# G22.3033.11 — Logic and Verification

## Lecture 9

# Review

## Last time

- Motivation
- First-Order Logic: Syntax
- First-Order Logic: Semantics
- Definability
- Homomorphisms and Undefinability

# Outline

- A Deductive Calculus
- Generalization and Deduction Theorems
- Soundness and Completeness
- Compactness
- Size of Models

Sources:

Sections 2.4 through 2.5 of Enderton.

W. Hodges. *A Shorter Model Theory*. Cambridge Press, 1997.

## Proofs

Suppose that $\Gamma \models \tau$.

How do we demonstrate or convince a skeptic of this fact?

In propositional logic, a skeptic could use a truth table to check such a fact.

In first-order logic, no such method exists: we cannot, in general, enumerate all possible models and variable assignments.

Instead, we rely on the notion of a mathematical proof.

# Proofs

A *proof* is a finite sequence of fixed indisputable steps.

A proof is built from *axioms*, facts which we accept without proof, and *theorems*, which are facts derived from axioms using an agreed-upon set of *rules of inference*.

Because the proof is finite and each step conforms to a pre-determined set of rules, the question of whether a given sequence of steps is a proof is decidable.

Thus, a proof is an effective mechanism for convincing a skeptic.

# A Deductive Calculus

There are many possible choices for the axioms and rules of inference.

A particular choice of axioms and rules of inference is often referred to as a *calculus*.

We present a calculus which has an infinite number of axioms, which we will denote as $\Lambda$, and which uses only a single rule of inference, known as *modus ponens*.

This rule states that given formulas $\alpha$ and $\alpha \to \beta$ we may infer $\beta$.

Rules of inference are often written in the following format with the given formulas above and the deduced formula below:

$$\frac{\alpha, \alpha \to \beta}{\beta}.$$

A set of formulas $\Delta$ is *closed under modus ponens* iff whenever $\alpha$ and $\alpha \to \beta$ are in $\Delta$, so is $\beta$.

# A Deductive Calculus

Given a set of formulas $\Gamma$, we say that $\Delta$ is *inductive* (with respect to $\Gamma$) iff $\Gamma \cup \Lambda \subseteq \Delta$ and $\Delta$ is closed under modus ponens.

The set of *theorems of* $\Lambda$ is the smallest inductive set.

Note that although this set is well-defined, it is not freely generated.

We write $\Gamma \vdash \phi$ iff $\phi$ belongs to the set generated from $\Gamma \cup \Lambda$ by modus ponens.

A *deduction of* $\phi$ *from* $\Gamma$ is a sequence $< \alpha_0, \ldots, \alpha_n >$ of formulas such that $\alpha_n = \phi$ and for each $i \leq n$ either

- $\alpha_i$ is in $\Gamma \cup \Lambda$, or
- for some $j$ and $k$ less than $i$, $\alpha_i$ is obtained by modus ponens from $\alpha_j$ and $\alpha_k$ (i.e. $\alpha_k = \alpha_j \rightarrow \alpha_i$).

# A Deductive Calculus

For propositional logic, we showed that the set $C_*$ of things having construction sequences coincides with the set $C^*$ of the intersection of all inductive sets.

The equivalent property in the current context is as follows.

**Theorem**

There exists a deduction of $\alpha$ from $\Gamma$ iff $\Gamma \vdash \alpha$.

**Proof**

If there is a deduction $< \alpha_0, \ldots, \alpha_n >$, then by induction on $i$, each $\alpha_i$ belongs to the set generated from $\Gamma \cup \Lambda$ by modus ponens.

Conversely, the set of formulas for which deductions exist includes $\Gamma \cup \Lambda$. Furthermore, we can show that this set is closed under modus ponens. (How?)

$\square$

We can thus say that $\phi$ is *deducible* from $\Gamma$ iff $\Gamma \vdash \phi$.

# Axioms

A *wff* $\phi$ is a *generalization* of $\psi$ iff for some variables $x_1, \ldots, x_n$, where $n \geq 0$, we have $\phi = \forall x_1 \cdots \forall x_n \psi$.

The axioms $\Lambda$ are made up of all generalizations of *wffs* of the following forms, where $x$ and $y$ are variables and $\alpha$ and $\beta$ are *wffs*.

1. Tautologies
2. $\forall x \, \alpha \to \alpha^x_t$, where $t$ is substitutable for $x$ in $\alpha$;
3. $\forall x \, (\alpha \to \beta) \to (\forall x \, \alpha \to \forall x \, \beta)$;
4. $\alpha \to \forall x \, \alpha$, where $x$ does not occur free in $\alpha$;
5. $x = x$;
6. $x = y \to (\alpha \to \alpha')$, where $\alpha$ is atomic and $\alpha'$ is obtained from $\alpha$ by replacing $x$ in zero or more places by $y$.

