CHAPTER 2

Learning how to count and reason (Cont'd)

1.5. How to prove things. So formulas have meanings now, which is a great and good thing. That being said, going back to Hilbert's problem, we'd like a way of proving which formulas are always true (i.e. the tautologies) that is fully automated, that is, we'd like a system of proofs that a "computer" whatever that means, could carry out. It would be great if our computer was sound enough to ONLY be able to prove tautologies, and it would be even greater if our computer could prove ALL tautologies.

Recall that we have shown that $\{\rightarrow, \neg\}$ is an adequate set of connectives. In this section, our computer will only have access to these connectives, but of course, since they are adequate, that should be good enough for our purposes (we're only doing this to make life easier, if we wanted to we could really be using more connectives, but we'd have to introduce more axioms).

Let's start by expanding on what this "computer" does:

We will formally refer to the symbolic way of producing proofs as a **proof system**. A proof system comes with some **axioms** (i.e. statements that it assumes are true) and some **deduction rules** (i.e. statements that let it, given stuff it's already proved to prove new stuff).

We will work in a proof system with:

- Axioms:

  (A1) $(\phi \rightarrow (\psi \rightarrow \phi))$

  (A2) $((\phi \rightarrow (\psi \rightarrow \chi)) \rightarrow ((\phi \rightarrow \psi) \rightarrow (\phi \rightarrow \chi)))$

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

  for all formulas ϕ, ψ and χ.

- Deduction Rules:

(MP) GIVEN: $\phi \to \psi$ and ϕ
DEDUCE: ψ

A **formal proof** of formula ϕ is a finite sequence:

$$(\phi_1, \ldots, \phi_n)$$

of formulas such that $\phi_n = \phi$ and for each $i \leq n$, one of the following holds:

- Either ϕ_i is an instance of an axiom;
- Or ϕ_i can be deduced from an instance of (MP) for some $j, k < i$.

If there is a formal proof of ϕ, we write $\vdash \phi$, and call ϕ a **theorem**,

More generally, let Γ be a set of formulas. We say that ϕ is **deducible** from Γ if there is a finite sequence:

$$(\phi_1, \ldots, \phi_n)$$

of formulas such that $\phi_n = \phi$ and for each $i \leq n$, one of the following holds:

- Either ϕ_i is an instance of an axiom;
- Or $\phi_i \in \Gamma$
- Or ϕ_i can be deduced from an instance of (MP) for some $j, k < i$.

In this case, we write $\Gamma \vdash \phi$.[1]

Formal proofs can be rather tedious, but they're fun game to play. This is where it's really really important to keep our brackets close(d).

Example 1.5.1.

(1) $\vdash (\phi \to \phi)$. Here is a deduction:

$$\begin{aligned}
&\phi_1 : (\phi \to ((\phi \to \phi) \to \phi)) && \text{(A1)}\\
&\phi_2 : (((\phi \to ((\phi \to \phi) \to \phi)) \to ((\phi \to (\phi \to \phi)) \to (\phi \to \phi))) && \text{(A2)}\\
&\phi_3 : ((\phi \to (\phi \to \phi)) \to (\phi \to \phi)) && \text{(MP)}\\
&\phi_4 : (\phi \to \phi) && \text{(MP)}
\end{aligned}$$

[1] This is the same as a formal proof of ϕ, where we have added all formulas in Γ to the list of axioms of our formal system.

(2) If $\Gamma = \{(\phi \to \psi), (\psi \to \chi)\}$ then $\Gamma \vdash (\phi \to \chi)$.

$$\begin{aligned}
&\phi_1 : (\psi \to \chi) && \text{(Ass)}\\
&\phi_2 : ((\psi \to \chi) \to (\phi \to (\psi \to \chi))) && \text{(A1)}\\
&\phi_3 : (\phi \to (\psi \to \chi)) && \text{(MP)}\\
&\phi_4 : ((\phi \to (\psi \to \chi)) \to ((\phi \to \psi) \to (\phi \to \chi))) && \text{(A2)}\\
&\phi_5 : ((\phi \to \psi) \to (\phi \to \chi))) && \text{(MP)}\\
&\phi_6 : (\phi \to \psi) && \text{(Ass)}\\
&\phi_7 : (\phi \to \chi) && \text{(MP)}
\end{aligned}$$

First, we shall prove that our computer cannot prove wrong things. This is usually the easy part.

