Logic and Computation: I

Chapter 2 Propositional logic and computational complexity

Kazuyuki Tanaka

BIMSA

November 22, 2022

北京雁栖湖应用数学研究院
YANQI LAKE BEIJING INSTITUTE OF MATHEMATICAL SCIENCES AND APPLICATIONS

Logic and Computation I

- **Part 1. Introduction to Theory of Computation**
- **Part 2. Propositional Logic and Computational Complexity**
- **Part 3. First Order Logic and Decision Problems**

Part 2. Schedule

- Nov.17, (1) Tautologies and proofs
- Nov.22, (2) The completeness theorem of propositional logic
- Nov.24, (3) SAT and NP-complete problems
- Nov.29, (4) NP-complete problems about graph
- Dec. 1, (5) Time-bound and space-bound complexity classes
- Dec. 6, (6) PSPACE-completeness and TQBF

Recap

- Propositional logic is the study of logical connections between propositions.

  $\neg$ (not $\cdots$), $\wedge$ (and), $\vee$ (or), $\rightarrow$ (implies).

- If a proposition φ is always true, i.e., $V(\varphi) = \mathrm{T}$ for any truth-value function V, then φ is said to be **valid** or a **tautology**, written as $\models \varphi$.

- The followings are tautologies.

  P1. $\varphi \rightarrow (\psi \rightarrow \varphi)$

  P2. $\big(\varphi \rightarrow (\psi \rightarrow \theta)\big) \rightarrow \big((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \theta)\big)$

  P3. $(\neg\psi \rightarrow \neg\varphi) \rightarrow (\varphi \rightarrow \psi)$

- P1 was shown on p.11 of the last note. P2 is shown as below.

  $\because$ By way of contradiction, there exists a truth-value function V such that $V((\varphi \rightarrow (\psi \rightarrow \theta)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \theta))) = \mathrm{F}$. By condition (2d) of Def. of V, $V(\varphi \rightarrow (\psi \rightarrow \theta)) = \mathrm{T}$ and $V((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \theta)) = \mathrm{F}$. From the latter, $V(\varphi \rightarrow \psi) = \mathrm{T}$ and $V(\varphi \rightarrow \theta) = \mathrm{F}$, and then from the latter, $V(\varphi) = \mathrm{T}$, $V(\theta) = \mathrm{F}$. Then by the former $V(\varphi \rightarrow \psi) = \mathrm{T}$, $V(\psi) = \mathrm{T}$. Hence, $V(\varphi) = V(\psi) = \mathrm{T}$ and $V(\theta) = \mathrm{F}$, therefore $V(\varphi \rightarrow (\psi \rightarrow \theta)) = \mathrm{F}$, a contradiction.

  P3 can be proved similarly.

- We consider an axiomatic system that derives all valid propositions only using $\neg, \to$. We can omit $\vee$ and $\wedge$ by setting $\varphi \vee \psi := \neg\varphi \to \psi$, $\varphi \wedge \psi := \neg(\varphi \to \neg\psi)$.

- A **proof** is a sequence of propositions $\varphi_0, \varphi_1, \cdots, \varphi_n$ satisfying the following conditions: For $k \leq n$,
  (1) φ_k is one of axioms $\mathrm{P1}$, $\mathrm{P2}$, $\mathrm{P3}$, or
  (2) There exist $i, j < k$ such that $\varphi_j = \varphi_i \to \varphi_k$ (MP).

  The last component of proof φ_n is called a **theorem**, and we denote $\vdash \varphi_n$.

- P1, P2, P3 are theorems by themselves. $\varphi \to \varphi$ was proved on p.18 of the last note.

