Proof Theory

Ikhan Choi
Lectured by Toshiyasu Arai
University of Tokyo, Spring 2023

May 1, 2023

Contents

1 Day 1: April 10

In this lecture we only consider classical 1st order logic.

Completeness theorem

$$\text{logically valid} \quad \Leftrightarrow \quad \text{provable}$$

If a statement is provable, then it is true, isn't it? If a statement can't be proved, then it is not true, is it? No!

Most references share the common notion of logical validity, but provability slightly differs although they are same eventually. Provability depends on the choice of axioms and inference rules, and we will choose G. Gentzen's(1934/35).

Informally,

- a *formula* is a formal expression which represents propositions,
- the truth of a formula is determined by a *structure* and *satisfaction relation*,
- a *language* can give strucures their shapes.

Definition 1.1. A language is a set $\mathcal{L}$ of symbols. The set of symbols $\mathcal{L} = \mathcal{F} \cup \mathcal{P}$ are divided into two categories: functions and predicates(also called relations or conditions). A non-negative integer, called arity, is assigned to each symbol. A 0-ary function is called a constant. We will write the set of n-ary function symbols as $\mathcal{F}_n$ and n-ary predicate symbols as $\mathcal{P}_n$. (Symbols given in a language is somtimes called non-logical symbols, because they depend on the definition of languages.)

Definition 1.2. Let $\mathcal{L}$ be a language. An $\mathcal{L}$-structure is a pair $\mathcal{M} = (M, F)$ of a set M and a function F with domain $\mathcal{L}$ such that $F(p) = p^{\mathcal{M}} \subset M^n$, $F(f) = f^{\mathcal{M}} : M^n \to M$.

Definition 1.3 (Term)**.** Let $\mathcal{L}$ be a language. A variable is an element of a countable set Var such that $\mathrm{Var} \cap \mathcal{L} = \emptyset$. A term is an element of $\mathrm{Tm}_{\mathcal{L}}$, recursively defined such that

(a) $\mathrm{Var} \subset \mathrm{Tm}_{\mathcal{L}}$,

(b) If $t_1, \cdots, t_n \in \mathrm{Tm}_{\mathcal{L}}$ and $f \in \mathcal{F}_n$, then $f(t_1, \cdots, t_n) \in \mathrm{Tm}_{\mathcal{L}}$.

Let $\mathcal{M}$ be an $\mathcal{L}$-structure and let $\mathcal{L}(\mathcal{M}) := \mathcal{L} \cup \{c_\alpha : \alpha \in M\}$. $\mathcal{M}$ is a $\mathcal{L}(\mathcal{M})$-structure by letting $c_\alpha^{\mathcal{M}} := \alpha$. A closed term is a term which does not contain any variables, so that it is recursively constructed from constants by functions. Let $\mathcal{M}$ be an $\mathcal{L}$-structure and t be a closed $\mathcal{L}(\mathcal{M})$-term. If $t \equiv f(t_1, \cdots, t_n)$ (completely equal as sequences of symbols), then $t^{\mathcal{M}}$ is recursively defined by $t^{\mathcal{M}} := f^{\mathcal{M}}(t_1^{\mathcal{M}}, \cdots, t_n^{\mathcal{M}}) \in M$.

Definition 1.4 (Formula)**.** Let $\mathcal{L}$ be a language. A formula is an element of $\mathrm{Fml}_{\mathcal{L}}$, recursively defined such that

(a) if $t_1, \cdots, t_n \in \mathrm{Tm}_{\mathcal{L}}$ and $p \in \mathcal{P}_n$, then $p(t_1, \cdots, t_n) \in \mathrm{Fml}_{\mathcal{L}}$,

(b) if $A, B \in \mathrm{Fml}_{\mathcal{L}}$, then $\neg A$, $A \vee B$, $A \wedge B$, $A \to B \in \mathrm{Fml}_{\mathcal{L}}$,

(c) if $A \in \mathrm{Fml}_{\mathcal{L}}$ and $x \in \mathrm{Var}$, then $\exists x A$, $\forall x A \in \mathrm{Fml}_{\mathcal{L}}$.

