

# Proof Theory

Ikhan Choi

Lectured by Toshiyasu Arai  
University of Tokyo, Spring 2023

June 19, 2023

## Contents

1	Day 1: April 10	2
2	Day 2: April 17	3
3	Day 3: April 24	5
4	Day 4: May 1	7
5	Day 5: May 8	9
6	Day 6: May 15	11
7	Day 7: June 5	13
8	Day 8: June 12	15
9	Day 9: June 19	17

# 1 Day 1: April 10

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

Completeness theorem

$$\text{logically valid} \iff \text{provable}$$

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 structures 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 sometimes 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  $F(p) = p^{\mathcal{M}} \subset M^n$ ,  $F(f) = f^{\mathcal{M}} : M^n \rightarrow M$ .

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

- (a)  $\text{Var} \subset \text{Tm}_{\mathcal{L}}$ ,
- (b) If  $t_1, \dots, t_n \in \text{Tm}_{\mathcal{L}}$  and  $f \in \mathcal{F}_n$ , then  $f(t_1, \dots, t_n) \in \text{Tm}_{\mathcal{L}}$ .

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  $t \equiv f(t_1, \dots, t_n)$  (completely equal as sequences of symbols), then  $t^{\mathcal{M}}$  is recursively defined by  $t^{\mathcal{M}} := f^{\mathcal{M}}(t_1^{\mathcal{M}}, \dots, t_n^{\mathcal{M}}) \in M$ .

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

- (a) if  $t_1, \dots, t_n \in \text{Tm}_{\mathcal{L}}$  and  $p \in \mathcal{P}_n$ , then  $p(t_1, \dots, t_n) \in \text{Fml}_{\mathcal{L}}$ ,
- (b) if  $A, B \in \text{Fml}_{\mathcal{L}}$ , then  $\neg A, A \vee B, A \wedge B, A \rightarrow B \in \text{Fml}_{\mathcal{L}}$ ,
- (c) if  $A \in \text{Fml}_{\mathcal{L}}$  and  $x \in \text{Var}$ , then  $\exists x A, \forall x A \in \text{Fml}_{\mathcal{L}}$ .

The symbols  $\neg, \vee, \wedge, \rightarrow$  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  $\text{Var}(t) \subset \text{Var}$  is defined as

- (a) if  $x \in \text{Var}$ , then  $\text{Var}(x) = \{x\}$ ,
- (b)  $\text{Var}(f(t_1, \dots, t_n)) = \bigcup_{i=1}^n \text{Var}(t_i)$ .

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

- (a)  $\text{Var}(p(t_1, \dots, t_n)) = \bigcup_{i=1}^n \text{Var}(t_i)$ .
- (b) if  $\circ \in \{\vee, \wedge, \rightarrow\}$ , then  $\text{Var}(A \circ B) = \text{Var}(A) \cup \text{Var}(B)$ ,
- (c) if  $\circ \in \{\exists, \forall\}$  and  $x \in \text{Var}$ , then  $\text{Var}(\circ x A) = \text{Var}(A) \setminus \{x\}$ .

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

**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)  $\mathcal{M} \models p(t_1, \dots, t_n)$  iff  $(t_1^{\mathcal{M}}, \dots, t_n^{\mathcal{M}}) \in p^{\mathcal{M}}$ ,
- (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  $c_\alpha$  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  $\{x_1, \dots, x_n\} = \text{Var}(A)$ .

**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

$$\text{nnf} ::= \text{literal} \mid A_0 \bigwedge_{\bigvee} A_1 \mid \bigvee_{\bigwedge} x A.$$

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

*Proof.* We have four logically valid formulas

$$\models (A \rightarrow B) \leftrightarrow (\neg A \vee B),$$

$$\models \neg(A \bigvee_{\bigwedge} B) \leftrightarrow (\neg A \bigwedge_{\bigvee} \neg B),$$

$$\models \neg(\bigvee_{\bigwedge} x A) \leftrightarrow \bigvee_{\bigwedge} x \neg A,$$

$$\models \neg \neg A \leftrightarrow A.$$

□

### 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  $\{A_1, \dots, A_n\}$  intends to be the disjunction  $A_1 \vee \dots \vee A_n$ . Greek alphabets  $\Gamma, \Delta$  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  $\mathbb{G}$ :

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

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

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

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

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

In a proof system, derivable sequents 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  $\mathbb{G} + (cut)$ ). *If  $\mathbb{G} + (cut) \vdash \Gamma$ , 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  $\mathbb{G} + (cut) \vdash \Gamma$ , then  $\mathbb{G} \vdash \Gamma$ .*

*Proof.* Clear from the soundness of  $\mathbb{G} + (cut)$  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  $\Delta$  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 countably 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  $\vee$ ,

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

For  $\exists$ ,

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

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):  $p_0, p_1, p_2, \dots$ .
- literals:  $p_0, \overline{p_0}, p_1, \overline{p_1}, \dots$
- formulas:  $A ::= p \mid \overline{p} \mid A \vee A \mid A \wedge A$
- truth assignment:  $\nu : \{p_0, p_1, \dots\} \rightarrow \{0, 1\}$

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 tautology if  $\nu(A) = 1$  for all truth assignment  $\nu$ , and satisfiable if  $\nu(A) = 1$  for some truth assignment  $\nu$ .

