Lecture 19

Pete Manolios
Northeastern

Thomas Wahl

Pitching his spring class

Proof Theory

- Goal: relate $\Phi \models \phi$ to $\Phi \vdash \phi$
- We defined $\models$, next we define $\vdash$
- $\Phi \vdash \phi$ denotes that ϕ is provable from Φ
- Provability should be machine checkable
- It may seem hopeless to nail down what a proof is
  - don't mathematicians expand their proof methods?
- FOL has a fairly simply set of obvious rules
- There are many equivalent ways of defining proof
  - In fact, we've seen how to do this already in a very sophisticated way using U-/UH-resolution

Sequent Calculus

- A sequent is a nonempty sequence of formulas
- Sequent rules:

$$\frac{\begin{array}{l}\Gamma \;\; \neg\phi \;\; \psi \\ \Gamma \;\; \neg\phi \;\; \neg\psi\end{array}}{\Gamma \;\; \phi} \qquad \frac{}{\Gamma \;\; \phi} \text{ if } \phi \text{ is a member of } \Gamma$$

- The left rule says if you have a proof of both $\neg\psi$ and ψ from $\Gamma \cup \{\neg\phi\}$, that constitutes a proof of ϕ from Γ
- If there is a derivation of the sequent $\Gamma\ \phi$, then we write $\vdash \Gamma\ \phi$ and say that $\Gamma\ \phi$ is *derivable*
- A formula ϕ is *formally provable* or *derivable* from a set Φ of formulas, written $\Phi \vdash \phi$, iff there are *finitely* many formulas $\phi_1, \ldots, \phi_n$ in Φ s.t. $\vdash \phi_1 \ldots \phi_n\ \phi$

Sequent Rules

Antecedent Rule (Ant)

$$\frac{\Gamma \quad \varphi}{\Gamma' \quad \varphi} \text{ if every member of } \Gamma \text{ is also a member of } \Gamma'.$$

A sequent Γ ϕ is *correct* if Γ ⊨ ϕ

A rule is *correct*: applied to correct sequents, it yields correct sequents

Notice that the sequent rules are correct

Assumption Rule (Assm)

$$\frac{}{\Gamma \quad \varphi} \text{ if } \varphi \text{ is a member of } \Gamma.$$

Proof by Cases Rule (PC)

$$\begin{array}{lll} \Gamma & \psi & \varphi \\ \Gamma & \neg\psi & \varphi \\ \hline \Gamma & & \varphi \end{array}$$

Contradiction Rule (Ctr)

$$\begin{array}{lll} \Gamma & \neg\varphi & \psi \\ \Gamma & \neg\varphi & \neg\psi \\ \hline \Gamma & & \varphi \end{array}$$

Sequent Rules for ∨

∨-Rule for the Antecedent (∨ A)

$$\frac{\begin{array}{lll}\Gamma & \varphi & \xi \\ \Gamma & \psi & \xi\end{array}}{\Gamma \quad (\varphi \lor \psi) \quad \xi}$$

∨-Rule for the Succedent (∨ S)

$$\text{(a)}\,\frac{\Gamma \quad \varphi}{\Gamma \quad (\varphi \lor \psi)} \qquad\qquad \text{(b)}\,\frac{\Gamma \quad \varphi}{\Gamma \quad (\psi \lor \varphi)}$$

Derived Sequent Rules

Tertium non datur (Ctr)

$$\frac{}{(\varphi \vee \neg\varphi)}$$

Proof? We can prove it by assuming φ, getting $\varphi \vee \neg\varphi$ and similarly with $\neg\varphi$.

