Lecture 20 - First-Order Theories

Vaishnavi Sundararajan

COL703 - Logic for Computer Science

Recap: Natural deduction and intuitionistic logic

- Natural deduction proof system for propositional fragment
- More closely mirrors human reasoning, better for automation
- Negation creates complications!
- Easier if we move to a constructive logic: intuitionistic logic
- No law of excluded middle, actually makes proof search easeir!
- Can “normalize” proofs; every proof has a normal equivalent
- Normal proofs of $\Gamma \vdash \varphi$ only mention subformulas of Γ and φ
- Yields an algorithm for proof search
- Full FO proof search undecidable; set of subformulas is itself infinite!
- Theorem provers use heuristics to get around this as much as possible

Formalizations in FOL

- How much of the world can we talk about using FOL?
- Today we will look at some familiar objects described using FOL
- Recall that we could axiomatize groups using FOL
- The following sentences characterize groups.

$$\forall x.\ [\forall y.\ [\forall z.\ [f(f(x,y),z) \equiv f(x,f(y,z))]]] \tag{G1}$$

$$\forall x.\ [f(x,\varepsilon) \equiv x] \tag{G2}$$

$$\forall x.\ [\exists y.\ [f(x,y) \equiv \varepsilon]] \tag{G3}$$

- $\gamma_{\text{grps}} \coloneqq G1 \wedge G2 \wedge G3$ axiomatizes all groups.
- Any structure $\mathscr{M} = (M, \iota)$ which is a model for $(G1)$–$(G3)$ defines a group over M with group operation f and identity ε

Groups

- In any group, the **cancellation law** holds.
- Consider a group G with operation $\circ$. The cancellation law states that for any $x, y, z \in G$, if $x \circ z = y \circ z$, then $x = y$. Can we state this in FO?

Groups

- In any group, the **cancellation law** holds.
- Consider a group G with operation $\circ$. The cancellation law states that for any $x, y, z \in G$, if $x \circ z = y \circ z$, then $x = y$. Can we state this in FO?

$$\varphi_c \coloneqq \forall x.\ [\forall y.\ [\forall z.\ [f(x,z) \equiv f(y,z) \supset x \equiv y]]]$$

- **Exercise**: Show that $G1, G2, G3 \vdash_{\mathcal{G}} \varphi_c$
- $g \in G$ such that $g \neq 0$ and $\underbrace{g \circ g \circ \ldots \circ g}_{n \text{ times}} = 0$ is said to be of order n
- We will write an interpreted structure as the domain along with the interpreted symbols (here $\Sigma = (\{\varepsilon\}, \{f\}, \emptyset)$ and $\iota(\varepsilon) = 0$ and $\iota(f) = \circ$)
- Is there a ψ such that, if $(G, \circ, 0) \vDash \gamma_{\text{grps}}$ and $(G, \circ, 0) \vDash \psi$, then $(G, \circ, 0)$ is a group with no elements of order 2?

Groups

- In any group, the **cancellation law** holds.
- Consider a group G with operation $\circ$. The cancellation law states that for any $x, y, z \in G$, if $x \circ z = y \circ z$, then $x = y$. Can we state this in FO?

$$\varphi_c \coloneqq \forall x.\ [\forall y.\ [\forall z.\ [f(x,z) \equiv f(y,z) \supset x \equiv y]]]$$

- **Exercise**: Show that $G1, G2, G3 \vdash_{\mathscr{G}} \varphi_c$
- $g \in G$ such that $g \neq 0$ and $\underbrace{g \circ g \circ \ldots \circ g}_{n \text{ times}} = 0$ is said to be of order n
- We will write an interpreted structure as the domain along with the interpreted symbols (here $\Sigma = (\{\varepsilon\}, \{f\}, \emptyset)$ and $\iota(\varepsilon) = 0$ and $\iota(f) = \circ$)
- Is there a ψ such that, if $(G, \circ, 0) \vDash \gamma_{\text{grps}}$ and $(G, \circ, 0) \vDash \psi$, then $(G, \circ, 0)$ is a group with no elements of order 2?