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

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

rules

- $\frac{\Gamma, A_0, A_1}{\Gamma} (\vee)$  if  $(A_0 \vee A_1) \in \Gamma$
- $\frac{\Gamma, A_0 \quad \Gamma, A_1}{\Gamma} (\wedge)$  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  $\sigma \in T$  ( $* : 2^n \times 2^{m-n} \rightarrow 2^m$  is the concatenation  $(a_0, \dots, a_{n-1}) * (a_n, \dots, a_{m-1}) = (a_0, \dots, a_{m-1})$ ). 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):

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

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

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

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

Then,

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

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

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

Then,

$$\begin{aligned} \text{Seq}_0(\sigma * (0)) &:= \Gamma_0, NL(A_0), & \text{Seq}_1(\sigma * (0)) &:= \Gamma_1, A_0 \wedge A_1, L(A_0), \\ \text{Seq}_0(\sigma * (1)) &:= \Gamma_0, NL(A_1), & \text{Seq}_1(\sigma * (1)) &:= \Gamma_1, A_0 \wedge A_1, L(A_1). \end{aligned}$$

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

$$\frac{\frac{\frac{\vdots}{A_0, A_1, A_0, A_1, A_0 \vee A_1, \Gamma}}{A_0, A_1, A_0 \vee A_1, \Gamma}}{A_0 \vee A_1, \Gamma}.$$

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

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

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

Define for the leaf  $\sigma$  a set

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

In other words,  $A \in S$  iff  $A$  occurs in the path from  $\sigma$  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  $\nu$ . 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.  $\square$

## 4 Day 4: May 1

### Completeness of first order logic

Assuming  $\mathbb{G} \not\models \Gamma$ , 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  $\text{Tm}(\sigma; \exists x B(x))$  such that  $t \in \text{Tm}(\sigma; \exists x B(x))$  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  $\sigma$ .

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

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

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

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

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

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  $\text{Tm} = \{t_0, t_1, \dots\}$  such that  $t_n \notin \text{Tm}(\sigma; \exists x B(x))$ . 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  $\text{Seq}_0$ , not  $\text{Seq}_1$ .

Suppose  $\mathbb{G} \not\models \Gamma$ . If  $T$  is finite, then every leaf is an axiom so that the tree is indeed a derivation of  $\Gamma$ ,  $T$  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  $\sigma_n$  recursively as follows: suppose  $\sigma_n$  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,  $\sigma_n$  defines an infinite path in  $T$ .  $\square$

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

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

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

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

**Claim.** If  $A \in \text{Seq}(P)$ , then  $\mathcal{M} \models A$ .

*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  $B(a) \in \text{Seq}(P)$  so that  $\mathcal{M} \models B(a)$  by the induction hypothesis.

For the Case 6:  $A \equiv \exists x B(x)$ . We have  $\exists x B(x) \in \text{Seq}(P)$ , and it implies  $\{B(t) : t \in \text{Tm}\} \subset \text{Seq}(P)$ . By the induction hypothesis,  $\mathcal{M} \models B(t)$  for all  $t \in \text{Tm}$ , hence  $\mathcal{M} \models \exists x B(x)$ .  $\square$



## 5 Day 5: May 8

We have shown completeness theorems for logic (in a proof system): propositional logic and first order logic. From now we discuss the completeness theorem for theories.

**Definition.** Let  $\mathcal{L}$  be a language,  $\mathcal{M}$  a  $\mathcal{L}$ -structure,  $A$  a  $\mathcal{L}$ -formula,  $\Gamma$  a  $\mathcal{L}$ -sequent. A *theory* (or axiomatic system)  $T$  over  $\mathcal{L}$  is a set of closed  $\mathcal{L}$ -formulas (=  $\mathcal{L}$ -sentences). We write  $\mathcal{M} \models T$  and say  $\mathcal{M}$  is a model of  $T$  if  $\mathcal{M} \models A$  for all  $A \in T$ . We write  $T \models A$  and say  $A$  is a logical consequence of  $T$  if for every  $\mathcal{L}$ -structure  $\mathcal{M}$  such that  $\mathcal{M} \models T$  we have  $\mathcal{M} \models A$ . We write  $T \vdash \Gamma$  for a sequent  $\Gamma$  and say  $\Gamma$  is provable from  $T$  if there exists a derivation of  $\Gamma$  in the proof system  $\mathbb{G}$  together with an additional inference rule

$$\frac{\neg A, \Delta}{\Delta} \text{ (T)}$$

for  $A \in T$ . Note that  $\neg A \vee B \equiv A \rightarrow B$ .

*Remark.*  $T \vdash \Gamma$  iff there is a finite subset  $\{A_1, \dots, A_n\} \subset_{\text{fin}} T$  such that  $\mathbb{G} \vdash \{\neg A_1, \dots, \neg A_n\}, \Gamma$ . Therefore, assuming the following theorem (will be proved in the next lecture), we can prove the completeness theorem ( $T \models A$  implies  $T \vdash A$ ) by a little modification of the completeness of  $\mathbb{G}$ :

**Theorem (Compactness).**  $T \models A$  if and only if  $T_0 \models A$  for some  $T_0 \subset_{\text{fin}} T$ .

Modification of the completeness proof we did in the last week for a theory  $T$ . Suppose  $\mathcal{L}$  is countable and  $T \not\models \Gamma$ . We want to find a model  $\mathcal{M}$  of  $T$  such that  $\mathcal{M} \not\models \bigvee \Gamma$ . Modify the proof search procedure in  $\mathbb{G}$  as follows: for a node  $\sigma$  with length  $n$ , if  $n$  is even then analyze the leftmost formula to the semicolon as we did in the last week, if  $n = 2m + 1$  is odd then after enumeration  $T = \{A_0, A_1, \dots\}$  we construct

$$\frac{\Gamma_0, NL(\neg A_m); L(\neg A_m), \Gamma_1}{\Gamma_0; \Gamma_1} \text{ (T)}.$$

The proof tree constructed as above must be infinite since  $T \not\models \Gamma$ . Pick an infinite path  $P$  from the root in that tree using the König argument. If  $\text{Seq}(P) := \bigcup_{\sigma \in P} (\text{Seq}_0(\sigma) \cup \text{Seq}_1(\sigma))$ , then  $\{\bar{L}, L\} \not\subset P$ ,  $\exists x B(x) \in \text{Seq}(P)$  implies  $\{B(t_n)\}_n \subset \text{Seq}(P)$ , and  $\{\neg A\}_{A \in T} \subset \text{Seq}(P)$ . Let  $\mathcal{M}$  be the structure obtained from the path  $P$  such that  $A \in \text{Seq}(P)$  implies  $\mathcal{M} \models A$ . Then,  $\mathcal{M} \models T$  and  $\mathcal{M} \not\models A$ .