- $\neg\varphi \to (\varphi \to \psi)$ (homework) can be proved as follows.
  First, we show that if A is a theorem, then for any B, $B \to A$ is a theorem.
  By P1, $A \to (B \to A)$. By applying MP to this and A, we have $B \to A$.
  Now, from this and P3, we have $\neg\varphi \to ((\neg\psi \to \neg\varphi)) \to (\varphi \to \psi))$. By P2,
  $(\neg\varphi \to ((\neg\psi \to \neg\varphi) \to (\varphi \to \psi))) \to ((\neg\varphi \to (\neg\psi \to \neg\varphi)) \to (\neg\varphi \to (\varphi \to \psi)))$.
  By MP, we have $(\neg\varphi \to (\neg\psi \to \neg\varphi)) \to (\neg\varphi \to (\varphi \to \psi))$. By applying MP to this and P1, we have $\neg\varphi \to (\varphi \to \psi)$.

- In this lecture, we will prove the completeness theorem: $\vdash \varphi \Leftrightarrow \models \varphi$.

Completeness theorem for propositional logic

We first extend the concept "Proof" as follows.

Definition (Proof)

Given a set of propositions Γ, a sequence of propositions $\psi_0, \psi_1, \cdots, \psi_n$ is said to be a **proof** of ψ_n in Γ if for each $k \leq n$,

(1) ψ_k belongs to $\{P_1, P_2, P_3\} \cup \Gamma$, or

(2) There exist $i, j < k$ such that $\psi_j = \psi_i \to \psi_k$.

If there exists a proof of ψ in Γ, then ψ is said to be **provable** in Γ, or a **theorem** of Γ, written as $\Gamma \vdash \psi$.

The definitions of a proof and a theorem in the last lecture are obtained as a special case by setting $\Gamma = \varnothing$.

Theorem (Deduction Theorem)

If $\Gamma \cup \{\varphi\} \vdash \psi$, $\Gamma \vdash \varphi \to \psi$.

Proof. Let $\psi_0, \psi_1, \cdots, \psi_k (= \psi)$ be a proof of ψ in $\Gamma \cup \{\varphi\}$. We prove by induction on the proof length $k+1$.

Case $k = 0$

(1) If ψ belongs to $\{P_1, P_2, P_3\} \cup \Gamma$, the following is a proof of $\varphi \to \psi$ in Γ.

$$\begin{aligned} \varphi_0 &= \psi && : \text{in } \{P_1, P_2, P_3\} \cup \Gamma \\ \varphi_1 &= \psi \to (\varphi \to \psi) && : P1 \\ \varphi_2 &= \varphi \to \psi && : \varphi_1 = \varphi_0 \to \varphi_2 \end{aligned}$$

(2) If $\psi = \varphi$, $\varphi \to \psi$ is the same as $\varphi \to \varphi$, which was proved in the last lecture.

Case $k \geq 1$

(1) If $\psi_k = \psi$ belongs to $\{P_1, P_2, P_3\} \cup \Gamma \cup \{\varphi\}$, the same as case $k = 0$.

(2) Consider the case where there exist $i, j < k$ and $\psi_j = \psi_i \to \psi_k$.

- By the induction hypothesis, we have $\Gamma \vdash \varphi \to \psi_i$ and $\Gamma \vdash \varphi \to \psi_j$.
- Let $\varphi_0, \varphi_1, \cdots, \varphi_m$ be a proof of $\varphi \to \psi_i$ in Γ, and let $\varphi_{m+1}, \cdots, \varphi_n$ be a proof of $\varphi \to \psi_j$ in Γ.
- Then $\varphi_0, \cdots, \varphi_m, \varphi_{m+1}, \cdots, \varphi_n$ is also a proof of $\varphi \to \psi_j$ in Γ.
- If we add the following $\varphi_{n+1}, \varphi_{n+2}, \varphi_{n+3}$ after $\varphi_0, \cdots, \varphi_n$, we obtain a proof of $\varphi \to \psi$ in Γ.

$$\begin{aligned}
\varphi_{n+1} &= (\varphi \to (\psi_i \to \psi_k)) \to ((\varphi \to \psi_i) \to (\varphi \to \psi_k)) && : P2 \\
\varphi_{n+2} &= (\varphi \to \psi_i) \to (\varphi \to \psi_k) && : \varphi_{n+1} = \varphi_n \to \varphi_{n+2} \\
\varphi_{n+3} &= \varphi \to \psi_k && : \varphi_{n+2} = \varphi_m \to \varphi_{n+3}
\end{aligned}$$

The converse of Deduction Theorem "If $\Gamma \vdash \varphi \to \psi$, $\Gamma \cup \{\varphi\} \vdash \psi$" can be obtained directly by Modus Ponens.

