easy to prove strong completeness.

A first step is to show that any consistent set of formulas extends to a *maximal* consistent set: a set whose proper supersets are all inconsistent.

Theorem (Henkin) Let $S \subseteq \mathscr{F}$ be consistent. Then there exists a maximal consistent S^* that contains S.

Proof: Because the set of atomic proposition symbols is countably infinite, the same is true of the set of formulas. So the elements of $\mathscr{F}$ can be enumerated:

$$A_1,\ A_2,\ A_3,\ \ldots$$

Define the following nondecreasing sequence of sets of formulas:

$$S_0 = S\ ;$$

$$S_{i+1} = \begin{cases} S_i \cup \{\ \ A_{i+1}\} & \text{, if } S_i \cup \{A_{i+1}\} \text{ is consistent;} \\ S_i \cup \{\neg A_{i+1}\} & \text{, otherwise.} \end{cases}$$

By a simple induction on i, every S_i is consistent. Because proofs are finite, it follows that $S^* := \bigcup_{i \in \mathbb{N}} S_i$ is consistent: any proof of, say, *false* based on S^* assumes only a finite number of elements of S^*; all such elements must be contained in some S_k, but S_k is consistent – a contradiction.

Suppose that S^* is not maximally consistent. Then there is some $A_k \notin S^*$ such that $S^* \cup \{A_k\}$ is consistent. But in that case, $S_{k-1} \cup \{A_k\} \subseteq S^* \cup \{A_k\}$ is consistent, so $A_k \in S_k \subseteq S^*$, a contradiction. □

Of course, we can't generally compute in a finite number of steps all of the subsets S_i, so the construction of the above proof is not computationally 'effective.'

Theorem Any set of propositional formulas is satisfiable if and only if it is consistent.

Proof: Let $S \subseteq \mathscr{F}$ be consistent, and let S^* be the maximal consistent set 'constructed' in the proof of the preceding theorem. Define the interpretation

$$\begin{aligned} \mathscr{I} : \mathscr{P}_{S^*} &\longrightarrow \{T,\ F\} \\ p &\mapsto \begin{cases} T & \text{, if } p \in S^* \text{ ;} \\ F & \text{, if } \neg p \in S^* \text{ .} \end{cases} \end{aligned}$$

This does indeed define an interpretation, because S^* is maximally consistent: for any formula $A \in \mathscr{F}$ (including atomic propositions), either $S^* \cup \{A\}$ or $S^* \cup \{\neg A\}$ is consistent. So by maximality, either $A \in S^*$ or $\neg A \in S^*$ (but not both).

Now it can be shown by structural induction that for any $A \in \mathscr{F}$, $v_{\mathscr{I}}(A) = T$ if and only if $A \in S^*$. Indeed, the base case holds by the definition of $\mathscr{I}$ and the consistency of S^*. For the induction step, suppose first that $A = \neg A_1$; then

$$v_{\mathscr{I}}(A) = T \text{ iff } v_{\mathscr{I}}(A_1) = F \text{ iff } A_1 \notin S^* \text{ iff } A \in S^* \text{ .}$$

(where the second step follows by inductive assumption, and the last by the construction of S^*). On the other hand, if $A = A_1 \Rightarrow A_2$, then

$$\begin{aligned}
v_{\mathscr{I}}(A) = F \text{ iff } & v_{\mathscr{I}}(A_1) = T \ \ \& \ \ v_{\mathscr{I}}(A_2) = F \\
\text{iff } & A_1 \in S^* \ \ \& \ \ A_2 \notin S^* && \text{(ind. hyp.)} \\
\text{iff } & A_1 \in S^* \ \ \& \ \ \neg A_2 \in S^* && \text{(by construction)} \\
\text{iff } & A \notin S^* && (S^* \text{ is maximally consistent,} \\
& && \text{MP, Axiom 1, Thm 3.20)}
\end{aligned}$$

This completes the induction.

It follows that any set is satisfiable if (and only if, by soundness) it is consistent. □

3.8 Strong completeness and compactness

Theorem 3.47 (Strong completeness) Let U be a finite or countably infinite set of formulas, and let A be a formula. If $U \vDash A$ then $U \vdash A$.

Proof: Let $U \subseteq \mathscr{F}$ and $A \in \mathscr{F}$. Then

$$\begin{aligned}
U \vDash A \text{ iff } & U \cup \{\neg A\} \text{ is unsatisfiable} \\
\text{iff } & U \cup \{\neg A\} \text{ is inconsistent} \\
\text{iff } & U \vdash \neg\neg A && \text{Theorem 3.45} \\
\text{iff } & U \vdash A && \text{Double Negation Rule}
\end{aligned}$$

□

Strong completeness in turn implies the following purely semantic property:

Theorem 3.48 (Compactness) Let S be a finite or countably infinite set of formulas and suppose that every finite subset of S is satisfiable. Then S is satisfiable.

Proof outline: By the contrapositive. Suppose that S is not satisfiable. Then, for any A, $S \vDash A$ and $S \vDash \neg A$. But then, by strong completeness, S

is inconsistent. But because a proof is a finite sequence of formulas, there is therefore a finite subset S' of S that is inconsistent:

$$\begin{array}{ll} S' \vdash A \;\&\; S' \vdash \neg A & \\ \text{iff } S' \vDash A \;\&\; S' \vDash \neg A & \qquad \text{strong soundness and completeness} \end{array}$$

That finite subset is therefore unsatisfiable. □

3.9 Variant forms of the deductive systems

– skipped.

3.10 Chapter summary

- Mathematical logic was developed in order to formalize mathematical reasoning in the form of deductive systems.
- Nearly all mathematical theories take the form of Hilbert systems like $\mathscr{H}$:
  - a set of axioms,
  - Modus Ponens as the sole inference rule,
  - proofs as sequences of formulas.
- $\mathscr{H}$ is strongly sound and strongly complete. These properties will take on particular importance when $\mathscr{H}$ is extended to predicate (first-order) logic.
- But in the propositional case, satisfiability, validity, and logical consequence (of a finite set of assumptions) are decidable by means of algorithms. In the next chapters, we shall study more efficient algorithms and data structures than those based on truth tables for establishing such properties.