1.	φ	φ	(Ant)
2.	φ	$(\varphi \vee \neg\varphi)$	($\vee$ S)
3.	$\neg\varphi$	$\neg\varphi$	(Ant)
4.	$\neg\varphi$	$(\varphi \vee \neg\varphi)$	($\vee$ S)
5.		$(\varphi \vee \neg\varphi)$	(PC)

- Defining derived rules helps us keep proofs short
- For our purposes, we want a minimal set of built-in rules
- If we wanted to use the logic, we would want a large set of rules (consider ACL2s)

Sequent Rules

Reflexivity Rule for Equality ($\equiv$)

$$\frac{}{t \equiv t}$$

Substitution Rule for Equality (Sub)

$$\frac{\Gamma \qquad\qquad \varphi\frac{t}{x}}{\Gamma \quad t \equiv t' \quad \varphi\frac{t'}{x}}$$

- Can derive that equality is symmetric and transitive (so equivalence)
- Can derive that equality is a congruence
- Suppose Φ is a set of equations (universal formulas of the form $s \equiv t$) and ϕ is an equation
  - Then, $\Phi \vDash \phi$ iff $\Phi \vdash \phi$ where we only use Assm, Sub, equivalence and congruence rules (Birkhoff's theorem)
  - More on this soon

Sequent Rules for ∃

∃-Introduction in the Succedent (∃ S)

$$\frac{\Gamma \quad \varphi\frac{t}{x}}{\Gamma \quad \exists x\varphi}$$

Proof Suppose $\Gamma \models \varphi\frac{t}{x}$. If $\mathcal{J} \models \Gamma$, we have $\mathcal{J} \models \varphi\frac{t}{x}$. By the substitution lemma, $\mathcal{J}\frac{\mathcal{J}.t}{x} \models \varphi$ and thus $\mathcal{J} \models \exists x\varphi$. $\square$

∃-Introduction in the Antecedent (∃ A)

$$\frac{\Gamma \quad \varphi\frac{y}{x} \quad \psi}{\Gamma \quad \exists x\varphi \quad \psi} \text{ if } y \text{ is not free in } \Gamma\ \exists x\varphi\ \psi.$$

Proof So, $\Gamma\varphi\frac{y}{x} \models \psi$. Suppose $\mathcal{J} \models \Gamma$ and $\mathcal{J} \models \exists x\varphi$. Then there is an a such that $\mathcal{J}\frac{a}{x} \models \varphi$, but by the coincidence lemma, $(\mathcal{J}\frac{a}{y})\frac{a}{x} \models \varphi$. Since $\mathcal{J}\frac{a}{y}(y) = a$, we have $(\mathcal{J}\frac{a}{y})\frac{\mathcal{J}\frac{a}{y}(y)}{x} \models \varphi$ and by substitution lemma $\mathcal{J}\frac{a}{y} \models \varphi\frac{y}{x}$. Since $\mathcal{J} \models \Gamma$ and $y \notin \text{free}.\Gamma$, we get $\mathcal{J}\frac{a}{y} \models \Gamma$. Now, we get $\mathcal{J}\frac{a}{y} \models \psi$ and therefore $\mathcal{J} \models \psi$ because $y \notin \text{free}.\psi$. $\square$

Gödel's Completeness Part 1

- For all Φ and ϕ, $\Phi \vdash \phi$ iff there is a finite $\Phi_0 \subseteq \Phi$ s.t. $\Phi_0 \vdash \phi$
  - Directly from definition of derivable
- Easy part of Gödel's completeness theorem
  - $\Phi \vdash \phi$ implies $\Phi \models \phi$
  - By induction on structure of derivations, using the correctness of sequent rules

Consistency

- Φ is *consistent*, Con Φ, iff there is no formula ϕ s.t. $\Phi \vdash \phi$ and $\Phi \vdash \neg\phi$
- Φ is *inconsistent*, Inc Φ, iff Φ is not consistent: $\exists\ \phi$ s.t. $\Phi \vdash \phi$ and $\Phi \vdash \neg\phi$
- Inc Φ iff for all ϕ, $\Phi \vdash \phi$
- Con Φ iff there is some ϕ s.t. not $\Phi \vdash \phi$
- For all Φ, Con Φ iff Con Φ_0 for all finite subsets Φ_0 of Φ
- Sat Φ implies Con Φ
  - Inc $\Phi \Rightarrow \Phi \vdash \phi$ and $\Phi \vdash \neg\phi \Rightarrow \Phi \vDash \phi$ and $\Phi \vDash \neg\phi \Rightarrow$ not Sat Φ
- For all Φ and ϕ the following holds
  - $\Phi \vdash \phi$ iff Inc $\Phi \cup \{\neg\phi\}$
  - $\Phi \vdash \neg\phi$ iff Inc $\Phi \cup \{\phi\}$
  - If Con Φ, then Con $\Phi \cup \{\phi\}$ or Con $\Phi \cup \{\neg\phi\}$