The following example demonstrate the application of Deduction Theorem.

Example: Using the deduction theorem to show $\vdash \neg\varphi \to (\varphi \to \psi)$

- By the deduction theorem, it suffices to show $\{\neg\varphi, \varphi\} \vdash \psi$.
- Since $\{\neg\varphi, \varphi\} \vdash \neg\varphi$, then using MP to P1 and this, we have $\{\neg\varphi, \varphi\} \vdash \neg\psi \to \neg\varphi$.
- By applying MP to P3, $\{\neg\varphi, \varphi\} \vdash \varphi \to \psi$.
- Again by MP, $\{\neg\varphi, \varphi\} \vdash \psi$.

- This last example asserts that the contradiction ($\neg\varphi$ and φ) implies any proposition ψ.
- We investigate this in more detail. Let $\perp$ be a proposition representing "contradiction", say $\neg(p_0 \to p_0)$.

Definition (Inconsistent)

The set Γ of propositions is said to be **inconsistent** if $\perp$ is provable from Γ. Otherwise, Γ is said to be **consistent**.

Lemma (1)

$\Gamma \vdash \psi$ for any ψ if Γ is inconsistent.

$\because$ If Γ is inconsistent, $p_0 \to p_0$ and $\neg(p_0 \to p_0)$ are provable in Γ.

Lemma (2)

If there exists φ such that $\Gamma \vdash \varphi$ and $\Gamma \vdash \neg\varphi$, then Γ is inconsistent.
That is, if Γ is consistent, then for any φ, φ or $\neg\varphi$ cannot be proved from Γ.

The following lemma establishes the basic principle connecting the notions of provability and contradiction.

Lemma (3)

$\Gamma \cup \{\neg\varphi\}$ is inconsistent $\Leftrightarrow \Gamma \vdash \varphi$.

Proof.
To show $\Rightarrow$.
Assume $\Gamma \cup \{\neg\varphi\} \vdash \neg(p_0 \to p_0)$. By Deduction Theorem, $\Gamma \vdash \neg\varphi \to \neg(p_0 \to p_0)$. So by P3, $\Gamma \vdash (p_0 \to p_0) \to \varphi$. By $\vdash (p_0 \to p_0)$, thus $\Gamma \vdash \varphi$.
To show $\Leftarrow$.
If $\Gamma \vdash \varphi$, $\Gamma \cup \{\neg\varphi\}$ can prove both φ and $\neg\varphi$. So $\Gamma \cup \{\neg\varphi\}$ is inconsistent. □

Therefore,

Lemma (4)

If Γ is consistent, then for any φ, $\Gamma \cup \{\varphi\}$ or $\Gamma \cup \{\neg\varphi\}$ is consistent.

This lemma lays the basis of the proof for completeness theorem.

Completeness theorem for propositional logic

Theorem (Completeness theorem for propositional logic)

$\vdash \varphi \quad \Longleftrightarrow \quad \models \varphi$

Proof

$\vdash \varphi \Longrightarrow \models \varphi$

- Let V be any truth value function.
- If φ is the axiom $\mathrm{P1}$, $\mathrm{P2}$, $\mathrm{P3}$, $V(\varphi) = \mathrm{T}$.
- Also, if $V(\varphi) = \mathrm{T}$ and $V(\varphi \to \psi) = \mathrm{T}$, then $V(\psi) = \mathrm{T}$.
- Thus, for all theorems φ, $V(\varphi) = \mathrm{T}$.