### Preparation 1 for the compactness theorem

**Definition** (Equality axiom).  $\text{Eq}$  denotes the set of closed formulas

$$\begin{aligned} & \forall x(x = x), \quad \forall x, y(x = y \rightarrow y = x), \quad \forall x, y, z(x = y \rightarrow y = z \rightarrow x = z), \\ & \forall x_1, \dots, x_n, y_1, \dots, y_n((x_1 = y_1 \wedge \dots \wedge x_n = y_n) \rightarrow f(x_1, \dots, x_n) = f(y_1, \dots, y_n)), \\ & \forall x_1, \dots, x_n, y_1, \dots, y_n((x_1 = y_1 \wedge \dots \wedge x_n = y_n) \rightarrow R(x_1, \dots, x_n) = R(y_1, \dots, y_n)). \end{aligned}$$

**Definition** (Usual definition of models). Suppose  $= \in \mathcal{P} \subset \mathcal{L}$ . A structure is  $\mathcal{M} = \langle M \mid f^{\mathcal{M}}, \dots, R^{\mathcal{M}}, \dots, =^{\mathcal{M}} \rangle$  such that  $f^{\mathcal{M}}$  and  $R^{\mathcal{M}}$  are interpretations we did, and  $=^{\mathcal{M}}$  satisfies the following:  $\mathcal{M} \models c_\alpha = c_\beta$  iff  $\alpha =^{\mathcal{M}} \beta$  iff  $\alpha = \beta$  for  $\alpha, \beta \in M$ .

If a structure  $\mathcal{M}$  in the sense we have done so far satisfies  $\mathcal{M} \models \text{Eq}$ , then the above “real equality” can be realized by the “quotient” of  $\mathcal{M}$ .

### Preparation 2 for the compactness theorem

**Definition.** Let  $I \neq \emptyset$ . A filter  $D$  over  $I$  is a set  $D \subset \mathcal{P}(I)$  such that

- (i)  $\emptyset \notin D, I \in D,$

- (ii)  $x \in D$  and  $x \subset y \subset I$  imply  $y \in D$ ,
- (iii)  $x, y \in D$  implies  $x \cap y \in D$ .

An ultrafilter is a filter  $D$  such that for every  $x \in I$  we have either  $x \in D$  or  $x^c \in D$ .

**Definition.** We say a set  $S \subset \mathcal{P}(I)$  satisfies the finite intersection property if for any  $S_0 \subset_{\text{fin}} S$  we have  $\bigcap S_0 \neq \emptyset$ . If  $S \subset \mathcal{P}(I)$  satisfies the finite intersection property, then the filter  $D$  generated by  $S$  is explicitly given by

$$D = \{y \in I : \exists S_0 \subset_{\text{fin}} S \text{ s.t. } \bigcap S_0 \subset y\}.$$

**Lemma.** A filter is a ultrafilter if and only if it is maximal.

## 6 Day 6: May 15

**Theorem.** Let  $D \subset \mathcal{P}(I)$  be a filter. The following statements are equivalent:

- (a)  $D$  is an ultrafilter.
- (b) For  $X \in D$ , if  $X \subset Y \cup Z$ , then  $\{Y, Z\} \cap D \neq \emptyset$ .
- (c)  $D$  is maximal among filters.

*Proof.* (a) $\Rightarrow$ (b) If  $Y \notin D$  and  $Z \notin D$ , then since  $D$  is an ultrafilter so that  $Y^c, Z^c \in D$ , so  $(Y \cup Z)^c = Y^c \cap Z^c \in D$ . However,  $X \cap (Y \cup Z)^c = \emptyset$ , contradiction.

(b) $\Rightarrow$ (a) Suppose  $D$  is not an ultrafilter, then there is  $X$  such that  $X \notin D$  and  $X^c \notin D$ . Then,  $I \subset X \cup X^c$  but  $\{X, X^c\} \cap D = \emptyset$ .

(a) $\Rightarrow$ (c) Suppose  $E$  is a filter such that  $D \subset E$ . If  $X \in E$  and assume  $X^c \in D$ , then  $X^c \in D \subset E$  implies  $\{X, X^c\} \subset E$ , which contradicts to the assumption that  $E$  is a filter, hence  $X \in D$ .

(c) $\Rightarrow$ (a) Suppose  $X \subset I$  and  $X \notin D$ . We want to show  $X^c \in D$ . For  $Y \in D$ , we have  $Y \cap X^c \neq \emptyset$ . It means  $D \cup \{X^c\}$  satisfies the finite intersection property. Therefore, there is a filter containing  $D \cup \{X^c\}$ . Because  $D$  is maximal,  $X^c \in D$ .  $\square$

For  $\emptyset \neq X \subset I$ ,  $\langle X \rangle := \{Y \subset I : X \subset Y\}$  is called the principal filter generated by  $X$ , and a filter  $D$  is called principal if there is  $X \subset I$  such that  $D = \langle X \rangle$ . For infinite  $I$ , the Fréchet filter or the cofinite filter is the filter  $F := \{X \subset I : |X^c| < \aleph_0\}$ .