Useful Lemma

For all $i \in \omega$, let S_i be a symbol set s.t. $S_i \subseteq S_{i+1}$ and let Φ_i be a set of S_i-formulae s.t. $\mathrm{Con}_{S_i}\ \Phi_i$ and $\Phi_i \subseteq \Phi_{i+1}$. Let $S = \bigcup_{i\in\omega} S_i$ and $\Phi = \bigcup_{i\in\omega} \Phi_i$.

Then $\mathrm{Con}_S\ \Phi$

Proof:

$\mathrm{Inc}_S\ \Phi$

$\Rightarrow$ { $\mathrm{Inc}_S\ \Psi$ for finite Ψ s.t. $\Psi \subseteq \Phi$, thus $\Psi \subseteq \Phi_k$ for some k }

$\mathrm{Inc}_S\ \Phi_k$

$\Rightarrow$ {Any derivation of ϕ, $\neg\phi$ is finite so all symbols are in S_m for some $m \geq k$ }

$\mathrm{Inc}_{S_m}\ \Phi_m$

Gödel's Completeness Part 2

- Gödel's completeness theorem, part 2: $\Phi \vDash \phi$ implies $\Phi \vdash \phi$
- Lemma: Con Φ implies Sat Φ
- Proof: $\Phi \vDash \phi$

  iff {previous lemma} not Sat $(\Phi \cup \{\neg\phi\})$

  iff {above lemma, soundness} not Con $(\Phi \cup \{\neg\phi\})$

  iff {hint: use Contradiction Rule} $\Phi \vdash \phi$

Contradiction Rule (Ctr)

$$\begin{array}{lll} \Gamma & \neg\varphi & \psi \\ \Gamma & \neg\varphi & \neg\psi \\ \hline \Gamma & & \varphi \end{array}$$

Henkin's Theorem

- The insight: if Con Φ, just reflect the syntax into the semantics
- $\mathscr{I} = \langle T^S, \mathfrak{a}, \beta \rangle$ (so the universe is the set of terms)
  - $\beta(v_i) = v_i$
  - $\mathfrak{a}.c = c$, $\mathfrak{a}.f(t) = ft$
- This doesn't work! $\mathscr{I}(v_0) \neq \mathscr{I}(v_1)$, but what if $v_0 \equiv v_1 \in \Phi$?
- The plan is to fix this and a number of other problems until it works!
- First idea: use equivalence classes of terms, so that provably equivalent terms are in the same class, so v_0 and v_1 will be equal under $\mathscr{I}$ because they are in the same equivalence class

Term Structure

Define the equivalence relation on T^S

$t_1 \sim t_2$ iff $\Phi \vdash t_1 \equiv t_2$

1. $\sim$ is an equivalence relation.

2. If $t_1 \sim t'_1, \ldots, t_n \sim t'_n$ then for n-ary $f \in S$: $ft_1 \ldots t_n \sim ft'_1 \ldots t'_n$ and for n-ary $R \in S$: $\Phi \vdash Rt_1 \ldots t_n$ iff $\Phi \vdash Rt'_1 \ldots t'_n$.

Let $\bar{t} = \{t' \in T^S : t \sim t'\}$, *i.e.*, $\bar{t}$ is the equivalence class of t.

Let T^Φ be the set of equivalence classes: $T^\Phi = \{\bar{t} : t \in T^S\}$. Note that T^Φ is not empty. We now define the term structure over T^Φ, $\mathcal{T}^\Phi$ as follows.

1. $c^{\mathcal{T}^\Phi} = \bar{c}$

2. $f^{\mathcal{T}^\Phi}(\overline{t_1}, \ldots, \overline{t_n}) = \overline{ft_1 \ldots t_n}$

3. $R^{\mathcal{T}^\Phi}\overline{t_1} \ldots \overline{t_n}$ iff $\Phi \vdash Rt_1 \ldots t_n$

Term Interpretation

We define the *term interpretation* associated with Φ to be $\mathcal{J}^{\Phi} = \langle \mathcal{T}^{\Phi}, \beta^{\Phi} \rangle$, where $\beta^{\Phi}(x) = \overline{x}$.