THEOREM 1.5.2 (Soundness of Predicate Logic). *If $\Gamma \vdash \psi$, then $\Gamma \vDash \psi$. In particular, every theorem is a tautology.*

PROOF. We have to show that $\{\phi : \Gamma \vDash \phi\}$ contains all the axioms, all the formulas in Γ and is closed under (MP). But the first part is trivial, since we have already shown that (A1)-(A3) are tautologies (Exercise 2.3.4, and Proposition 2.3.12 – tautologies are closed under substitutions). For the second part, suppose that $\Gamma \vDash (\phi \to \psi)$ and $\Gamma \vDash \phi$. We have to show that $\Gamma \vDash \psi$. But this is exactly Lemma 2.3.11. □

Now, we embark on the slightly longer journey to completeness, i.e. that our computer can prove *all* the things:

THEOREM 1.5.3 (Completeness of Predicate Logic). *If $\Gamma \vDash \psi$ then $\Gamma \vdash \psi$. In particular, every tautology is a theorem.*

First, an appetiser:

Lemma 1.5.4 (The Deduction Theorem)**.** *The following are equivalent:*

(1) $\Gamma \vdash (\phi \to \psi)$.

(2) $\Gamma \cup \{\phi\} \vdash \psi$.

PROOF. Of course, (1) $\implies$ (2) follows immediately by (MP). We really just have to show (2) $\implies$ (1). Let $\phi_1, \ldots, \phi_n$ be a deduction of ψ from $\Gamma \cup \phi$, i.e. $\phi_n = \psi$

We will show by induction on $i \leq n$ that $\Gamma \vdash \phi \to \phi_i$. If ϕ_i is an axiom or an element of Γ, then we have:

$$\begin{aligned} \chi_1 &: \phi_i && \text{(Ass)} \\ \chi_2 &: \phi_i \to (\phi \to \phi_i) && \text{(A1)} \\ \chi_3 &: (\phi \to \phi_i) && \text{(MP)} \end{aligned}$$

If $\phi = \psi$, then we have copy the deduction from Example 1.5.1. Finally, suppose that by induction we have deductions $\Gamma \vdash (\phi \to \phi_j)$ for all $j \leq i$. We wish to show that we have a deduction $\Gamma \vdash (\phi \to \phi_i)$. By assumption, ϕ_i is not an axiom nor an element of Γ, hence it is deducible using (MP) from some ϕ_{j_1}, ϕ_{j_2}. So ϕ_{j_2} must be of the form $\phi_{j_1} \to \phi_i$. By induction we have deductions $\Gamma \vdash (\phi \to \phi_{j_1})$ and $\Gamma \vdash (\phi \to (\phi_{j_1} \to \phi_i))$. Now let us write $\chi_1, \ldots, \chi_n$ and $\chi'_1, \ldots, \chi'_n$ for these two deductions and continue as follows:

$$\begin{aligned} \chi_{2n+1} &: ((\phi \to (\phi_{j_1} \to \phi_i)) \to ((\phi \to \phi_{j_1}) \to (\phi \to \phi))) && \text{(A2)} \\ \chi_{2n+2} &: ((\phi \to \phi_{j_1}) \to (\phi \to \phi)) && \text{(MP)} \\ \chi_{2n+3} &: (\phi \to \phi_i) && \text{(MP)} \end{aligned}$$

This does the trick. □

Exercise 1.5.5. Let Γ be a set of formulas. Prove that:

(1) If $\phi, \psi \in \Gamma$, then $\Gamma \vdash (\phi \to \psi)$.

(2) If $\neg\phi \in \Gamma$, then $\Gamma \vdash (\phi \to \psi)$ for any formula ψ.

(3) $\phi \to (\psi \to \chi) \vdash \psi \to (\phi \to \chi)$

Now for a little amuse bouche:

Definition 1.5.6. We say that a set of formulas Γ is *inconsistent* if there is a formula ϕ such that $\Gamma \vdash \phi$ and $\Gamma \vdash \neg\phi$. Otherwise, we say that Γ is *consistent*.