**Proposition.** Let  $I$  be an infinite set.

- (a) A principal filter  $\langle X \rangle$  is a ultrafilter if and only if  $|X| = 1$ .
- (b) An ultrafilter  $D$  is not principal if and only if  $F \subset D$ .

### Ultraproducts

Let  $\mathcal{L}$  be a language and  $I \neq \emptyset$ . For each  $i \in I$ , consider a  $\mathcal{L}$ -structure  $\mathcal{M}_i$  (not necessary to contain equality) which share symbols. Their product is a structure with the product universe and the same symbol set.

For a filter  $D \subset \mathcal{P}(I)$ , the reduced product  $\prod_D \mathcal{M}_i$  of  $\mathcal{M}_i$  by  $D$  is defined by

$$|\prod_D \mathcal{M}_i| = \{f_D : f \in \prod_{i \in I} |\mathcal{M}_i|\}.$$

For  $f, g \in \prod_{i \in I} |\mathcal{M}_i|$ , we can define an equivalence relation  $=_D$  such that  $f =_D g$  means that  $f(i) = g(i)$  a.e., i.e.  $\{i \in I : f(i) = g(i)\} \in D$ . The transitivity follows from the defining properties of the filter  $D$ .

For a relation symbol  $R$ , we define  $\prod_i \mathcal{M}_i \models R(f_1, \dots, f_n)$  for  $\forall i \mathcal{M}_i \models R(f_1(i), \dots, f_n(i))$  and  $\prod_D \mathcal{M}_i \models R(f_1, \dots, f_n)$  for  $\mathcal{M}_i \models R(f_1(i), \dots, f_n(i))$  a.e.

For a function symbol  $F$ , we define  $\prod_D \mathcal{M}_i \models F(f_1, \dots, f_n) =_D g$  for  $\mathcal{M}_i \models F(f_1(i), \dots, f_n(i)) = g(i)$  a.e.

If the filter  $D$  is an ultrafilter, then the reduced product is called an ultraproduct.

**Theorem** (Łoś, Fundamental theorem of ultraproduct). Let  $\mathcal{M}_i$  be an  $\mathcal{L}$ -structure,  $D$  an ultrafilter over  $I$ ,  $\varphi$  an  $\mathcal{L}$ -formula,  $f_1, \dots, f_n \in \prod_i |\mathcal{M}_i|$ . Then,  $\prod_D \mathcal{M}_i \models \varphi((f_1)_D, \dots, (f_n)_D)$  if and only if  $\mathcal{M}_i \models \varphi(f_1(i), \dots, f_n(i))$  a.e.

*Proof.* By induction on  $l.c.(\varphi)$ , the number of logical symbols  $\wedge, \neg, \exists$ . The conjunction follows from that  $D$  is a filter, the negation follows from that  $D$  is an ultrafilter, and the existential quantifier follows from:

Suppose  $\prod_D \mathcal{M}_i \models \exists x_0 \psi(x_0, (f_1)_D, \dots)$ . Pick  $f_0 \in \prod_i |\mathcal{M}_i|$  such that  $\prod_D \mathcal{M}_i \models \psi((f_0)_D, (f_1)_D, \dots)$ . By the induction hypothesis,

$$\{i \in I : \mathcal{M}_i \models \psi((f_0)_D, (f_1)_D, \dots)\} \in D.$$

Since

$$\{i \in I : \mathcal{M}_i \models \psi((f_0)_D, (f_1)_D, \dots)\} \subset \{i \in I : \mathcal{M}_i \models \exists x_0 \psi(x_0, (f_1)_D, \dots)\} =: J,$$

$J \in D$ . Pick  $f_0 \in \prod_i |\mathcal{M}_i|$  such that  $\mathcal{M}_i \models \psi(f_0(i), f_1(i), \dots)$  for all  $i \in J$ . Then,  $\mathcal{M}_i \models \psi(f_0(i), f_1(i), \dots)$  a.e. implies  $\prod_D \mathcal{M}_i \models \psi((f_0)_D, (f_1)_D, \dots)$ , hence  $\prod_D \mathcal{M}_i \models \exists x_0 \psi(x_0, (f_1)_D, \dots)$ .  $\square$

**Corollary.** For a closed formula  $\varphi$ ,  $\prod_D \mathcal{M}_i \models \varphi$  if and only if  $\{i \in I : \mathcal{M}_i \models \varphi\} \in D$ . In particular, if  $\mathcal{M}_i \models T$  for every  $i \in I$ , then  $\prod_D \mathcal{M}_i \models T$ .

**Theorem** (Compactness theorem). Let  $\mathcal{L}$  be a language and  $T$  an  $\mathcal{L}$ -theory. If  $T$  is finitely satisfiable, then  $T$  is satisfiable.

*Proof.* Suppose  $T$  is finitely satisfiable and let  $I = \{T_0 \subset_{\text{fin}} T\}$ . Then, for each  $T_0 \subset_{\text{fin}} T$  there is  $i \in I$  such that  $\mathcal{M}_i \models T_0$  for some  $\mathcal{M}_i$ . Define

$$S := \{\{i \in I : \mathcal{M}_i \models T_0\} : T_0 \subset_{\text{fin}} T\} \subset \mathcal{P}(I).$$

The set  $S$  satisfies the finite intersection property. Using Zorn's lemma to take an ultrafilter  $D$  containing  $S$ . Then,  $\prod_D \mathcal{M}_i \models T$  since for  $\varphi \in T$  we have  $\{i \in I : \mathcal{M}_i \models \varphi\} \in D$  by the Łoś fundamental theorem.  $\square$