$\vdash \varphi \Longleftarrow\ \models \varphi$

- Suppose that proposition φ is not a theorem.
  Goal: prove there exists a truth value function V s.t. $V(\varphi) = \mathrm{F}$.
- List all the propositions in an appropriate order as $\varphi_0, \varphi_1, \varphi_2, \cdots$.
- Given $\Gamma_0 = \{\neg\varphi\}$[1], we define an infinitely increasing sequence of consistent sets $\Gamma_0 \subseteq \Gamma_1 \subseteq \Gamma_2 \subseteq \cdots$ as follows. For any $n \geq 0$,
  - if $\Gamma_n \cup \{\varphi_n\}$ is consistent, $\Gamma_{n+1} = \Gamma_n \cup \{\varphi_n\}$;
  - otherwise $\Gamma_{n+1} = \Gamma_n$.
- Then $\Gamma = \bigcup_n \Gamma_n$ is consistent.
  - Suppose Γ were inconsistent. Since the number of elements of Γ used in the proof of $\perp$ is finite, there is a sufficiently large N s.t. Γ_N includes all such elements. Therefore, $\Gamma_N \vdash \perp$, which violates the consistency of Γ_N.

[1]: Γ_0 is consistent by Lemma (3)

$\vdash \varphi \Longleftarrow\ \models \varphi$ (continued)

- Furthermore, Γ is a maximal consistent set. That is, either $\varphi_n \in \Gamma$ or $\neg\varphi_n \in \Gamma$ holds for any φ_n.
- Suppose $\Gamma \nvdash \varphi_n$. Then, $\Gamma \cup \{\neg\varphi_n\}$ is consistent. So letting $\varphi_m = \neg\varphi_n$, $\Gamma_m \cup \{\varphi_m\}$ is consistent, and so $\varphi_m \in \Gamma_{m+1} \subseteq \Gamma$, that is, $\neg\varphi_n \in \Gamma$.
- Similarly, if $\Gamma \nvdash \neg\varphi_n$, then $\varphi_n \in \Gamma$.
- Since Γ is consistent, by Lemma (2) φ_n or $\neg\varphi_n$ cannot be proved from Γ, and so φ_n or $\neg\varphi_n$ belongs to Γ.
- Thus we note that for any formula φ_n, $\varphi_n \notin \Gamma \Leftrightarrow \neg\varphi_n \in \Gamma$.

$\vdash \varphi \Longleftarrow \models \varphi$ (continued)

- Now, define a function V as follows:

$$V(\varphi_n) = \mathrm{T} \Leftrightarrow \varphi_n \in \Gamma_{n+1}.$$

- We then show that V is a truth value function.
  - It follows from the maximal consistency that

$$V(\neg\varphi_n) = \mathrm{T} \Leftrightarrow V(\varphi_n) = \mathrm{F}.$$

  - By the maximal consistency, we also show $\varphi_m \to \varphi_n \in \Gamma \Leftrightarrow \neg\varphi_m \in \Gamma$ or $\varphi_n \in \Gamma$. Then we have

$$V(\varphi_m \to \varphi_n) = \mathrm{T} \Leftrightarrow V(\varphi_m) = \mathrm{F} \text{ or } V(\varphi_n) = \mathrm{T}.$$

- It is clear that $V(\varphi) = \mathrm{F}$ since $\Gamma_0 = \{\neg\varphi\}$. Thus V is a truth-value function that assigns the value F to φ, and so φ is not a tautology.

- As we generalized provability $\vdash$, we can also generalize validity $\models$.
- By $\Gamma \models \varphi$, we mean that if a truth-value function V assigns the value T to all propositions in Γ then it assigns the value T to φ. In such a case, φ is called the **tautological consequence** of Γ.
- The completeness theorem can also be generalized as follows.