It is at no loss to our proof system to assume that $\top$ is an axiom. Of course $\top$ is shorthand for $\neg\bot$. This gives us an alternative characterisation of inconsistency:

Lemma 1.5.7 (The Adequacy Theorem)**.** *If* Γ *is unsatisfiable, then* Γ *is inconsistent.*

Before proving the Adequacy Theorem (whose proof is really the heart of everything), let's see how it implies the completeness theorem:

PROOF. Suppose that $\Gamma \vDash \phi$. Then, $\Gamma \cup \{\neg\phi\}$ is unsatisfiable. So, by the Adequacy Lemma, it is inconsistent, and therefore we have that $\Gamma \cup \{\neg\phi\} \vdash \psi$ and $\Gamma \cup \{\neg\phi\} \vdash \neg\psi$, for some formula ψ. By the Deduction theorem, we have that $\Gamma \vdash (\neg\phi \to \neg\psi)$ and $\Gamma \vdash (\neg\phi \to \psi)$ and hence by (A3) and two applications of (MP) we have that $\Gamma \vdash \phi$. □

This proof was like way too easy. The real difficulty is in the proof of the Adequacy Lemma. This will be the hardest proof we've done so far, so let's pull up our sleeves and do it!

PROOF OF THE ADEQUACY LEMMA. We will prove the contrapositive, that is:

If Γ is consistent, then Γ is satisfiable.

What this means is that from the PURELY SYMBOLIC assumption that for all formulas ψ we have that $\Gamma \nvdash \psi$ or $\Gamma \nvdash \neg\psi$ we will have to build an assignment $\mathcal{A} \in \mathbb{A}$ such that $\phi[\mathcal{A}] = T$ for all $\phi \in \Gamma$.

- Step 1. Enumerate all the formulas – Since Var is countable, the set of all propositional formulas is countable, so there is an enumeration $\{\phi_1, \phi_2, \dots\}$.
- Step 2. Define $\Gamma_0 = \Gamma$. This is consistent. Then, inductively define:

  $$\Gamma_n = \begin{cases} \Gamma_{n-1} \cup \{\phi_n\} & \text{if this set is consistent} \\ \Gamma_{n-1} \cup \{\neg\phi_n\} & \text{otherwise.} \end{cases}$$

  By definition, if $\Gamma_{n-1} \cup \{\phi_n\}$ is inconsistent, then $\Gamma_{n-1} \cup \{\phi_n\} \vdash \psi$ and $\Gamma_{n-1} \cup \{\phi_n\} \vdash \neg\psi$, for some formula ψ. By the deduction theorem, (A3) and (MP) applied twice we have that $\Gamma_{n-1} \vdash \neg\phi$ an hence $\Gamma_{n-1} \cup \{\neg\phi_n\}$ is consistent (since, if $\Gamma_{n-1} \vdash \neg\phi_n$, then for any formula ϕ we have that $\Gamma_{n-1} \vdash \psi$ if and only if $\Gamma_{n-1} \cup \{\neg\phi_n\} \vdash \psi$, but the former was assumed to be consistent, by induction).
- Step 3. Let $\Gamma' = \bigcup_{n\in\mathbb{N}} \Gamma_n$. Then Γ' is consistent. If not, then there is a formula ψ such that $\Gamma' \vdash \psi$ and $\Gamma' \vdash \neg\psi$, but then, there is a finite sequence of formulas $\phi_1, \dots, \phi_k \in \Gamma'$ which is a proof of ψ and a finite sequence of formulas $\phi'_1, \dots, \phi'_l \in \Gamma'$ which is a proof of $\neg\psi$. But these proofs (together) would have shown up in some Γ_n, a contradiction. By construction, for every formula ϕ we have that exactly one of ϕ and $\neg\phi$ is in Γ'.
- Step 4. Define a valuation $\mathcal{A}$ by setting $\mathcal{A}(A) = T$ if and only if $A \in \Gamma'$.

- Step 5. Show that for all ϕ we have that $\phi[\mathcal{A}] = T$ if and only if $\phi \in \Gamma'$. We prove this by induction on ϕ.
  - Case I. ϕ is a propositional variable A. Then, by definition of $\mathcal{A}$ we have that $A \in \Gamma'$ if and only if $A[\mathcal{A}] = T$.
  - Case II. ϕ is of the form $(\neg\psi)$. By inductive hypothesis we have that $\psi[\mathcal{A}] = T$ if and only if $\psi \in \Gamma$. If $(\neg\psi)[\mathcal{A}] = T$, then $\psi[\mathcal{A}] = F$ so $\psi \notin \Gamma'$ and hence $(\neg\psi) \in \Gamma'$. Similarly, if $\psi[\mathcal{A}] = F$, then $\psi \in \Gamma'$ so $(\neg\psi) \notin \Gamma'$.
  - Case III. ϕ is of the form $(\psi \to \chi)$. By inductive hypothesis we have that $\chi[\mathcal{A}] = T$ if and only if $\chi \in \Gamma'$ and similarly $\psi[\mathcal{A}] = T$ if and only if $\psi \in \Gamma'$.