The symbols $\neg$, $\vee$, $\wedge$, $\to$ are called connectives, and the symbols $\exists$, $\forall$ are called quantifiers. They are called logical symbols, which does not depend on languages.

Definition 1.5 (Free variables)**.** For a term t, the set $\mathrm{Var}(t) \subset \mathrm{Var}$ is defined as

(a) if $x \in \mathrm{Var}$, then $\mathrm{Var}(x) = \{x\}$,

(b) $\mathrm{Var}(f(t_1, \cdots, t_n)) = \bigcup_{i=1}^n \mathrm{Var}(t_i)$.

For a formula A, the set $\mathrm{Var}(A) \subset \mathrm{Var}$ is defined as

(a) $\mathrm{Var}(p(t_1,\cdots,t_n)) = \bigcup_{i=1}^{n} \mathrm{Var}(t_i)$.

(b) if $\circ \in \{\vee, \wedge, \to\}$, then $\mathrm{Var}(A \circ B) = \mathrm{Var}(A) \cup \mathrm{Var}(B)$,

(c) if $\circ \in \{\exists, \forall\}$ and $x \in \mathrm{Var}$, then $\mathrm{Var}(\circ x\, A) = \mathrm{Var}(A) \setminus \{x\}$.

An element of $\mathrm{Var}(A)$ is called a free variable, and a formula A is said to be closed if $\mathrm{Var}(A) = \varnothing$.

Definition 1.6 (Satisfiability relation)**.** Let A be a closed formula over $\mathcal{M}$. We write $\mathcal{M} \models A$ and say A holds on $\mathcal{M}$ or $\mathcal{M}$ satisfies A if

(a) $\mathcal{M} \models p(t_1,\cdots,t_n)$ iff $(t_1^{\mathcal{M}},\cdots,t_n^{\mathcal{M}}) \in p^{\mathcal{M}}$,

(b) $\mathcal{M} \models \neg A$ iff $\mathcal{M} \not\models A$,

(c) $\mathcal{M} \models A \vee B$ iff $\mathcal{M} \models A$ or $\mathcal{M} \models B$ (similarly for $\wedge$ and $\to$),

(d) $\mathcal{M} \models \exists x\, A$ iff there is $\alpha \in M$ such that $\mathcal{M} \models A[x := c_\alpha]$, where $A[x := c_\alpha]$ is the result of replacing the variable x by c_α in A (similarly for $\forall$).

2 Day 2: April 17

Let A be a formula. Then, the universal closure is $\forall(A) := \forall x_1 \cdot \forall x_n A$, where $\{x_1,\cdots,x_n\} = \mathrm{Var}(A)$.

Definition. A formula A is called *logically valid* if its universal closure holds on every structure $\mathcal{M}$ and write $\models A$. A formula A is called to be *logically equivalent* to another formula B if $\models A \leftrightarrow B$.

Definition. A *literal* is an atomic formula or its negation. A *negation normal form*(nnf) of a formula is a formula in which negation symbols are placed as inner as possible. We may also write

$$nnf ::= literals \mid A_0 \mathop{\wedge}_{\vee} A_1 \mid \mathop{\exists}_{\forall} x\, A.$$

Proposition. *For each formula A, there is a logically equivalent nnf.*

Proof. We have four logically valid formulas

$$\begin{aligned}
&\models (A \to B) \leftrightarrow (\neg A \vee B),\\
&\models \neg(A \mathop{\vee}_{\wedge} B) \leftrightarrow (\neg A \mathop{\wedge}_{\vee} \neg B),\\
&\models \neg(\mathop{\exists}_{\forall} x\, A) \leftrightarrow \mathop{\forall}_{\exists} x\, \neg A,\\
&\models \neg\neg A \leftrightarrow A.
\end{aligned}$$

□

1. Sequent calculus

Languages are assumed to be countable.

Definition 1.1. A finite set of formulas in nnf is said to be a *sequent*. Then, a sequence $\{A_1,\cdots,A_n\}$ intends to be the disjunction $A_1 \vee \cdots \vee A_n$. Greek alphabets Γ, Δ will be used to denote sequents, and comma between sequents actually mean their union, i.e. $\Gamma, \Delta = \Gamma \cup \Delta$, and $\Gamma, \{A\} = \Gamma \cup \{A\}$. The empty sequent denotes an absurdity.

