

Propositional and Predicate Logic - XII

Petr Gregor

KTIML MFF UK

WS 2024/2025

Hilbert's calculus in predicate logic

- basic connectives and quantifier: \neg , \rightarrow , $(\forall x)$ (others are derived)
- allows to prove any formula (not just sentences)
- **logical axioms** (schemes of axioms):

$$(i) \quad \varphi \rightarrow (\psi \rightarrow \varphi)$$

$$(ii) \quad (\varphi \rightarrow (\psi \rightarrow \chi)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \chi))$$

$$(iii) \quad (\neg\varphi \rightarrow \neg\psi) \rightarrow (\psi \rightarrow \varphi)$$

$$(iv) \quad (\forall x)\varphi \rightarrow \varphi(x/t) \quad \text{if } t \text{ is substitutable for } x \text{ to } \varphi$$

$$(v) \quad (\forall x)(\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow (\forall x)\psi) \quad \text{if } x \text{ is not free in } \varphi$$

where φ, ψ, χ are any formulas (of a given language), t is any term, and x is any variable

- in a language with equality we include also the **axioms of equality**
- **rules of inference**

$$\frac{\varphi, \varphi \rightarrow \psi}{\psi} \quad (\text{modus ponens}), \quad \frac{\varphi}{(\forall x)\varphi} \quad (\text{generalization})$$

Hilbert-style proofs

A **proof** (in *Hilbert-style*) of a formula φ from a theory T is a **finite** sequence $\varphi_0, \dots, \varphi_n = \varphi$ of formulas such that for every $i \leq n$

- φ_i is a logical axiom or $\varphi_i \in T$ (an axiom of the theory), or
- φ_i can be inferred from the previous formulas applying a rule of inference.

A formula φ is **provable** from T if it has a proof from T , denoted by $T \vdash_H \varphi$.

Theorem (soundness) For every theory T and formula φ , $T \vdash_H \varphi \Rightarrow T \models \varphi$.

Proof

- If φ is an axiom (logical or from T), then $T \models \varphi$ (l. axioms are tautologies),
- if $T \models \varphi$ and $T \models \varphi \rightarrow \psi$, then $T \models \psi$, i.e. modus ponens is **sound**,
- if $T \models \varphi$, then $T \models (\forall x)\varphi$, i.e. generalization is **sound**,
- thus every formula in a proof from T is valid in T . \square

Remark The **completeness** holds as well, i.e. $T \models \varphi \Rightarrow T \vdash_H \varphi$.

Theories of structures

What holds in particular structures?

The *theory of a structure* \mathcal{A} is the set $\text{Th}(\mathcal{A})$ of all sentences (of the same language) that are valid in \mathcal{A} .

Observation For every structure \mathcal{A} and a theory T of a language L ,

- (i) $\text{Th}(\mathcal{A})$ is a *complete* theory,
- (ii) if $\mathcal{A} \models T$, then $\text{Th}(\mathcal{A})$ is a simple (complete) *extension* of T ,
- (iii) if $\mathcal{A} \models T$ and T is complete, then $\text{Th}(\mathcal{A})$ is *equivalent* with T ,
i.e. $\theta^L(T) = \text{Th}(\mathcal{A})$.

E.g. $\text{Th}(\underline{\mathbb{N}})$ where $\underline{\mathbb{N}} = \langle \mathbb{N}, S, +, \cdot, 0, \leq \rangle$ is the arithmetics of natural numbers.

Remark Later, we will see that $\text{Th}(\underline{\mathbb{N}})$ is (algorithmically) *undecidable* although it is complete.

Elementary equivalence

- Structures \mathcal{A} and \mathcal{B} of a language L are *elementarily equivalent*, denoted $\mathcal{A} \equiv \mathcal{B}$, if they satisfy the same sentences (of L), i.e. $\text{Th}(\mathcal{A}) = \text{Th}(\mathcal{B})$.

For example, $\langle \mathbb{R}, \leq \rangle \equiv \langle \mathbb{Q}, \leq \rangle$ and $\langle \mathbb{Q}, \leq \rangle \not\equiv \langle \mathbb{Z}, \leq \rangle$ since every element has an immediate successor in $\langle \mathbb{Z}, \leq \rangle$ but not in $\langle \mathbb{Q}, \leq \rangle$.