Note that the axioms depend on the definition of a well-formed formula which requires that a language be specified. The last two items are only included if the language includes equality.

# Axioms

### Tautologies

Axiom group 1 consists of *tautologies*. These are the *wffs* obtainable from tautologies of propositional logic by replacing each propositional symbol by a *wff* of the first-order language.

For example, consider the propositional tautology

$$(A \to \neg B) \to (B \to \neg A).$$

A corresponding axiom is the formula

$$\forall\, x\, [(\forall\, y\, \neg Py \to \neg Px) \to (Px \to \neg \forall\, y\, \neg Py)].$$

There is a more direct way to view the relationship of first-order and propositional logic.

A first-order formula is *prime* if it is atomic or of the form $\forall\, x\, \alpha$.

First-order formulas correspond exactly to propositional logic formulas in which the set of propositional symbols is taken to be all prime first-order formulas.

# Tautologies

By viewing first-order formulas as instances of propositional logic formulas, all propositional notions are also defined for first-order formulas.

Thus, the notions of *tautology*, *tautological consequence*, and *tautological implication* are thus directly applicable to first-order formulas.

**Theorem**

If $\Gamma$ tautologically implies $\phi$, then $\Gamma$ logically implies $\phi$.

Note that the converse fails.

**Theorem**

$\Gamma \vdash \phi$ iff $\Gamma \cup \Lambda$ tautologically implies $\phi$.

**Proof**

$\Rightarrow$: Follows from the fact that modus ponens is propositionally valid.

$\Leftarrow$: By the compactness theorem for propositional logic, there is a finite subset $\Delta = \{\delta_1, \ldots, \delta_m\}$ of $\Gamma \cup \Lambda$ which tautologically implies $\phi$. Thus, $\delta_1 \to \ldots \to \delta_m \to \phi$ is a tautology and hence is in $\Lambda$. By applying modus ponens $m$ times, we obtain $\phi$.

# Substitution

The second axiom group contains formulas of the form $\forall\, x\, \alpha \to \alpha^x_t$.

The notation $\alpha^x_t$ denotes the expression obtained from $\alpha$ by replacing $x$, wherever it occurs free in $\alpha$, by the term $t$.

We must also impose the restriction that $t$ be *substitutable* for $x$ in $\alpha$, defined as follows.

- For atomic $\alpha$, $t$ is substitutable for $x$ in $\alpha$.
- $t$ is substitutable for $x$ in $(\neg\alpha)$ iff it is substitutable for $x$ in $\alpha$, and $t$ is substitutable for $x$ in $(\alpha \to \beta)$ iff it is substitutable for $x$ in both $\alpha$ and $\beta$.
- $t$ is substitutable for $x$ in $\forall\, y\, \alpha$ iff either
  - $x$ does not occur free in $\forall\, y\, \alpha$, or
  - $y$ does not occur in $t$ and $t$ is substitutable for $x$ in $\alpha$.

# Example

For convenience, we repeat the first three axiom groups here:

1. Tautologies
2. $\forall x\, \alpha \to \alpha^x_t$, where $t$ is substitutable for $x$ in $\alpha$;
3. $\forall x\, (\alpha \to \beta) \to (\forall x\, \alpha \to \forall x\, \beta)$;

We will prove $\vdash \forall x\, (Px \to \exists y\, Py)$.

| | | |
|---|---|---|
| 1. | $\forall x\, [(\forall y\, \neg Py \to \neg Px) \to (Px \to \neg\forall y\, \neg Py)]$ | Tautology |
| 2. | $\forall x\, (\forall y\, \neg Py \to \neg Px) \to \forall x\, (Px \to \neg\forall y\, \neg Py)$ | MP(Axiom group 3, 1) |
| 3. | $\forall x\, (\forall y\, \neg Py \to \neg Px)$ | Axiom group 2 |
| 4. | $\forall x\, (Px \to \neg\forall y\, \neg Py)$ | MP(3, 2) |

# Generalization Theorem

**Theorem**

If $\Gamma \vdash \phi$ and $x$ does not occur free in any formula in $\Gamma$, then $\Gamma \vdash \forall x\, \phi$.

**Proof**

It suffices to show that the set $\{\phi \mid \Gamma \vdash \forall x\, \phi\}$ includes $\Gamma \cup \Lambda$ and is closed under modus ponens.