Definition 1.2 (Sequent calculus)**.** Our sequent calculus $\mathbb{G}$ is a proof system defined as follows. We have only one logical axiom for $\mathbb{G}$:

- $\Gamma, L, \overline{L}$ for arbitrary sequent Γ and literal L.

We have the following inference rules for $\mathbb{G}$:

- $\dfrac{\Gamma, A_0, A_1}{\Gamma}\ (\vee)$ if $(A_0 \vee A_1) \in \Gamma$.
- $\dfrac{\Gamma, A_0 \quad \Gamma, A_1}{\Gamma}\ (\wedge)$ if $(A_0 \wedge A_1) \in \Gamma$.
- $\dfrac{\Gamma, A(t)}{\Gamma}\ (\exists)$ if $(\exists x A(x)) \in \Gamma$, where $A(t) :\equiv A[x := t] = A[t/x]$.
- $\dfrac{\Gamma, A(a)}{\Gamma}\ (\forall)$ if $(\forall x A(x)) \in \Gamma$, provided that the variable a does not occur in any formulas in Γ. Such a variable a is called *eigenvariable* of the rule $(\forall)$.

We also consider another inference rule, which is not for $\mathbb{G}$:

- $\dfrac{\Gamma, \neg C \quad C, \Gamma}{\Gamma}\ (cut)$

In a proof system, derivable seuqents are defined recursively as follows: all logical axioms are derivable, for each inference rule the lower sequent is derivable if all sequents in the upper sequent is derivable.

Theorem 1.3 (Soundness of $\mathbb{G} + (\text{cut})$)**.** *If* $\mathbb{G} + (\text{cut}) \vdash \Gamma$*, then* $\models \Gamma$.

Proof. We can check from definition. □

Theorem 1.4 (Completeness of $\mathbb{G}$)**.** *If* $\models \Gamma$*, then* $\mathbb{G} \vdash \Gamma$.

Corollary 1.5 (Cut elimination theorem)**.** *If* $\mathbb{G} + (\text{cut}) \vdash \Gamma$*, then* $\mathbb{G} \vdash \Gamma$.

Proof. Clear from the soundness of $\mathbb{G} + (\text{cut})$ and the completeness of $\mathbb{G}$. □

Corollary 1.6 (Weakening)**.** *If* $\mathbb{G} \vdash \Gamma$*, then* $\mathbb{G} \vdash \Gamma, \Delta$.

Proof. In the proof tree, add Δ in every nodes(sequents). Then, every inference rule is preserved (for $(\forall)$-rule, we can obtain same result by changing eigenvariables into another eigenvariables, and it is done because the eigenvariables are finite and the set of variables is countebly infinite). □

Proposition 1.7. $\mathbb{G} \vdash \Gamma, \neg A, A$*. (Note that A is not a literal in general, it is not a logical axiom)*

Proof. It is done by induction on the number of $\vee, \wedge, \exists, \forall$ occurring in A. For $\vee$,

$$\dfrac{\dfrac{\Gamma, \neg A_0, A_0}{\Gamma, \neg A_0, A_0 \vee A_1}\ (\vee) \quad \dfrac{\Gamma, \neg A_1, A_1}{\Gamma, \neg A_1, A_0 \vee A_1}\ (\vee)}{\Gamma, \neg(A_0 \vee A_1), A_0 \vee A_1}\ (\wedge).$$

For $\exists$,

$$\dfrac{\dfrac{\Gamma, \neg A(a), A(a)}{\Gamma, \neg A(a), \exists x A(x)}\ (\exists)}{\Gamma, \neg(\exists x A(x)), \exists x A(x)}\ (\forall),$$

where a is an eigenvariable. (Here, we cannot change the order of $(\forall)$-rule and $(\exists)$-rule because the eigenvariable can occur in inferences) □