## 7 Day 7: June 5

### Some applications of compactness theorem

Let  $\mathcal{L} \subset \mathcal{L}'$ . Let  $\mathcal{M}$  and  $\mathcal{M}'$  be  $\mathcal{L}$  and  $\mathcal{L}'$ -structures. We call  $\mathcal{M}'$  an *expansion* of  $\mathcal{M}$  and  $\mathcal{M}$  a *reduct* of  $\mathcal{M}'$  if  $\mathcal{M}' = \langle M; f^{\mathcal{M}}, \dots, R^{\mathcal{M}}, \dots, g^{\mathcal{M}'}, \dots, P^{\mathcal{M}'}, \dots \rangle$  for  $\mathcal{M} = \langle M; f^{\mathcal{M}}, \dots, R^{\mathcal{M}}, \dots \rangle$  and  $g, P \in \mathcal{L}' \setminus \mathcal{L}$ . Then, for  $\varphi \in \mathcal{L}(\mathcal{M}) = \mathcal{L} \cup \{c_\alpha : \alpha \in M\}$  we have  $\mathcal{M} \models \varphi$  if and only if  $\mathcal{M}' \models \varphi$ .

Let  $\mathcal{M}$  and  $\mathcal{N}$  be  $\mathcal{L}$ -structures. We say  $\mathcal{M}$  is a *submodel* of  $\mathcal{N}$  or  $\mathcal{N}$  is an *extension* of  $\mathcal{M}$  and write  $\mathcal{M} \subset \mathcal{N}$ , if (1)  $M \subset N$ , (2)  $R^{\mathcal{M}} = \mathcal{N} \cap M_k$  for  $k$ -ary relations  $R \in \mathcal{L}$ , and (3)  $f^{\mathcal{M}} = f^{\mathcal{N}}|_{M^k}$  for  $k$ -ary functions  $f \in \mathcal{L}$ . Don't be confused about expansions and extensions.

**Definition.** An *existential* and *universal* formula is a formula without universal and existential quantifiers, respectively.

**Proposition.** Let  $\mathcal{M} \subset \mathcal{N}$ . If  $\varphi \in \mathcal{L}(\mathcal{M})$  is existential, then  $\mathcal{M} \models \varphi$  implies  $\mathcal{N} \models \varphi$ . If  $\varphi \in \mathcal{L}(\mathcal{M})$  is universal, then  $\mathcal{N} \models \varphi$  implies  $\mathcal{M} \models \varphi$ .

**Definition.** Let  $\mathcal{M}$  and  $\mathcal{N}$  be  $\mathcal{L}$ -structures. We say  $\mathcal{M}$  is a *elementary submodel* of  $\mathcal{N}$  or  $\mathcal{N}$  is an *elementary extension* of  $\mathcal{M}$  and write  $\mathcal{M} \prec \mathcal{N}$ , if  $\mathcal{M} \subset \mathcal{N}$  and for every  $\varphi \in \mathcal{L}(\mathcal{M})$  we have  $\mathcal{M} \models \varphi$  if and only if  $\mathcal{N} \models \varphi$ .

**Example.** Let  $\mathbb{R} = \langle \mathbb{R} : 0, 1, +, \cdot, <, f, \dots, R, \dots \rangle$ . There exists an elementary extension  ${}^*\mathbb{R}$  of  $\mathbb{R}$  such that  ${}^*\mathbb{R}$  is non-Archimedean. Recall that a field is non-Archimedean if for every  $x$  there is a natural number  $n$  such that  $x \leq n \cdot 1$ , which is equivalent to the existence of  $c$  with  $0 < c < n^{-1}$ .

*Proof.* Let  $\mathcal{L}' = \mathcal{L} \cup \{c\}$ . Let  $T := \{\varphi \in \mathcal{L}(\mathbb{R}) : \mathbb{R} \models \varphi\} \cup \{0 < c < n^{-1} : n = 1, 2, \dots\}$  be an  $\mathcal{L}'$ -theory. If there is a model  $\mathcal{M}$  of  $T$ , and if we define  ${}^*\mathbb{R}$  to be the reduct of  $\mathcal{M}$  to  $\mathcal{L}$ , then we are done.

For  $T_0 \subset_{\text{fin}} T$ , since  $T_0$  contains only finite number of formulas of the form  $0 < c < n^{-1}$ , which is clearly satisfiable by the standard  $\mathbb{R}$  with interpretation  $c^{\mathbb{R}} = k^{-1}$  for sufficiently large  $k$ . By the compactness theorem, the whole  $T$  is satisfiable.  $\square$

**Example.** If an  $\mathcal{L}$ -theory  $T$  has an arbitrary large finite model, i.e.  $\forall n \exists \mathcal{M} \models T$  such that  $n \leq \|\mathcal{M}\| (= |M|) < \infty$ , then  $T$  has an infinite model.

*Proof 1.* Define an  $\mathcal{L}$ -theory

$$T_1 := T \cup \{\exists x_1 \cdots \exists x_n \bigwedge_{1 \leq i < j \leq n} (x_i \neq x_j) : n = 1, 2, \dots\},$$

and take  $T_0 \subset_{\text{fin}} T_1$ . Then,  $T_0$  is satisfiable by the assumption, so  $T_1$  also has a model, which must be infinite.  $\square$

*Proof 2.* Let  $\mathcal{L}_2 := \mathcal{L} \cup \{c_0, c_1, \dots\}$ . Define an  $\mathcal{L}_2$ -theory

$$T_2 := T \cup \{c_i \neq c_j : i \neq j\}.$$

By the assumption, an  $\mathcal{L}_2$ -theory  $T \cup \{c_i \neq c_j : i \neq j, \max i, j \leq n\}$  is satisfiable, the compactness theorem implies  $T_2$  is satisfiable. Take a reduct.

