I211E: Mathematical Logic

Nao Hirokawa

JAIST

Term 1-1, 2023

https://www.jaist.ac.jp/~hirokawa/lectures/ml/

Schedule

	propositional logic		predicate logic
4/13	syntax, semantics	5/11	syntax, semantics
4/18	normal forms	5/16	normal forms
4/20	examples	5/18	natural deduction I
4/25	natural deduction I	5/23	natural deduction II
4/27	natural deduction II	5/25	examples, properties
5/2	completeness	5/30	advanced topics
5/9	midterm exam	6/1	summary
		6/6	exam

Evaluation

midterm exam (40) + final exam (60)

Contents

Aim

to learn how to write mathematical proofs

Contents

1. resolution principle
2. Gödel's Incompleteness Theorem
3. to conclude...

Resolution Principle

Validity via Unsatisfiability

Fact

- $\Gamma \vdash \phi$ if and only if $\Gamma \cup \{\neg\phi\}$ is unsatisfiable
- ϕ is unsatisfiable if and only if Skolem normal form of ϕ is unsatisfiable

Note

- this proof style is called refutational proof
- many automatic theorem provers adopt this approach

$$\{\forall X, Y.\ (X \subseteq Y \leftrightarrow (\forall z.\ (z \in X \to z \in Y)))\}$$
$$\vdash \forall X, Y, Z.\ ((X \subseteq Y \wedge Y \subseteq Z) \to X \subseteq Z)$$

$$\iff \bigwedge \left\{ \begin{array}{l} \forall X, Y, z. X \not\subseteq Y \ \vee\ z \notin X \ \vee\ z \in Y \\ \neg\forall X, Y, Z.((X \subseteq Y \wedge Y \subseteq Z) \to X \subseteq Z) \end{array} \right\} \text{ is unsatisfiable}$$

$$\iff \forall X, Y, z. \bigwedge \left\{ \begin{array}{l} X \not\subseteq Y \ \vee\ z \notin X \ \vee\ z \in Y \\ X \subseteq Y \ \vee\ \mathsf{f}(X, Y) \in X \\ X \subseteq Y \ \vee\ \mathsf{f}(X, Y) \notin Y \\ \mathsf{A} \subseteq \mathsf{B} \\ \mathsf{B} \subseteq \mathsf{C} \\ \mathsf{A} \not\subseteq \mathsf{C} \end{array} \right\} \text{ is unsatisfiable}$$

Resolution

- axioms: all clauses in matrix of Skolem normal form
- inference rule 1:

$$\frac{C \vee L \qquad C' \vee \neg L'}{C\theta \vee C'\theta}\ \text{RESOLVE}$$

  if θ is most general substitution with $L\theta = L'\theta$ (rename if necessary)
- inference rule 2:

$$\frac{C}{C\theta}\ \text{FACTORIZE}$$

  if σ is most general substitution that literals L and L' in C satisfy $L\theta = L'\theta$

Theorem (resolution principle)

sentence $\forall\vec{x}. \bigwedge\Gamma$ in Skolem normal form whose matrix is in CNF is unsatisfiable if and only if resolution derives $\perp$ from Γ

$$\bigwedge \left\{ \begin{array}{l} X \not\subseteq Y \ \vee\ z \notin X \ \vee\ z \in Y \\ X \subseteq Y \ \vee\ \mathsf{f}(X, Y) \in X \\ X \subseteq Y \ \vee\ \mathsf{f}(X, Y) \notin Y \\ \mathsf{A} \subseteq \mathsf{B} \\ \mathsf{B} \subseteq \mathsf{C} \\ \mathsf{A} \not\subseteq \mathsf{C} \\ z \notin \mathsf{A} \ \vee\ z \in \mathsf{B} \\ z \notin \mathsf{B} \ \vee\ z \in \mathsf{C} \\ z \notin \mathsf{A} \ \vee\ z \in \mathsf{C} \\ \mathsf{f}(\mathsf{A}, \mathsf{C}) \in \mathsf{A} \\ \mathsf{f}(\mathsf{A}, \mathsf{C}) \notin \mathsf{C} \\ \mathsf{f}(\mathsf{A}, \mathsf{C}) \in \mathsf{C} \\ \perp \end{array} \right\}$$

thus, original claim is correct

Gödel's Incompleteness Theorem

Is Mathematics Consistent?

Theorem (?)

$-1 = 1$

Proof (which of = is wrong?).

using Euler's formula $e^{i\theta} = \cos\theta + i\sin\theta$

$$-1 = e^{i\pi} = e^{i2\pi\cdot\frac{1}{2}} = (e^{i2\pi})^{\frac{1}{2}} = 1^{\frac{1}{2}} = 1 \qquad \square$$

Theorem (Russell's Paradox 1902)

naive set theory is inconsistent, so $-1 = 1$

Proof.

for $A = \{X \mid X \notin X\}$ we have $A \in A$ iff $A \notin A$. contradiction $\square$

Aftermath

- proofs were formalized; natural deduction was introduced
- naive set theory was replaced by axiomatic set theories including $\mathbf{ZFC}$
- now consistency of math seems to be recovered, but what about its proof?
- suppose that we adopt natural deduction for first-order logic with $\mathbf{ZFC}$
- if $\mathbf{ZFC}$ is consistent, its consistency cannot be shown in $\mathbf{ZFC}$
  (Gödel's second incompleteness theorem; Rosser's incompleteness theorem)
- if $\mathbf{ZFC}$ is inconsistent, consistency of $\mathbf{ZFC}$ can be shown in $\mathbf{ZFC}$ (sigh)

To Conclude...