3 Day 3: April 24

Completeness of propositional logic

- atoms(propositional variables): $p_0,\ p_1,\ p_2,\ \cdots$.
- literals: $p_0,\ \overline{p_0},\ p_1,\ \overline{p_1},\ \cdots$
- formulas: $A ::= p \mid \overline{p} \mid A \vee A \mid A \wedge A$
- truth assignment: $\nu : \{p_0, p_1, \cdots\} \to \{0, 1\}$

For connectives, truth assignment must satisfy

$$\nu(\overline{p}) = 1 - \nu(p), \quad \nu(A_0 \vee A_1) = \max\{\nu(A_0), \nu(A_1)\}, \quad \nu(A_0 \wedge A_1) = \min\{\nu(A_0), \nu(A_1)\}.$$

We say a formula A is tautoloy if $\nu(A) = 1$ for all truth assignment ν, and satisfiable if $\nu(A) = 1$ for some truth assignment ν.

Definition ($\mathbb{G}_0$; propositional fragment of $\mathbb{G}$)**.** axioms

- $\Gamma, p, \overline{p}$

rules

- $\dfrac{\Gamma, A_0, A_1}{\Gamma}\ (\vee)$ if $(A_0 \vee A_1) \in \Gamma$
- $\dfrac{\Gamma, A_0 \quad \Gamma, A_1}{\Gamma}\ (\wedge)$ if $(A_0 \wedge A_1) \in \Gamma$

Soundness of $\mathbb{G}_0$ means that $\mathbb{G}_0 \vdash \Gamma$ implies that $\bigvee \Gamma$ is a tautology, and completeness means the converse.

Proof of completeness. $T \subset {}^{<\omega}2 = \bigcup_{n=0}^{\infty} 2^n$ is a tree iff $T \neq \emptyset$, $\sigma * \tau \in T$ implies $\sigma \in T$ ($* : 2^n \times 2^{m-n} \to 2^m$ is the concatentation $(a_0, \cdots, a_{n-1}) * (a_n, \cdots, a_{m-1}) = (a_0, \cdots, a_{m-1})$). Each element means a node, and the length of node means the depth.

Define the following recursively on sequences(=nodes) $\sigma \in {}^{<\omega}2$ and a tree T(= $\emptyset$initially):

- $\mathrm{Seq}(\sigma) = \mathrm{Seq}_0(\sigma) \cup \mathrm{Seq}_1(\sigma)$ = sequents at σ.
- $\mathrm{Ord}(\sigma)$ = total order on $\mathrm{Seq}_0(\sigma)$
- for the empty sequence $\emptyset$(=root node),

$$\mathrm{Seq}_0(\emptyset) := NL(\Gamma) = \text{non-literals in } \Gamma, \quad \mathrm{Seq}_1(\emptyset) := L(\Gamma) = \text{literals in } \Gamma.$$

- if $\mathrm{Seq}(\sigma)$ is an axiom, that is, there is an atom p such that $\{p, \overline{p}\} \subset \mathrm{Seq}(\sigma)$, then σ is a leaf of T.
- if $\mathrm{Seq}_0(\sigma) = \emptyset$, then σ is a leaf of T.
- Suppose B is the leftmost member of $\mathrm{Seq}_0(\sigma)$; we have two cases.
  The first case is $B \equiv A_0 \vee A_1$. We put $\sigma * (0)$ into T and write

$$\mathrm{Seq}_0(\sigma) = A_0 \vee A_1, \Gamma_0, \quad \mathrm{Seq}_1(\sigma) = \Gamma_1.$$

  Then,

$$\mathrm{Seq}_0(\sigma * (0)) := \Gamma_0, NL(A_0, A_1), \quad \mathrm{Seq}_1(\sigma * (0)) := \Gamma_1, A_0 \vee A_1, L(A_0, A_1).$$

  For the second case $B \equiv A_0 \wedge A_1$, we put $\sigma * (0)$ and $\sigma * (1)$ into T and write

$$\mathrm{Seq}_0(\sigma) = A_0 \wedge A_1, \Gamma_0, \quad \mathrm{Seq}_1(\sigma) = \Gamma_1.$$