IN PARTICULAR, we can take an arbitrarily large model of  $T$  by letting  $\mathcal{L}_2 := \mathcal{L} \cup \{c_\alpha : \alpha \in I\}$  with  $|I| = \kappa$  for any cardinal  $\kappa$ .  $\square$

**Theorem** (Upward Löwenheim-Skolem-Tarski theorem). Let  $T$  be an  $\mathcal{L}$ -theory. Suppose for every  $n \in \mathbb{N}$  there is a model  $\mathcal{M}$  of  $T$  with  $\|\mathcal{M}\| \geq n$ . Then, there is a model  $\mathcal{M}$  of  $T$  with  $\|\mathcal{M}\| = \kappa$  for every  $\kappa \geq |\mathcal{L}| + \aleph_0$ .

**Theorem** (Downward Löwenheim-Skolem-Tarski theorem). *Let  $T$  be an  $\mathcal{L}$ -theory. Let  $\mathcal{M}$  be an infinite model of  $T$ . Then, for every  $X \subset M$ , there is an elementary submodel  $\mathcal{H}(X)$  of  $\mathcal{M}$  such that  $X \subset |\mathcal{H}(X)|$  and  $|\mathcal{H}(X)| \leq |X| + |\mathcal{L}| + \aleph_0$ . The model  $\mathcal{H}(X)$  is called the Skolem hull of  $X$  in  $\mathcal{M}$ .*

**Example** (Skolem's paradox). Downward Löwenheim-Skolem theorem implies that  $ZF$  has a countably infinite model by taking  $X = \emptyset$ . Even though the existence of the power set of  $\mathbb{N}$  is provable in  $ZF$ , it is not a contradiction.

*Proof of the upward LST.* Pick a model  $\mathcal{M}$  of  $T$  such that  $\|\mathcal{M}\| \geq \kappa$ . Let  $X \subset M$  with  $|X| = \kappa$ . By the downward Löwenheim-Skolem, there is  $\mathcal{H}(X) \prec \mathcal{M}$  such that  $|\mathcal{H}(X)| \leq \kappa + |\mathcal{L}| + \aleph_0 = \kappa$ . Therefore,  $\kappa \leq |X| \leq |\mathcal{H}(X)|$  implies  $|\mathcal{H}(X)| = \kappa$ . □

## 8 Day 8: June 12

**Theorem** (Downward Löwenheim-Skolem-Tarski theorem). *Let  $T$  be an  $\mathcal{L}$ -theory. Let  $\mathcal{M}$  be an infinite model of  $T$ . Then, for every  $X \subset M$ , there is an elementary submodel  $\mathcal{H}(X)$  of  $\mathcal{M}$  such that  $X \subset |\mathcal{H}(X)|$  and  $|\mathcal{H}(X)| \leq |X| + |\mathcal{L}| + \aleph_0$ . The model  $\mathcal{H}(X)$  is called the Skolem hull of  $X$  in  $\mathcal{M}$ .*

*Proof.* Let  $\mathcal{L}_0 := \mathcal{L}$  and  $\mathcal{L}_{i+1} := \mathcal{L}_i \cup \mathcal{F}_i$ , where  $\mathcal{F}_i$  is constructed as follows: for each quantifier-free formula  $\theta[\bar{x}; \bar{y}]$  in  $\mathcal{L}_i$ , where  $\bar{x} = (x_1, \dots, x_n)$  and  $\bar{y} = (y_1, \dots, y_m)$ , we introduce new  $n$ -ary function symbols  $\{f_1, \dots, f_m\} = \mathcal{F}_i \setminus \mathcal{L}_i$ . Define  $\mathcal{L}_{sk} := \bigcup_i \mathcal{L}_i$  and  $\mathcal{F}_{sk} := \bigcup_i \mathcal{F}_i$ . Then,  $|\mathcal{F}_i| \leq |\mathcal{L}| + \aleph_0$  implies  $|\mathcal{F}_{sk}| \leq (|\mathcal{L}| + \aleph_0) \cdot \aleph_0 = |\mathcal{L}| + \aleph_0$ . The elements of  $\mathcal{F}_{sk}$  are called the Skolem functions.

We want to construct  $T_{sk}$  a theory over  $\mathcal{L}_{sk}$  such that

- (a) each  $\varphi \in T_{sk}$  is a universal formula in  $\mathcal{L}_{sk}$ ,
- (b) each  $\mathcal{L}$ -structure  $\mathcal{M}$  can be expanded to an  $\mathcal{L}_{sk}$ -structure  $\mathcal{M}_{sk}$  such that  $\mathcal{M}_{sk} \models T_{sk}$ ,
- (c) each  $\mathcal{L}$ -formula  $\varphi$  is equivalent to a universal formula  $\varphi_{\forall}$  and an existential formula  $\varphi_{\exists}$  in  $\mathcal{L}_{sk}$  over  $T_{sk}$ , i.e.  $T_{sk} \models \varphi \leftrightarrow \varphi_{\forall} \leftrightarrow \varphi_{\exists}$ .

Define  $T_{sk}$  by the following universal formula is an axiom in  $T_{sk}$ :

$$\forall \bar{x} \forall \bar{y} \theta[\bar{x}, \bar{y}] \rightarrow \theta[\bar{x}, \bar{f}(\bar{x})],$$

where  $\bar{f}(\bar{x}) := (f_1(\bar{x}), \dots, f_m(\bar{x}))$ . Then, (a) is clear.

If  $\varphi \equiv \forall x \exists y \theta[x, y]$  for a quantifier-free formula  $\theta$ , then

$$T_{sk} \models \varphi \leftrightarrow \forall x \theta[x, f(x)],$$

where  $f$  is any Skolem function. If  $\varphi \equiv \exists x \forall y \theta[x, y]$  for a quantifier-free formula  $\theta$ , then

$$T_{sk} \models \varphi \leftrightarrow \exists x \theta[x, g(x)],$$

where  $g$  is any function such that

$$\forall x, y (\neg \theta(x, y) \leftrightarrow \neg \theta(x, g(x)))$$

By operations to change any formula  $\varphi$  into a prenex normal form without harming the logical equivalence (we can establish an algorithm for it by extracting the quantifiers outside each negation, conjunction, and disjunction), (c) follows.