- T is complete iff it has a single model, up to elementary equivalence.

For example, the theory of dense linear orders without ends (DeLO).

How to describe models of a given theory (up to elementary equivalence)?

Observation For every models \mathcal{A}, \mathcal{B} of a theory T , $\mathcal{A} \equiv \mathcal{B}$ if and only if $\text{Th}(\mathcal{A}), \text{Th}(\mathcal{B})$ are *equivalent* (simple complete extensions of T).

Remark If we can describe *effectively (recursively)* for a given theory T all simple complete extensions of T , then T is (algorithmically) *decidable*.

Simple complete extensions - an example

The theory $DeLO^*$ of dense linear orders of $L = \langle \leq \rangle$ with equality has axioms

$$x \leq x \quad (\text{reflexivity})$$

$$x \leq y \wedge y \leq x \rightarrow x = y \quad (\text{antisymmetry})$$

$$x \leq y \wedge y \leq z \rightarrow x \leq z \quad (\text{transitivity})$$

$$x \leq y \vee y \leq x \quad (\text{dichotomy})$$

$$x < y \rightarrow (\exists z) (x < z \wedge z < y) \quad (\text{density})$$

$$(\exists x)(\exists y)(x \neq y) \quad (\text{nontriviality})$$

where ' $x < y$ ' is a shortcut for ' $x \leq y \wedge x \neq y$ '.

Let φ, ψ be the sentences $(\exists x)(\forall y)(x \leq y)$, resp. $(\exists x)(\forall y)(y \leq x)$. We will see

$$DeLO = DeLO^* \cup \{\neg\varphi, \neg\psi\}, \quad DeLO^\pm = DeLO^* \cup \{\varphi, \psi\},$$

$$DeLO^+ = DeLO^* \cup \{\neg\varphi, \psi\}, \quad DeLO^- = DeLO^* \cup \{\varphi, \neg\psi\}$$

are the all (nonequivalent) simple complete extensions of the theory $DeLO^*$.

Corollary of the Löwenheim-Skolem theorem

We already know the following theorem, by a canonical model (with equality).

Theorem Let T be a consistent theory of a countable language L . If L is without equality, then T has a *countably infinite* model. If L is with equality, then T has a model that is *countable* (finite or countably infinite).

Corollary For every structure \mathcal{A} of a countable language *without equality* there exists a *countably infinite* structure \mathcal{B} with $\mathcal{A} \equiv \mathcal{B}$.

Proof $\text{Th}(\mathcal{A})$ is consistent since it has a model \mathcal{A} . By the previous theorem, it has a countably inf. model \mathcal{B} . Since $\text{Th}(\mathcal{A})$ is complete, we have $\mathcal{A} \equiv \mathcal{B}$. \square

Corollary For every *infinite* structure \mathcal{A} of a countable language *with equality* there exists a *countably infinite* structure \mathcal{B} with $\mathcal{A} \equiv \mathcal{B}$.

Proof Similarly as above. Since the sentence “there is exactly n elements” is false in \mathcal{A} for all n and $\mathcal{A} \equiv \mathcal{B}$, it follows that \mathcal{B} is infinite. \square

A countable algebraically closed field

We say that a field \mathcal{A} is *algebraically closed* if every polynomial (of nonzero degree) has a root in \mathcal{A} ; that is, for every $n \geq 1$ we have

$$\mathcal{A} \models (\forall x_{n-1}) \dots (\forall x_0) (\exists y) (y^n + x_{n-1} \cdot y^{n-1} + \dots + x_1 \cdot y + x_0 = 0)$$

where y^k is a shortcut for the term $y \cdot y \cdot \dots \cdot y$ (\cdot applied $(k - 1)$ -times).

For example, the field $\mathbb{C} = \langle \mathbb{C}, +, -, \cdot, 0, 1 \rangle$ is algebraically closed, whereas the fields \mathbb{R} and \mathbb{Q} are not (since the polynomial $x^2 + 1$ has no root in them).