1. *For all* t, $\mathcal{J}^{\Phi}(t) = \overline{t}$.
2. *For every atomic formula* φ, $\mathcal{J}^{\Phi} \models \varphi$ *iff* $\Phi \vdash \varphi$.
3. *For every formula* φ *and pairwise disjoint variables* $x_1, \ldots, x_n$
   (a) $\mathcal{J}^{\varphi} \models \exists x_1 \ldots \exists x_n \varphi$ *iff there are* $t_1, \ldots, t_n \in T^S$ *s.t.* $\mathcal{J}^{\Phi} \models \varphi \frac{t_1 \ldots t_n}{x_1 \ldots x_n}$.
   (b) $\mathcal{J}^{\varphi} \models \forall x_1 \ldots \forall x_n \varphi$ *iff for all* $t_1, \ldots, t_n \in T^S$ *we have* $\mathcal{J}^{\Phi} \models \varphi \frac{t_1 \ldots t_n}{x_1 \ldots x_n}$.

More Problems

Where are we? Well, by the previous lemma $\mathfrak{J}^\Phi$ is a model of the atomic formulas in Φ, but we do not know that it is a model of all formulas in Φ. In fact, it isn't. Consider $\Phi = \{\exists x Rx\}$. Then, by (3) of the previous lemma, $\mathfrak{J}^\Phi \models \Phi$ iff there is a term (in our case a variable) y such that $\exists x Rx \vdash Ry$, but this does not hold, as one of the exercises requires you to show. Consider $\Phi \cup \{\neg Ry : y$ is a variable $\}$. This set is satisfiable, thus consistent, but for no term $t \in T^S$ do we have $\Phi \vdash Rt$.

1. *For all t, $\mathfrak{J}^\Phi(t) = \bar{t}$.*
2. *For every atomic formula φ, $\mathfrak{J}^\Phi \models \varphi$ iff $\Phi \vdash \varphi$.*
3. *For every formula φ and pairwise disjoint variables $x_1, \ldots, x_n$*
   (a) *$\mathfrak{J}^\varphi \models \exists x_1 \ldots \exists x_n \varphi$ iff there are $t_1, \ldots, t_n \in T^S$ s.t. $\mathfrak{J}^\Phi \models \varphi \frac{t_1 \ldots t_n}{x_1 \ldots x_n}$.*
   (b) *$\mathfrak{J}^\varphi \models \forall x_1 \ldots \forall x_n \varphi$ iff for all $t_1, \ldots, t_n \in T^S$ we have $\mathfrak{J}^\Phi \models \varphi \frac{t_1 \ldots t_n}{x_1 \ldots x_n}$.*

Closure Conditions

Φ is *negation complete* iff for every formula φ, $\Phi \vdash \varphi$ or $\Phi \vdash \neg\varphi$.

Φ *contains witnesses* iff for every formula of the form $\exists x\varphi$, there is a term t such that $\Phi \vdash (\exists x\varphi \to \varphi\frac{t}{x})$.

Lemma 21 *If Φ is consistent, negation complete, and contains witnesses, then for all φ and ψ.*

1. $\Phi \vdash \neg\varphi$ *iff not* $\Phi \vdash \varphi$
2. $\Phi \vdash (\varphi \vee \psi)$ *iff* $\Phi \vdash \varphi$ *or* $\Phi \vdash \psi$
3. $\Phi \vdash \exists x\varphi$ *iff there is a term t s.t.* $\Phi \vdash \varphi\frac{t}{x}$

Henkin's Theorem

If Φ is consistent, negation complete, and contains witnesses, then $\mathcal{J}^{\Phi} \models \Phi$

We now show that any consistent set of formulas can be extended to one that is consistent, negation complete, and contains witnesses. Then, from Henkin's theorem we get the completeness theorem.

we assume that $|S| \leq \omega$.