  Then,

$$\mathrm{Seq}_0(\sigma * (0)) := \Gamma_0, NL(A_0), \quad \mathrm{Seq}_1(\sigma * (0)) := \Gamma_1, A_0 \wedge A_1, L(A_0),$$
$$\mathrm{Seq}_0(\sigma * (1)) := \Gamma_0, NL(A_1), \quad \mathrm{Seq}_1(\sigma * (1)) := \Gamma_1, A_0 \wedge A_1, L(A_1).$$

The decomposition $\mathrm{Seq}(\sigma) = \mathrm{Seq}_0(\sigma) \cup \mathrm{Seq}_1(\sigma)$ is introduced in order to avoid

$$\dfrac{\dfrac{\dfrac{\vdots}{A_0, A_1, A_0, A_1, A_0 \vee A_1, \Gamma}}{A_0, A_1, A_0 \vee A_1, \Gamma}}{A_0 \vee A_1, \Gamma} \quad .$$

The set $\mathrm{Seq}_0(\sigma)$ is the set of *unanalyzed sequents*, which contains non-literals only. We will write the decomposition as $\mathrm{Seq}(\sigma) = \mathrm{Seq}_0(\sigma); \mathrm{Seq}_1(\sigma)$. The tree T is finite because if we define $lc(A)$ as the number of occurences of $\vee, \wedge$ in A and $lc(\sigma) = \sum_{A \in \mathrm{Seq}_0(\sigma)} lc(A)$, then we can check $lc(\sigma) > lc(\sigma * (i))$ for $i \in \{0, 1\}$.

Now we suppose $\mathbb{G}_0 \nvdash \Gamma$ so that there is a leaf $\sigma \in T$ such that $\mathrm{Seq}(\sigma)$ is not an axiom. For every atom p, we have $\{p, \overline{p}\} \not\subset \mathrm{Seq}_1(\sigma)$. Define any truth assignment ν such that

$$\nu(l) = 0 \text{ for literals } l \in \mathrm{Seq}_1(\sigma).$$

Define for the leaf σ a set

$$S := \bigcup_{\exists \rho, \tau * \rho = \sigma} \mathrm{Seq}(\tau).$$

In other words, $A \in S$ iff A occurs in the path from σ to the root. Let $B \in S$. We claim $\nu(B) = 0$. Use the induction on $lc(B)$. If B is a literal, then $\nu(B) = 0$ by definition of ν. If $B \equiv A_0 \vee A_1$, then we can show $\{A_0, A_1\} \subset S$, so $\nu(B) = 0$ by the induction hypothesis. If $B \equiv A_0 \wedge A_1$, then we can show $\{A_0, A_1\} \cap S \neq \emptyset$, so $\nu(B) = 0$ by the induction hypothesis. From $\Gamma \subset S$, we have $\nu(A) = 0$ for all $A \in \Gamma$, so $\nu(\bigvee \Gamma) = 0$, i.e. $\bigvee \Gamma$ is not a tautology. □

4 Day 4: May 1

Completeness of first order logic

Assuming $\mathbb{G} \nvdash \Gamma$, we have to construct a structure $\mathcal{M}$ such that $\mathcal{M} \not\models \bigvee \Gamma$ (i.e.$\mathcal{M} \not\models \forall \bigvee \Gamma$, the universal closure). For this, we have to make a set and construct interpretations of each symbol of the given language, the set of non-logical symbols.

(1) For universal formula,

$$\frac{\cdots, NL(A(a)); \cdots, \forall x\, A(x), L(A(a))}{\forall x\, A(x), \cdots;}.$$

(2) Suppose an existential formula $\exists x\, A(x)$ occurs in a path P. Note that $\mathcal{M} \not\models \exists x\, A(x)$ implies $\mathcal{M} \not\models A(t)$ for any term t. For each term t, $A(t)$ should occur in the path P. Define $\mathrm{Tm}(\sigma; \exists x\, B(x))$ such that $t \in \mathrm{Tm}(\sigma; \exists x\, B(x))$ if and only if an inference

$$\frac{\cdots, B(t); \cdots}{\exists x\, B(x), \cdots; \cdots}$$

occurs in the path from the root $\emptyset$ to the node σ.