Theorem (The generalized completeness theorem of propositional logic)

$$\Gamma \vdash \varphi \quad \Longleftrightarrow \quad \Gamma \models \varphi.$$

Proof.
(To show $\Rightarrow$) Let V be a truth-value function that assigns the value T to all propositions in Γ. For the three axioms φ, we have already seen $V(\varphi) = \mathrm{T}$. Also, when $V(\varphi) = \mathrm{T}$ and $V(\varphi \to \psi) = \mathrm{T}$, $V(\psi) = \mathrm{T}$. Thus, for all theorems φ derived from Γ, $V(\varphi) = \mathrm{T}$.
(To show $\Leftarrow$) Suppose that the proposition φ is not a theorem of Γ. It suffices to show that there exists a truth-value function V that assigns value T to all propositions of Γ and value F to φ. To construct such a V, just replace $\Gamma_0 = \Gamma \cup \{\neg\varphi\}$ in the proof of the last theorem. □

- We say that Γ is **satisfiable** if there is a truth value function that assigns the value T to all propositions belonging to Γ.

  We can state the completeness theorem as follows.

Completeness theorem (another version)

Γ is consistent $\iff$ Γ is satisfiable.

- Γ is consistent
  - $\Leftrightarrow$ $\Gamma \nvdash \bot$
  - $\Leftrightarrow$ $\Gamma \not\models \bot$
  - $\Leftrightarrow$ there is a V that assigns T to all in Γ but F to $\bot$
  - $\Leftrightarrow$ there is a V that assigns T to all in Γ
  - $\Leftrightarrow$ Γ is satisfiable.

Theorem (Compactness theorem of propositional logic)

If any finite subset of Γ is satisfiable, then Γ is also satisfiable.

Proof.

- By contrapositive method, suppose no truth-value function assigns the value T to all propositions in Γ. Goal: there is some finite subset $\Gamma' \subset \Gamma$ s.t. there is no truth-value function that assigns the value T to all propositions of Γ'.
- Now, by assumption, any proposition is a tautological consequence of Γ, especially $\Gamma \models \bot$.
- Thus, by the generalized completeness theorem, we get $\Gamma \vdash \bot$.
- Since the proof consists of a finite number of propositions, there exists a finite subset Γ' of Γ such that $\Gamma' \vdash \bot$.
- Again, by the generalized completeness theorem, $\Gamma' \models \bot$.
- Since there is no truth-value function that assigns the value T to $\bot$, a truth-value function that assigns the value T to all propositions in Γ' does not exist.

The name of compactness theorem comes from the Heine-Borel compactness of topological spaces.

Alternative proof for compactness theorem

- Consider $X = \{\mathrm{T}, \mathrm{F}\}^{\mathbb{N}}$ as a topological space with product topology. $\{\mathrm{T}, \mathrm{F}\}$ has a discrete topology. Since every finite space is compact, the product space X is also compact by Tikhonov's theorem (also equivalent to the finite intersections property).
- Elements of X can be interpreted as functions v that assign truth values T, F to atomic propositions $p_0, p_1, p_2, \cdots$.
- Also, the function v can be uniquely extended to the truth value function $V = \bar{v}$, so they are interchangeable.
- Now, for a proposition φ, let C_φ be the set of functions v that assign T to φ. That is, $C_\varphi = \{v \in X : \bar{v}(\varphi) = \mathrm{T}\}$.
- Since there are only finite atomic propositions in φ, C_φ is a clopen (i.e., closed and open) set of X.
- In fact, C_φ is obtained by finite Boolean operations from an open and closed set of the form $B_i = \{v \in X : v(i) = \mathrm{T}\}$.

Homework:Use the compactness theorem to prove the following

An infinite graph (vertices) can be colored with k colors (each edge has a different color at each end) iff any finite subgraph of it can be colored with k colors.

Summary

We have shown

- Deduction theorem: If $\Gamma \cup \{\varphi\} \vdash \psi$, $\Gamma \vdash \varphi \to \psi$.
- Completeness theorem: $\Gamma \vdash \varphi \quad \Leftrightarrow \quad \Gamma \models \varphi$.
- Completeness theorem (another version): Γ is consistent $\quad \Leftrightarrow \quad$ Γ is satisfiable.
- Compactness theorem: If any finite subset of Γ is satisfiable, then Γ is also satisfiable.

Further readings

E. Mendelson. *Introduction to Mathematical Logic*, CRC Press, 6th edition, 2015.

Thank you for your attention!