- Suppose $\phi \in \Gamma$. Then $x$ does not occur free in $\phi$. Thus $\phi \rightarrow \forall x\, \phi$ is in axiom group 4, and it follows that $\Gamma \vdash \forall x\, \phi$.
- Suppose $\phi \in \Lambda$. Then $\forall x\, \phi$ is also an axiom, so $\Gamma \vdash \forall x\, \phi$.
- Suppose $\Gamma \vdash \forall x\, \psi$ and $\Gamma \vdash \forall x\, (\psi \rightarrow \phi)$. Using axiom group 3, we obtain $\Gamma \vdash \forall x\, \psi \rightarrow \forall x\, \phi$, and thus $\Gamma \vdash \forall x\, \phi$.

**Theorem (rule T)**

If $\Gamma \vdash \alpha_1, \ldots, \Gamma \vdash \alpha_n$ and $\{\alpha_1, \ldots, \alpha_n\}$ tautologically implies $\beta$, then $\Gamma \vdash \beta$.

**Proof**

Apply modus ponens $n$ times to $\alpha_1 \rightarrow \cdots \rightarrow \alpha_n \rightarrow \beta$, which is a tautology.

# Deduction Theorem

**Theorem**

If $\Gamma \cup \{\gamma\} \vdash \phi$ then $\Gamma \vdash (\gamma \to \phi)$.

**Proof**

$\Gamma \cup \{\gamma\} \vdash \phi$ iff $\Gamma \cup \{\gamma\} \cup \Lambda$ tautologically implies $\phi$
iff $\Gamma \cup \Lambda$ tautologically implies $\gamma \to \phi$
iff $\Gamma \vdash (\gamma \to \phi)$.

**Corollary (contraposition)**

$\Gamma \cup \{\phi\} \vdash \neg\psi$ iff $\Gamma \cup \{\psi\} \vdash \neg\phi$.

A set of formulas is *inconsistent* iff for some *wff* $\beta$, both $\beta$ and $\neg\beta$ are theorems of the set.

**Corollary (reductio ad absurdum)**

If $\Gamma \cup \{\phi\}$ is inconsistent, then $\Gamma \vdash \neg\phi$.

# Example

Often it is easiest to work backward. Consider showing that

$$\vdash \exists x\, \forall y\, \phi \rightarrow \forall y\, \exists x\, \phi.$$

By the deduction theorem, it suffices to show that

$$\exists x\, \forall y\, \phi \vdash \forall y\, \exists x\, \phi.$$

By the generalization theorem, it suffices to show that

$$\exists x\, \forall y\, \phi \vdash \exists x\, \phi,$$

which is equivalent to

$$\neg\forall x\, \neg\forall y\, \phi \vdash \neg\forall x\, \neg\phi.$$

By contraposition, it thus suffices to show that

$$\forall x\, \neg\phi \vdash \forall x\, \neg\forall y\, \phi.$$

And again, by generalization, it suffices to show that

$$\forall x\, \neg\phi \vdash \neg\forall y\, \phi.$$

# Example

To show

$$\forall x \, \neg\phi \vdash \neg\forall y \, \phi,$$

it suffices (by reductio ad absurdum) to show that

$$\forall x \, \neg\phi, \forall y \, \phi$$

is inconsistent.

But this is easy to see, since

$$\forall x \, \neg\phi \quad \vdash \quad \neg\phi \text{ and}$$
$$\forall y \, \phi \quad \vdash \quad \phi.$$

## Syntactic strategies

Often, a strategy for producing a proof can be chosen by looking at the syntax of the formula to be proved.

- Suppose $\phi = (\psi \to \theta)$. Then it is sufficient (and always possible) to show that $\Gamma \cup \{\psi\} \vdash \theta$
- Suppose that $\phi$ is $\forall\, x\; \psi$. If $x$ does not occur free in $\Gamma$, then it will suffice to show that $\Gamma \vdash \psi$. If $x$ does occur free in $\Gamma$, then it can be renamed so that it does not.
- Suppose $\phi$ is the negation of another formula.
  - If $\phi = \neg(\psi \to \theta)$, then it suffices (by rule T) to show that $\Gamma \vdash \psi$ and $\Gamma \vdash \neg\theta$.
  - If $\phi = \neg\neg\psi$, then it suffices to show $\Gamma \vdash \psi$.
  - If $\phi = \neg\forall\, x\; \psi$, then it suffices to show that $\Gamma \vdash \neg\psi^x_t$, where $t$ is substitutable for $x$ in $\psi$. Unfortunately, this is not always possible.