Now we are going to construct a tree T recursively from the root as follows:

Case 1: $\mathrm{Seq}_1(\sigma) \supset \{L, \overline{L}\}$ for some literal L, then we stop to prolong the tree. In what follows, assume no literals satisfy $\mathrm{Seq}_1(\sigma) \supset \{L, \overline{L}\}$.

Case 2: $\mathrm{Seq}_0(\sigma) = \emptyset$, then we repeat as

$$\frac{\emptyset; \mathrm{Seq}_1(\sigma)}{\emptyset; \mathrm{Seq}_1(\sigma).}$$

Now let A be the leftmost formula in $\mathrm{Seq}_0(\sigma)$.

Case 3: $A \equiv A_0 \vee A_1$. As in the last lecture.

Case 4: $A \equiv A_0 \wedge A_1$. As in the last lecture.

Case 5: $A \equiv \forall x\, B(x)$. Then, we extend the tree as follows:

$$\frac{\Gamma_0, NL(B(a)); \Gamma_1, \forall x\, B(x), L(B(a))}{\forall x\, B(x), \Gamma_0; \Gamma_1}.$$

Case 6: $A \equiv \exists x\, B(x)$. Let $t \equiv t_n$ be the first one in the enumeration $\mathrm{Tm} = \{t_0, t_1, \cdots\}$ such that $t_n \notin \mathrm{Tm}(\sigma; \exists x\, B(x))$. Then, we can extend the tree as

$$\frac{\Gamma_0, NL(B(t)), \exists x\, B(x); \Gamma_1, L(B(t))}{\exists x\, B(x), \Gamma_0; \Gamma_1}.$$

Note that we have put $\exists x\, B(x)$ into Seq_0, not Seq_1.

Suppose $\mathbb{G} \nvdash \Gamma$. If T is finite, then every leaf is an axiom so that the tree is indeed a derivation of Γ, T is infinite. By König's infinity lemma, there exists an infinite path P through the constructed binary tree T.

Proof of König's lemma. The lemma holds for general connected locally finite infinite graphs, but we assume the graph is tree. Choose σ_n recursively as follows: suppose σ_n satisfies that $\{\tau : \sigma * \tau \in T\}$ is infinite. By the local finiteness, there is i such that $\{\tau : \sigma * (i) * \tau \in T\}$ is infinite. Let $\sigma_{n+1} := \sigma_n * (i)$. Then, σ_n defines an infinite path in T. □

Now we construct the *Herbrand structure* $\mathcal{M} = \langle M; f^{\mathcal{M}}, \cdots, R^{\mathcal{M}}, \cdots \rangle$ as:

- $M := \mathrm{Tm}(\mathcal{L})$,
- $f^{\mathcal{M}}(t_1, \cdots, t_n) := f(t_1, \cdots, t_n)$,
- $R^{\mathcal{M}}(t_1, \cdots, t_n)$ is true if and only if

$$R(t_1, \cdots, t_n) \notin \mathrm{Seq}(P) := \bigcup_{\sigma \in P} \mathrm{Seq}(\sigma)$$

Then, $\mathcal{M} \models \overline{L}$ if and only if $L \in \mathrm{Seq}(P)$ for literals L.

Claim. *If $A \in \mathrm{Seq}(P)$, then $\mathcal{M} \not\models A$.*

Proof. Define the literal complexity $lc(A)$ by the number of occurrences of logical symbols in A, and use induction on $lc(A)$.

For the Case 5: $A \equiv \forall x\, B(x)$. We have $B(a) \in \mathrm{Seq}(P)$ so that $\mathcal{M} \not\models B(a)$ by the induction hypothesis.

For the Case 6: $A \equiv \exists x\, B(x)$. We have $\exists x\, B(x) \in \mathrm{Seq}(P)$, and it implies $\{B(t) : t \in \mathrm{Tm}\} \subset \mathrm{Seq}(P)$. By the induction hypothesis, $\mathcal{M} \not\models B(t)$ for all $t \in \mathrm{Tm}$, hence $\mathcal{M} \not\models \exists x B(x)$. □