Now we prove the theorem. Expand the given  $\mathcal{L}$ -structure  $\mathcal{M}$  to an  $\mathcal{L}_{sk}$ -structure  $\mathcal{M}_{sk} \models T_{sk}$ . Define  $\mathcal{H}(X) := \bigcup_n X_n$ , where  $X_0 := X$  and

$$X_{n+1} := X_n \cup \{f^{\mathcal{M}}(\alpha_1, \dots, \alpha_m) \in \mathcal{M} \mid \alpha_1, \dots, \alpha_m \in X_n, f \text{ function symbol in } \mathcal{L}_{sk}\}.$$

Then, since  $\mathcal{H}(X)$  is closed under symbols  $\mathcal{L}_{sk}$ , it is a universe of a submodel of  $\mathcal{M}$ . Moreover, since

$$|X_n| \leq |X| + |\mathcal{F}_{sk}| \leq |X| + |\mathcal{L}_{sk}| + \aleph_0 \leq |X| + (|\mathcal{L}| + \aleph_0) + \aleph_0 = |X| + |\mathcal{L}| + \aleph_0,$$

we have  $|\mathcal{H}(X)| \leq (|X| + |\mathcal{L}| + \aleph_0) \cdot \aleph_0 = |X| + |\mathcal{L}| + \aleph_0$ .

Now we claim  $\mathcal{H}(X)$  is elementary submodel of  $\mathcal{M}$ . Since  $\mathcal{M}_{sk} \models T_{sk}$  and  $T_{sk}$  is a universal theory, we have  $\mathcal{H}(X) \models T_{sk}$ . For  $\varphi[\bar{x}]$  an  $\mathcal{L}$ -formula and  $\bar{a} = (\alpha_1, \dots, \alpha_n)$  with  $\alpha_i \in \mathcal{H}(X)$ , we want to show  $\mathcal{H}(X) \models \varphi[\bar{a}]$  if and only if  $\mathcal{M} \models \varphi[\bar{a}]$ . Pick a universal  $\varphi_{\forall}$  and existential  $\varphi_{\exists}$  such that  $T_{sk} \models \varphi \leftrightarrow \varphi_{\forall} \leftrightarrow \varphi_{\exists}$ . Then,

$$\begin{array}{ccccc} \mathcal{H}(X) \models \varphi_{\forall}[\bar{a}] & \iff & \mathcal{H}(X) \models \varphi[\bar{a}] & \iff & \mathcal{H}(X) \models \varphi_{\exists}[\bar{a}] \\ \uparrow & & & & \downarrow \\ \mathcal{M} \models \varphi_{\forall}[\bar{a}] & \iff & \mathcal{M} \models \varphi[\bar{a}] & \iff & \mathcal{M} \models \varphi_{\exists}[\bar{a}]. \end{array}$$

□

**Definition.** An  $\mathcal{L}$ -theory  $T$  is called *complete* if for each closed  $\mathcal{L}$ -formula  $\varphi$ ,  $T \models \varphi$  or  $T \models \neg\varphi$ .

For an  $\mathcal{L}$ -structure  $\mathcal{M}$ , we define  $\text{Th}(\mathcal{M})$  to be the closed  $\mathcal{L}$ -formulas  $\varphi$  such that  $\mathcal{M} \models \varphi$ . Two  $\mathcal{L}$ -structures  $\mathcal{M}$  and  $\mathcal{N}$  is called to be *elementary equivalent* if  $\text{Th}(\mathcal{M}) = \text{Th}(\mathcal{N})$ . Then,  $T$  is complete if and only if there exists a unique model of  $T$  up to elementary equivalence.

**Definition.** Let  $\kappa$  be an infinite cardinal. A theory  $T$  is called  $\kappa$ -*categorical* if there exists a unique model  $\mathcal{M}$  of  $T$  such that  $\|\mathcal{M}\| = \kappa$  up to isomorphism.

**Theorem** (Vaught test). *If every model of consistent theory  $T$  is infinite, and  $T$  is  $\kappa$ -categorical for a cardinal  $\kappa \geq |\mathcal{L}| + \aleph_0$ , then  $T$  is complete.*

*Proof.* Suppose  $T$  is incomplete and pick an  $\mathcal{L}$ -closed formula  $\varphi$  such that  $T \not\models \varphi$  and  $T \not\models \neg\varphi$ . By the upward Löwenheim-Skolem theorem, there are models  $\mathcal{M}_0$  and  $\mathcal{M}_1$  of  $T$  such that  $\mathcal{M}_0 \models T \cup \{\neg\varphi\}$ ,  $\mathcal{M}_1 \models T \cup \{\varphi\}$ , and  $\|\mathcal{M}_0\| = \|\mathcal{M}_1\| = \kappa$ . Since  $T$  is  $\kappa$ -categorical,  $\mathcal{M}_0$  and  $\mathcal{M}_1$  are isomorphic, which is a contradiction.  $\square$

**Example.** The following theories are complete.

- (a) Algebraic closed field in characteristic  $p$  ( $\text{ACF}_p$ ),
- (b) Vector spaces over  $\mathbb{Q}$ ,
- (c) Non-trivial torsion free divisible abelian groups.