As an example of when the last strategy fails, consider $\neg\forall\, x\; \neg(Px \to \forall\, y\; Py)$.

It is true that $\vdash \neg\forall\, x\; \neg(Px \to \forall\, y\; Py)$, but for every term $t$, $\nvdash (Pt \to \forall\, y\; Py)$.

# Generalization on Constants

**Theorem**

Suppose $\Gamma \vdash \phi$ and $c$ is a constant symbol which does not occur in $\Gamma$. Then there is a variable $y$ which does not occur in $\Gamma$ such that $\Gamma \vdash \forall\, y\; \phi^c_y$. Furthermore, there is a deduction of $\forall\, y\; \phi^c_y$ in which $c$ does not occur.

**Proof**

Let $< \alpha_0, \ldots, \alpha_n >$ be a deduction of $\phi$ from $\Gamma$. Let $y$ be a variable which does not occur in any $\alpha_i$. We claim that $< (\alpha_0)^c_y, \ldots, (\alpha_n)^c_y >$ is a deduction from $\Gamma$ of $\phi^c_y$.

- Case 1: $\alpha_k \in \Gamma$. Then $c$ does not occur in $\alpha_k$, so $(\alpha_k)^c_y = \alpha_k$, which is in $\Gamma$.
- Case 2: $\alpha_k \in \Lambda$. A careful examination of the axioms reveals that if $(\alpha_k)^c_y$ must also be in $\Lambda$.
- Case 3: $\alpha_k$ is obtained by modus ponens from $\alpha_i$ and $\alpha_j$. It follows that $(\alpha_k)^c_y$ is obtained by modus ponens from $(\alpha_i)^c_y$ and $(\alpha_j)^c_y$.

It follows from the generalization theorem that there is a deduction of $\forall\, y\; \phi^c_y$, and it is not hard to see that $c$ does not occur in the deduction.

# Corollaries

**Corollary**

If $\Gamma \vdash \phi^x_c$, where $c$ does not occur in $\Gamma$ or in $\phi$, then $\Gamma \vdash \forall x\, \phi$, and there is a deduction in which $c$ does not occur.

**Corollary (rule EI)**

If $\Gamma \cup \{\phi^x_c\} \vdash \psi$ and $c$ does not occur in any of $\Gamma$, $\phi$, or $\psi$, then $\Gamma \cup \{\exists x\, \phi\} \vdash \psi$, and there is a deduction in which $c$ does not occur.

# Alphabetic Variants

An *alphabetic variant* of a formula $\phi$ is a formula $\phi'$ obtained by renaming some of the bound variables of $\phi$. This is useful when we want to substitute $t$ into $\phi$, but $t$ is not substitutable.

**Theorem (Existence of Alphabetic Variants)**

Let $\phi$ be a formula, $t$ a term, and $x$ a variable. Then there exists $\phi'$ such that

1. $\phi \vdash \phi'$ and $\phi' \vdash \phi$; and
2. $t$ is substitutable for $x$ in $\phi'$.

**Proof**

We construct $\phi'$ by recursion on $\phi$.

- If $\phi$ is atomic, $\phi' = \phi$
- $(\neg\phi)' = (\neg\phi')$ and $(\phi \to \psi)' = (\phi' \to \psi')$
- $(\forall\, y\, \phi)' = \forall\, z\, (\phi')^y_z$, where $z$ does not appear in $\phi'$ or $t$ or $x$.

It is not hard to show that the two conditions are satisfied by this definition.

# Equality

Assuming the language includes equality, the following are the standard set of common facts about equality. Their proofs are straightforward.

1. Reflexivity: $\vdash \forall x\, x = x$.

2. Symmetry: $\vdash \forall x\, \forall y\, (x = y \to y = x)$.

3. Transitivity: $\vdash \forall x\, \forall y\, \forall z\, (x = y \to y = z \to x = z)$.

4. Substitutivity in predicates: if $P$ is an $n$-place predicate symbol, then $\vdash \forall x_1 \ldots \forall x_n\, \forall y_1 \ldots \forall y_n\, (x_1 = y_1 \to \ldots \to x_n = y_n \to Px_1 \ldots x_n \to Py_1 \ldots y_n)$.

5. Substitutivity in functions: if $f$ is an $n$-place function symbol, then $\vdash \forall x_1 \ldots \forall x_n\, \forall y_1 \ldots \forall y_n\, (x_1 = y_1 \to \ldots \to x_n = y_n \to fx_1 \ldots x_n = fy_1 \ldots y_n)$.