$$\psi \coloneqq \neg\exists x.\ [\neg(x \equiv \varepsilon) \wedge f(x,x) \equiv \varepsilon]$$

Equivalence relations

- An equivalence relation is reflexive, symmetric, and transitive.
- Suppose we have a binary relation symbol $R \in \mathscr{P}$
- Can force R to be interpreted as an equivalence relation by ensuring that any structure satisfies the following sentences

Equivalence relations

- An equivalence relation is reflexive, symmetric, and transitive.
- Suppose we have a binary relation symbol $R \in \mathscr{P}$
- Can force R to be interpreted as an equivalence relation by ensuring that any structure satisfies the following sentences

$$\forall x.\ [R(x,x)] \tag{Eq1}$$

$$\forall x.\ [\forall y.\ [R(x,y) \supset R(y,x)]] \tag{Eq2}$$

$$\forall x.\ [\forall y.\ [\forall z.\ [R(x,y) \land R(y,z) \supset R(x,z)]]] \tag{Eq3}$$

- $\gamma_{\text{eqrel}} \coloneqq Eq1 \land Eq2 \land Eq3$ characterizes all equivalence relations R.
- **Exercise**: What if we wanted R to be interpreted as a congruence?

Equivalence relations (contd.)

- Let $\Sigma = \emptyset, \emptyset, \{R/2\}$
- R is an equivalence relation with at least two equivalence classes

Equivalence relations (contd.)

- Let $\Sigma = \emptyset, \emptyset, \{R/2\}$
- R is an equivalence relation with at least two equivalence classes

$$\gamma_{\text{eqrel}} \wedge \exists x.\ [\exists y.\ [\neg R(x, y)]]$$

- R is an equivalence relation with an equivalence class containing more than one element

Equivalence relations (contd.)

- Let $\Sigma = \emptyset, \emptyset, \{R/2\}$
- R is an equivalence relation with at least two equivalence classes

$$\gamma_{\text{eqrel}} \wedge \exists x.\ [\exists y.\ [\neg R(x,y)]]$$

- R is an equivalence relation with an equivalence class containing more than one element

$$\gamma_{\text{eqrel}} \wedge \exists x.\ [\exists y.\ [\neg(x \equiv y) \wedge R(x,y)]]$$

Orders

- A **total order** over a set is a binary relation $<$ (written in infix) which
  - is irreflexive and transitive, and
  - any two distinct elements in the set are related by $<$
- Can we axiomatize total orders in FOL?

Orders

- A **total order** over a set is a binary relation $<$ (written in infix) which
  - is irreflexive and transitive, and
  - any two distinct elements in the set are related by $<$
- Can we axiomatize total orders in FOL?

$$\forall x.\ [\neg(x < x)] \tag{TO1}$$

$$\forall x.\ [\forall y.\ [\forall z.\ [x < y \land y < z \supset x < z]]] \tag{TO2}$$

$$\forall x.\ [\forall y.\ [x < y \lor x \equiv y \lor y < x]] \tag{TO3}$$

- $\gamma_{\text{to}} \coloneqq TO1 \land TO2 \land TO3$ characterizes all total orders.
- **Exercise**: Axiomatize a partial order $\leqslant$ (Partial orders are reflexive, antisymmetric, and transitive)

Fields

- A field is a structure $(F, \circ, *, 0, 1)$ where $1 \neq 0$ and
  - $(F, \circ, 0)$ is a group where $\circ$ is commutative
  - $*$ is an associative commutative operation over F with identity 1
  - every element other than 0 has a right-inverse wrt $*$
  - $*$ distributes over $\circ$

Fields

- A field is a structure $(F, \circ, *, 0, 1)$ where $1 \neq 0$ and
  - $(F, \circ, 0)$ is a group where $\circ$ is commutative
  - $*$ is an associative commutative operation over F with identity 1
  - every element other than 0 has a right-inverse wrt $*$
  - $*$ distributes over $\circ$
- A field is axiomatized by $\gamma_{\text{flds}} \coloneqq \gamma_{\text{grps}} \wedge$