## 9 Day 9: June 19

### Cut elimination

The cut is an inference rule

$$\frac{\Gamma, \neg C \quad C, \Gamma}{\Gamma}$$

where  $C$  is called a *cut formula*. We will consider the *weakening*

$$\frac{\Gamma, A_i}{\Gamma} (\vee)_i$$

for  $i = 0, 1$  when  $A_0 \vee A_1 \in \Gamma$ , instead of

$$\frac{\Gamma, A_0, A_1}{\Gamma} (\vee).$$

We can describe the inference rules of  $\mathbb{G}$  as the set  $\{(\vee)_0, (\vee)_1, (\wedge), (\exists), (\forall)\}$ . Then, the only inference rule which has two assumption sequent is the cut.

**Definition.** We define the *rank*  $\text{rk}(A)$  of a formula  $A$  inductively by  $\text{rk}(L) = 0$  for literal  $L$  and

$$\text{rk}(A_0 \vee A_1) = \text{rk}(A_0 \wedge A_1) := \max\{\text{rk}(A_0), \text{rk}(A_1)\} + 1, \quad \text{rk}(\exists x A) = \text{rk}(\forall x A) := \text{rk}(A) + 1.$$

We write  $\vdash_c^a \Gamma$  if there is a derivation  $\mathcal{D}$  of  $\Gamma$  in  $\mathbb{G} + (\text{cut})$  such that  $\text{depth}(S) \leq a$  and  $\text{rk}(C) < c$  for each cut formula  $C$  in  $\mathcal{D}$ .

If  $\Gamma$  is an axiom, i.e.  $\{\bar{L}, L\} \subset \Gamma$  for some literal  $L$ , then  $\vdash_c^a \Gamma$  holds for every  $a$  and  $c$ . Then, every inference rule has  $\vdash_c^a$  versions: if  $b < a$  then  $\vdash_c^b \Gamma'$  implies  $\vdash_c^a \Gamma$ , where  $\Gamma'$  is an assumption sequent of each inference rule.

**Theorem** (Cut elimination). *If  $\vdash_c^a \Gamma$ , then  $\vdash_0^{2_c(a)} \Gamma$ , where  $2_c(a) := 2^{2_{c-1}(a)}$  and  $2_1(a) := 2^a$ .*

*Proof.* Clear from the following lemma. □

**Lemma.** *If  $\vdash_{c+1}^a \Gamma$ , then  $\vdash_c^{2^a} \Gamma$ .*

*Proof.* We can prove the lemma from the reduction lemma in the below by induction and case study of inferences: axioms, inference by binary connectives and quantifiers (using  $b < a$  implies  $2^b < 2^a$ ), and inference by cuts. For the former two cases are easy.

For  $b < a$ , let  $\vdash_{c+1}^b \Gamma, \neg C$  and  $\vdash_{c+1}^b C, \Gamma$ . We obtain by the induction hypothesis that  $\vdash_c^{2^b} \Gamma, \neg C$  and  $\vdash_c^{2^b} C, \Gamma$ . We may assume that  $\text{rk}(C) \leq c$  and  $C$  is one of literals,  $C_0 \vee C_1$ , or  $\exists D$ . The reduction lemma implies that  $\vdash_c^{2^b + 2^b} \Gamma$ . Since  $2^b + 2^b \leq 2^a$ , we have  $\vdash_c^{2^a} \Gamma$ . □

**Lemma** (Reduction lemma). *Suppose  $C$  is a literal,  $C_0 \vee C_1$ , or  $\exists x D$  such that  $\text{rk}(C) \leq c$ . If  $\vdash_c^a \Gamma, \neg C$  and  $\vdash_c^b C, \Delta$ , then  $\vdash_c^{a+b} \Gamma, \Delta$ .*

We have

(Weaking)  $\vdash_c^a \Gamma$  implies  $\vdash_{c+a}^{a+b} \Gamma, \Delta$

(Inversion)  $\vdash_c^a \Gamma, A_0 \wedge A_1$  implies  $\vdash_c^a \Gamma, A_i$  for  $i = 0, 1$

(Inversion)  $\vdash_c^a \Gamma, \forall x D$  implies  $\vdash_c^a \Gamma, D(t)$  for a term  $t$ .

*Proof.* We use the induction on  $b$ . Suppose  $\vdash_c^b C, \Delta$ .

Case 1:  $\{\bar{L}, L\} \subset \{C\} \cup \Delta$  for a literal  $L$ . If  $C \neq L$  nor  $\bar{L}$ , then  $\{\bar{L}, L\} \subset \Delta$  so that  $\Gamma, \Delta$  is an axiom. If  $C = L$ , then  $\bar{L} \in \Delta$  so that  $\Gamma \cup \{\neg C\} = \Gamma \cup \{\bar{L}\} \subset \Gamma \cup \Delta$ . Then by weakening  $\vdash_c^a \Gamma, \neg C$  implies  $\vdash_c^{a+b} \Gamma, \Delta$ .

Case 2:  $C$  is the major formula of the last inference in  $\vdash_c^b C, \Delta$  with  $C \equiv \exists x D(x)$  or  $C \equiv C_0 \vee C_1$ . For  $b_0 < b$ ,

$$\frac{\vdash_c^{b_0} D(t), \exists D, \Delta}{\vdash_c^b \exists x D(x), \Delta}.$$

The induction hypothesis yields  $\vdash_c^{a+b_0} \Gamma, \Delta, D(t)$  and  $\vdash_c^a \Gamma, \neg D(t)$  by inversion. A cut with  $\text{rk}(D(t)) < \text{rk}(\exists x D) \leq c$  gives  $\vdash_c^{a+b} \Gamma, \Delta$ .

Case 3: otherwise. The induction hypothesis yields  $\vdash_c^{a+b_0} \Gamma, \Delta, \neg D$  and  $\vdash_c^{a+b_0} \Gamma, \Delta, D$ . We obtain  $\vdash_c^{a+b} \Gamma, \Delta$ .

□