    First, we show that if $(\psi \to \chi)[\mathcal{A}] = T$, then $(\psi \to \chi) \in \Gamma'$:

    * Case III(a). If $\psi[\mathcal{A}] = T$ then we must have that $\chi[\mathcal{A}] = T$, since $(\psi \to \chi)[\mathcal{A}] = T$. It follows that $\psi, \chi \in \Gamma'$ and hence $\Gamma' \vdash (\psi \to \chi)$. Since $(\psi \to \chi)$ is a formula, it is ϕ_n, for some $n \in \mathbb{N}$. Then, $\Gamma_{n-1} \cup \{(\psi \to \chi)\}$ is consistent. If not, then we have that $\Gamma_n = \Gamma_{n-1} \cup \{\neg(\psi \to \chi)\}$, so $\Gamma' \vdash \neg(\psi \to \chi)$, but then Γ' would be inconsistent. Thus, we have that $(\psi \to \chi) \in \Gamma_n \subseteq \Gamma'$.
    * Case III(b). If $\psi[\mathcal{A}] = F$, then we have that $\psi \notin \Gamma'$, and hence (arguing as above) we have that $\neg\psi \in \Gamma'$. Thus, by Exercise 1.5.5(2) we have that $\Gamma' \vdash (\psi \to \chi)$ and arguing again as above we have that $(\psi \to \chi) \in \Gamma'$.

    Next we show that if $(\psi \to \chi)[\mathcal{A}] = F$, then $(\psi \to \chi) \notin \Gamma'$. In this case, we have that $\psi[\mathcal{A}] = T$, so $\psi \in \Gamma'$ and $\chi[\mathcal{A}] = F$, so $\chi \notin \Gamma'$. If $\psi \to \chi \in \Gamma'$ then, since $\psi \in \Gamma'$, by (MP) we would have that $\chi \in \Gamma'$, a contradiction.
- Step 6. Tie up all loose ends. Since there is an assignment $\mathcal{A}$ which makes all formulas in Γ' true, and $\Gamma \subseteq \Gamma'$ we have that for all $\phi \in \Gamma$, $\phi[\mathcal{A}] = T$, so Γ is satisfiable. □

Phew! We got through that. Let's get some nice corollaries:

Corollary 1.5.8 (Propositional Compactness)**.** *If $\Gamma \vDash \phi$, then there is a finite subset $\Delta \subseteq \Gamma$ such that $\Delta \vDash \phi$.*

PROOF. Since $\Gamma \vDash \phi$ if and only if $\Gamma \vdash \phi$, there is a deduction $\phi_0, \ldots, \phi_n$. Only finitely many formulas from Γ appear in this deduction, so there is some finite subset $\Delta \subseteq \Gamma$ such that $\Delta \vdash \phi$, but then $\Delta \vDash \phi$. □

Corollary 1.5.9 (Decidability of Propositional Logic)**.** *There is an "algorithm"*[2] *which given a finite set of propositional formulas* Γ *and a formula* ϕ *determines whether or not* $\Gamma \vdash \phi$*.*

PROOF. Write out the truth table of Γ and ϕ, if in every row in which all entries from Γ are T we have that ϕ is T then $\Gamma \vDash \phi$ and so $\Gamma \vdash \phi$. That's the algorithm! □

So what, you could say, well proofs are finite sequences, so given Γ just start writing out proofs. If $\Gamma \vdash \phi$ then the proof of ϕ will eventually show up. The problem is that we don't know if our machine is still running because it hasn't found a proof yet or because a proof does not exist!

A limitation which is certainly beyond the scope of this section:

FACT. *There is no algorithm which given a set of axioms can decide if the proof system with that set of axioms together with (MP) is complete.*

[2] See later.

Homework 2