  $\neg(\varepsilon_\circ \equiv \varepsilon_*) \ \wedge \ \forall x. \ [\forall y. \ [x \circ y \equiv y \circ x]] \ \wedge \ \forall x. \ [\forall y. \ [x * y \equiv y * x]]$

  $\forall x. \ [x * \varepsilon_* \equiv x] \ \wedge \ \forall x. \ [\forall y. \ [\forall z. \ [x * (y * z) \equiv (x * y) * z]]]$

  $\wedge \ \forall x. \ [(x \equiv \varepsilon_\circ) \vee \exists y. \ [x * y \equiv \varepsilon_*]]$

  $\wedge \ \forall x. \ [\forall y. \ [\forall z. \ [x * (y \circ z) \equiv (x * y) \circ (x * z)]]]$

Characterizing sizes of structures

- Recall $\exists x_1.\ [\exists x_2.\ [\ldots \exists x_n.\ [\forall y.\ [y \equiv x_1 \vee y \equiv x_2 \vee \ldots \vee y \equiv x_n]]\ \ldots]]$
- Which structures satisfy this sentence (call it $\varphi_{\leqslant n}$)?
- What about $\exists x.\ [\exists y.\ [\neg(x \equiv y)]]$?

Characterizing sizes of structures

- Recall $\exists x_1.\ [\exists x_2.\ [\ldots \exists x_n.\ [\forall y.\ [y \equiv x_1 \vee y \equiv x_2 \vee \ldots \vee y \equiv x_n]] \ldots]]$
- Which structures satisfy this sentence (call it $\varphi_{\leqslant n}$)?
- What about $\exists x.\ [\exists y.\ [\neg(x \equiv y)]]$?
- All structures with at least two distinct elements. Call this $\varphi_{\geqslant 2}$.
- Can we write a $\varphi_{\geqslant n}$?

Characterizing sizes of structures

- Recall $\exists x_1.\ [\exists x_2.\ [\ldots \exists x_n.\ [\forall y.\ [y \equiv x_1 \vee y \equiv x_2 \vee \ldots \vee y \equiv x_n]] \ldots]]$
- Which structures satisfy this sentence (call it $\varphi_{\leqslant n}$)?
- What about $\exists x.\ [\exists y.\ [\neg(x \equiv y)]]$?
- All structures with at least two distinct elements. Call this $\varphi_{\geqslant 2}$.
- Can we write a $\varphi_{\geqslant n}$?
- $\exists x_1.\ \left[\exists x_2.\ \left[\ldots \exists x_n.\ \left[\bigwedge_{1 \leqslant i < j \leqslant n} \neg(x_i \equiv x_j)\right] \ldots\right]\right]$
- What about $\psi_n = \varphi_{\leqslant n} \wedge \varphi_{\geqslant n}$?
- **Exercise**: Can one specify an infinite structure?

Reals

- Consider the structure $(\mathbb{R}, +, \times, 0)$, where $+$ and $\times$ are interpreted to be addition and multiplication as usual.
- Can we define the relation $<$ in this structure?
- Is there a formula $\varphi(x, y)$ such that for all $a, b \in \mathbb{R}$, $((\mathbb{R}, +, \times, 0), [x \mapsto a, y \mapsto b]) \models \varphi(x, y)$ iff $a < b$?

Reals

- Consider the structure $(\mathbb{R}, +, \times, 0)$, where $+$ and $\times$ are interpreted to be addition and multiplication as usual.
- Can we define the relation $<$ in this structure?
- Is there a formula $\varphi(x, y)$ such that for all $a, b \in \mathbb{R}$, $((\mathbb{R}, +, \times, 0), [x \mapsto a, y \mapsto b]) \models \varphi(x, y)$ iff $a < b$?
- $\varphi(x, y) := \exists z.\ [\neg(z \equiv 0) \land \exists w.\ [z \equiv w \times w] \land x + z \equiv y]$
- We say that $<$ is **elementary definable** in this structure
- An n-ary relation R is said to be elementary definable in a structure $\mathcal{M}$ if there is a formula φ with n parameters such that $\mathcal{M}, [x_1 \mapsto m_1, \ldots, x_n \mapsto m_n] \models \varphi(x_1, \ldots, x_n)$ iff $(m_1, \ldots, m_n) \in R$.

