Proof Theory

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

April 17, 2023

Contents

1 Day 1: April 10

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

Completeness theorem

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

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 $\mathrm{Var} \cap \mathcal{L} = \varnothing$. 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 $\circ \in \{\vee,\wedge,\rightarrow\}$, 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 $\rightarrow$),

(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

$$nnf ::= literals \mid A_0 \overset{\wedge}{\underset{\vee}{}} A_1 \mid \overset{\exists}{\underset{\forall}{}} x A.$$

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

Proof. We have four logically valid formulas

$$\begin{aligned}
&\models (A\rightarrow B) \leftrightarrow (\neg A \vee B),\\
&\models \neg(A \overset{\vee}{\underset{\wedge}{}} B) \leftrightarrow (\neg A \overset{\wedge}{\underset{\vee}{}} \neg B),\\
&\models \neg(\overset{\exists}{\underset{\forall}{}} x A) \leftrightarrow \overset{\forall}{\underset{\exists}{}} x\, \neg A,\\
&\models \neg\neg A \leftrightarrow A.
\end{aligned}$$

□

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 $\vee$,

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

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) ☐