# Soundness and Completeness

An important question for any calculus is its relationship to the semantic notion of validity.

If only valid formulas are deducible, then the calculus is said to be *sound*.

If all valid formulas are deducible, then the calculus is said to be *complete*.

The existence of a sound and complete calculus for first-order logic is an important result which demonstrates that it is a reasonable model of mathematical thinking.

# Soundness

### Soundness Theorem

If $\Gamma \vdash \phi$, then $\Gamma \models \phi$.

### Proof

The idea of the proof is that the logical axioms are logically valid, and that modus ponens preserves logical implications.

We first assume the axioms are valid and prove by induction that any formula $\phi$ deducible from $\Gamma$ is logically implied by $\Gamma$.

- Case 1: if $\phi$ is a logical axiom, then by our assumption, $\models \phi$, and thus $\Gamma \models \phi$.
- Case 2: If $\phi \in \Gamma$, then clearly $\Gamma \models \phi$.
- Case 3: If $\phi$ is obtained by modus ponens from $\psi$ and $\psi \rightarrow \phi$, then by the inductive hypothesis, $\Gamma \models \psi$ and $\Gamma \models (\psi \rightarrow \phi)$. It follows by the definition of $\models$ for $\rightarrow$ that $\Gamma \models \phi$.

# Soundness

It remains to show that the axioms are valid. We will consider only Axiom Group 2 (the others are straightforward). First a lemma.

**Substitution Lemma**

If the term $t$ is substitutable for the variable $x$ in the *wff* $\phi$, then for any model $M$ and variable assignment $\rho$, $M \models_\rho \phi^x_t$ iff $M \models_{\rho(x|\overline{\rho}(t))} \phi$.

This lemma states that if we replace a variable $x$ with a term $t$, the semantics are the same as if the variable assignment is modified so that $x$ takes on the same value as the term $t$.

The proof is by induction on $\phi$.

Now, consider Axiom Group 2: $\forall\, x\, \alpha \to \alpha^x_t$, where $t$ is substitutable for $x$ in $\alpha$.

Assume $M \models_\rho \forall\, x\, \alpha$. We must show that $M \models_\rho \alpha^x_t$. We know from $M \models_\rho \forall\, x\, \alpha$ that for any $d \in \mathit{dom}(M)$, $M \models_{\rho(x|d)} \alpha$. In particular, if we let $d = \overline{\rho}(t)$, then we have $M \models_{\rho(x|\overline{\rho}(t))} \alpha$. But by the substitution lemma, this implies that $M \models_\rho \alpha^x_t$.

# Soundness Corollaries

**Corollary**

If $\vdash (\phi \leftrightarrow \psi)$, then $\phi$ and $\psi$ are logically equivalent.

**Corollary**

If $\phi'$ is an alphabetic variant of $\phi$, then $\phi$ and $\phi'$ are logically equivalent.

Recall that a set $\Gamma$ is consistent iff there is no formula $\phi$ such that both $\Gamma \vdash \phi$ and $\Gamma \vdash \neg\phi$. Define $\Gamma$ to be *satisfiable* iff there is some model $M$ and variable assignment $\rho$ such that $M \models_\rho \Gamma$.

**Corollary**

If $\Gamma$ is satisfiable, then $\Gamma$ is consistent.

# Completeness

**Completeness Theorem (Gödel, 1930)**

If $\Gamma \models \phi$, then $\Gamma \vdash \phi$.

We will prove an equivalent statement: any consistent set of formulas is satisfiable (the proof that this is equivalent is part of the homework).

# Compactness

### Compactness Theorem

If every finite subset $\Gamma_0$ of $\Gamma$ is satisfiable, then $\Gamma$ is satisfiable.

### Proof

Suppose every finite subset $\Gamma_0$ of $\Gamma$ is satisfiable. By soundness, every finite subset is consistent. But since deductions are finite, it follows that $\Gamma$ is consistent. Thus, by completeness, $\Gamma$ is satisfiable.

$\square$

### Corollary

If $\Gamma \models \phi$, then for some finite $\Gamma_0 \subseteq \Gamma$ we have $\Gamma_0 \models \phi$.

### Proof

Suppose to the contrary that $\Gamma_0 \not\models \phi$ for every finite $\Gamma_0 \subseteq \Gamma$. Then every finite subset of $\Gamma \cup \{\neg\phi\}$ is satisfiable, and thus $\Gamma \cup \{\neg\phi\}$ is satisfiable. It follows that $\Gamma \not\models \phi$.

$\square$