Reals (contd.)

- Consider $(\mathbb{R}, +, 0)$. Is $<$ elementary definable here?

Reals (contd.)

- Consider $(\mathbb{R}, +, 0)$. Is $<$ elementary definable here? **No.**
- Suppose there exists some $\varphi(x, y)$ such that $((\mathbb{R}, +, 0), [x \mapsto a, y \mapsto b]) \vDash \varphi(x, y)$ iff $a < b$. Want a contradiction.
- **Theorem**: If $\mathscr{M}$ and $\mathscr{M}'$ are isomorphic Σ-structures, then for all expressions φ, $\mathscr{M} \vDash \varphi$ iff $\mathscr{M}' \vDash \varphi$.
- Aside: Why the same φ? $\mathscr{M}$ and $\mathscr{M}'$ both Σ-structures, and $\varphi \in \mathsf{FO}_\Sigma$!
- Suppose there is an isomorphism η from $\mathscr{M} = (A, \iota)$ to $\mathscr{M}' = (B, \iota')$. Then, $\eta : A \to B$ and $\eta^{-1} : B \to A$ are both structure-preserving.

$$\left.\begin{aligned} &\eta(\mathsf{f}_A(a_1, \ldots, a_n)) = \mathsf{f}_B(\eta(a_1), \ldots, \eta(a_n)) \\ &\eta^{-1}(\mathsf{f}_B(b_1, \ldots, b_n)) = \mathsf{f}_A\left(\eta^{-1}(b_1), \ldots, \eta^{-1}(b_n)\right) \end{aligned}\right\} \; f \in \mathscr{F}, \iota(f) = \mathsf{f}_A, \iota'(f) = \mathsf{f}_B$$

- Similar statements hold for the relation symbols in $\mathscr{P}$ also.
- One can also show that for every $\sigma : \mathscr{V} \to A$, $\eta \circ \sigma : \mathscr{V} \to B$, and for every $\sigma' : \mathscr{V} \to B$, $\eta^{-1} \circ \sigma' : \mathscr{V} \to A$.

Reals (contd.)

- Suppose there exists some $\varphi(x, y)$ such that $((\mathbb{R}, +, 0), [x \mapsto a, y \mapsto b]) \vDash \varphi(x, y)$ iff $a < b$. Want a contradiction.
- If we can demonstrate a structure $\mathscr{M}'$ isomorphic to $(\mathbb{R}, +, 0)$ (obtained via some isomorphism η) and contradict the iff using $\mathscr{M}'$, we are done.
- Let $\eta(r) = -r$. Is η a structure-preserving isomorphism?

Reals (contd.)

- Suppose there exists some $\varphi(x, y)$ such that $((\mathbb{R}, +, 0), [x \mapsto a, y \mapsto b]) \vDash \varphi(x, y)$ iff $a < b$. Want a contradiction.
- If we can demonstrate a structure $\mathscr{M}'$ isomorphic to $(\mathbb{R}, +, 0)$ (obtained via some isomorphism η) and contradict the iff using $\mathscr{M}'$, we are done.
- Let $\eta(r) = -r$. Is η a structure-preserving isomorphism? Yes!
  - $\eta(0) = 0$ and $\eta(a + b) = -(a + b) = (-a) + (-b) = \eta(a) + \eta(b)$
- So η is an isomorphism from $(\mathbb{R}, +, 0)$ to itself.
- So $(\mathbb{R}, +, 0), \sigma \vDash \varphi(a, b)$ iff $(\mathbb{R}, +, 0), \sigma \vDash \varphi(-a, -b)$
- $(\mathbb{R}, +, 0), \sigma \vDash \varphi(a, b)$ iff $a < b$, and $(\mathbb{R}, +, 0), \sigma \vDash \varphi(-a, -b)$ iff $-a < -b$.
- Contradiction! So $<$ cannot be elementary defined in the theory of reals using $+$ and 0.