Completeness Theorem

Theorem 4 *Let $\Phi \subseteq L^S$ be a consistent set of formulas and let $|free(\Phi)| < \omega$. Then, Φ is satisfiable.*

Proof

$$\text{Con } \Phi \wedge \Phi \subseteq L^S \wedge |\text{free}(\Phi)| < \omega$$

$$\Rightarrow \quad \{ \text{ Lemma 23 } \}$$

$$\exists \Psi \text{ s.t. Con } \Psi \wedge \Phi \subseteq \Psi \subseteq L^S \wedge \Psi \text{ contains witnesses}$$

$$\Rightarrow \quad \{ \text{ Lemma 22 } \}$$

$$\exists \Theta \text{ s.t. Con } \Theta \wedge \Psi \subseteq \Theta \subseteq L^S \wedge \Theta \text{ contains witnesses and is negation complete}$$

$$\Rightarrow \quad \{ \text{ Henkin's Theorem } \}$$

$$\mathcal{J}^\Theta \text{ is a model of } \Theta, \Psi, \text{ and } \Phi$$

$$\Rightarrow \quad \{ \text{ Definition of Sat } \}$$

$$\text{Sat } \Phi \ \square$$

Negation Completeness

Lemma 22 *Let $\Psi \subseteq L^S$, Con Ψ. Then there exists Θ s.t. Con Θ, $\Psi \subseteq \Theta \subseteq L^S$, and Θ is negation complete.*

Proof Enumerate L^S: $\varphi_0, \varphi_1, \varphi_2, \ldots$. Define Θ_n as follows:

$$\Theta_0 = \Psi$$

$$\Theta_{n+1} = \Theta_n \cup \alpha, \text{ where } \alpha = \{\varphi_n\} \text{ if Con } \Theta_n \cup \{\varphi_n\} \text{ and } \alpha = \emptyset \text{ otherwise.}$$

Finally, $\Theta = \bigcup_{i \in \omega} \Theta_n$.

Since for all i, Con Θ_i, by lemma 18, we have Con Θ.

Θ is also negation complete. For every i if $\Theta \nvdash \neg\varphi_i$, then Con $\Theta \cup \{\varphi_i\}$ (lemma 17) so Con $\Theta \cup \{\varphi_i\}$ so $\varphi_i \in \Theta_{n+1} \subseteq \Theta$. $\square$

Witnesses

Lemma 23 *Let* $\Phi \subseteq L^S$, *Con* Φ, $|\mathit{free}(\Phi)| < \omega$. *Then there exists* Ψ *s.t. Con* Ψ, $\Phi \subseteq \Psi \subseteq L^S$, *and* Ψ *contains witnesses.*

Proof Enumerate all $\varphi \in L^S$ beginning with an existential quantifier: $\exists x_0 \varphi_0, \exists x_1 \varphi_1, \ldots$. Now, define ψ_n as follows:

$$\psi_n = (\exists x_n \varphi_n \rightarrow \varphi_n \frac{y_n}{x_n})$$

where y_n is the variable with the smallest index not free in $\Phi_n = \Phi \cup \{\varphi_i \ : 0 \leq i < n\}$. Let $\Psi = \cup_{i \in \omega} \Phi_i$. Now, $\Phi \subseteq \Psi$ and Ψ contains witnesses. If for all $i \in \omega$, Con Φ_i then Con Ψ by lemma 18. Proof by induction.

Gödel's Completeness Theorem

- $\Phi \vdash \phi$ iff $\Phi \models \phi$
- What does this mean for group theory?
- What about new proof techniques?
- Once we show the equivalence between $\vdash \phi$ and $\models$, we can transfer properties of one to the other
  - Compactness theorem:
    (a) $\Phi \models \phi$ iff there is a finite $\Phi_0 \subseteq \Phi$ such that $\Phi_0 \models \phi$
    (b) Sat Φ iff for all finite $\Phi_0 \subseteq \Phi$, Sat Φ_0
- From the proof, we get the Löwenheim-Skolem theorem: Every satisfiable and at most countable set of formulas is satisfiable over a domain which is at most countable