Final Exam

- closed book, written exam; about 90 min, at the lecture room
- about contents of lectures 8–14 and corresponding homework exercises

  1. soundness of propositional logic
  2. structures and models
  3. substitutions and variable capture
  4. prenex/Skolem normal forms
  5. natural deduction
  6. equality reasoning
  7. proof writing
  8. encodings in logic

- exam questions are similar to examples of slides and homework exercises

Samples of Exam Questions 1/2

1. Show that the inference rule for $\vee\mathrm{E}$ in propositional logic is valid.
2. Consider the structure $\mathcal{A} = (\mathbb{N}, \bar{\mathsf{P}})$ with

   $$\bar{\mathsf{P}} = \{(a, b) \mid a, b \in \mathbb{N} \text{ and } a > b\}$$

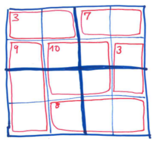
   Let $\phi = \mathsf{P}(x, y) \wedge \forall x \exists y\, \mathsf{P}(x, y)$.
   - a. Compute $\phi[y/x]$.
   - b. Does $\mathcal{A}, v \vDash \phi$ hold for $v = \{x \mapsto 1, y \mapsto 2\}$?
   - c. Prove or disprove $\mathcal{A} \models \forall x \exists y\, \mathsf{P}(x, y)$.
3. Show that $\forall x \exists y \mathsf{R}(x, y) \to \exists x \forall y \mathsf{R}(x, y)$ is invalid
4. Compute a prenex normal form and a Skolem normal form of the formula:

   $$\mathsf{P}(x) \leftrightarrow \forall x \exists y \mathsf{Q}(x, y)$$

5. Let ϕ be a sentence and θ a substitution. Show that $\phi\theta = \phi$.

Samples of Exam Questions 2/2

5. Write proof trees (derivations):
   1. $\vdash (\mathsf{P}(\mathsf{f}(x)) \wedge \forall x \mathsf{P}(x)) \to \forall x\, \mathsf{P}(\mathsf{f}(x)))$
   2. $\vdash (\neg \exists x \forall y\, \mathsf{P}(x, y)) \to \forall x \exists y\, \neg \mathsf{P}(x, y)$
   3. $\mathbf{Q} \vdash \neg(\mathsf{s}(0) + \mathsf{s}(0) \doteq 0)$
   4. $\mathbf{PA} \vdash \forall x(0 + x \doteq x)$
6. Show the equation on sets: $\bigcup_{i \in \mathbb{N}} \{i, i+1\} = \mathbb{N}$.
7. We solve the following Killer Sudoku problem by using the SMT solver.



   Encode the problem to a linear arithmetic constraint whose satisfying assignment results in a solution of the problem.

Reading/Writing Formulas and Proofs

- two plus three makes five:

  $$2 + 3 = 5$$

- every number $x \in \mathbb{R}$ satisfies $x^2 \geqslant 0$:

  $$\forall x \in \mathbb{R}. \quad x^2 \geqslant 0$$

- mathematical induction: $P(n)$ holds for all $n \in \mathbb{N}$ if next conditions hold: (i) $P(0)$, (ii) for every $k \in \mathbb{N}$ if $P(k)$ then $P(k+1)$:

  $$(P(0) \wedge (\forall k \in \mathbb{N}.\ P(k) \to P(k+1))) \ \to \forall n \in \mathbb{N}.\ P(n)$$

Proposition

If p implies q and q implies r then p implies r. $((p \to q) \land (q \to r)) \to (p \to r)$

Proof.

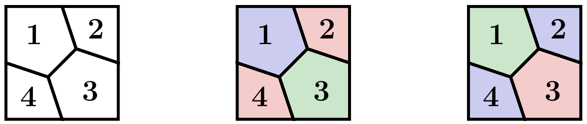
Assume that p implies q and q implies r. Suppose that p holds. By the first assumption we have q. By the second assumption we have r. Therefore, p implies r. □

$$\dfrac{\dfrac{\dfrac{\dfrac{[p]^2 \quad \dfrac{[(p \to q) \land (q \to r)]^1}{p \to q}\,\land\text{-E}}{q}\,\to\text{-E} \qquad \dfrac{[(p \to q) \land (q \to r)]^1}{q \to r}\,\land\text{-E}}{r}\,\to\text{-E}}{p \to r}\,\to\text{-I}_2}{((p \to q) \land (q \to r)) \to (p \to r)}\,\to\text{-I}_1$$

Solving Sudoku

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

Map Coloring



Goal of This Course

Goal

- able to **read and write** logical formulas
- able to **transform** formulas
- able to **prove/disprove** formulas

Ultimate Goal

develop skills to **read textbooks** and to **write definitions/proofs in thesis**