Corollary *There exists a countable algebraically closed field.*

Proof By the previous corollary, there is a countable structure elementarily equivalent with the field \mathbb{C} . Hence it is algebraically closed as well. \square

Isomorphisms of structures

Let \mathcal{A} and \mathcal{B} be structures of a language $L = \langle \mathcal{F}, \mathcal{R} \rangle$.

- A **bijection** $h: A \rightarrow B$ is an **isomorphism** of structures \mathcal{A} and \mathcal{B} if both
 - $h(f^{\mathcal{A}}(a_1, \dots, a_n)) = f^{\mathcal{B}}(h(a_1), \dots, h(a_n))$
for every n -ary function symbol $f \in \mathcal{F}$ and every $a_1, \dots, a_n \in A$,
 - $R^{\mathcal{A}}(a_1, \dots, a_n) \Leftrightarrow R^{\mathcal{B}}(h(a_1), \dots, h(a_n))$
for every n -ary relation symbol $R \in \mathcal{R}$ and every $a_1, \dots, a_n \in A$.
- \mathcal{A} and \mathcal{B} are **isomorphic** (via h), denoted $\mathcal{A} \simeq \mathcal{B}$ ($\mathcal{A} \simeq_h \mathcal{B}$), if there is an isomorphism h of \mathcal{A} and \mathcal{B} . We also say that \mathcal{A} is **isomorphic with** \mathcal{B} .
- An **automorphism** of a structure \mathcal{A} is an isomorphism of \mathcal{A} with \mathcal{A} .

For example, the power set algebra $\underline{\mathcal{P}(X)} = \langle \mathcal{P}(X), -, \cap, \cup, \emptyset, X \rangle$ with $|X| = n$ is isomorphic to the Boolean algebra $\langle \{0, 1\}^n, -_n, \wedge_n, \vee_n, 0_n, 1_n \rangle$ via $h: A \mapsto \chi_A$ where χ_A is the characteristic function of the set $A \subseteq X$.

Isomorphisms and semantics

We will see that isomorphism preserves semantics.

Proposition Let \mathcal{A} and \mathcal{B} be structures of a language $L = \langle \mathcal{F}, \mathcal{R} \rangle$. A bijection $h: A \rightarrow B$ is an *isomorphism* of \mathcal{A} and \mathcal{B} if and only if both

- (i) $h(t^{\mathcal{A}}[e]) = t^{\mathcal{B}}[e \circ h]$ for every term t and $e: \text{Var} \rightarrow A$, and
- (ii) $\mathcal{A} \models \varphi[e] \Leftrightarrow \mathcal{B} \models \varphi[e \circ h]$ for every formula φ and $e: \text{Var} \rightarrow A$.

Proof (\Rightarrow) By induction on the structure of the term t , resp. the formula φ .

(\Leftarrow) By applying (i) for each term $f(x_1, \dots, x_n)$ or (ii) for each atomic formula $R(x_1, \dots, x_n)$ and assigning $e(x_i) = a_i$ we verify that h is an isomorphism. \square

Corollary For every structures \mathcal{A} and \mathcal{B} of the same language,

$$\mathcal{A} \simeq \mathcal{B} \Rightarrow \mathcal{A} \equiv \mathcal{B}.$$

Remark The other implication (\Leftarrow) does not hold in general. For example, $\langle \mathbb{Q}, \leq \rangle \equiv \langle \mathbb{R}, \leq \rangle$ but $\langle \mathbb{Q}, \leq \rangle \not\equiv \langle \mathbb{R}, \leq \rangle$ since $|\mathbb{Q}| = \omega$ and $|\mathbb{R}| = 2^\omega$.

Definability and automorphisms

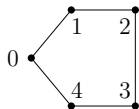
We show that definable sets are invariant under automorphisms.

Proposition Let $D \subseteq A^n$ be a set definable in a structure \mathcal{A} from parameters \bar{b} and h be an *automorphism* of \mathcal{A} that pointwise preserves \bar{b} . Then $h[D] = D$.

Proof Let $D = \varphi^{A, \bar{b}}(\bar{x}, \bar{y})$. Then for every $\bar{a} \in A^{|\bar{x}|}$

$$\begin{aligned} \bar{a} \in D &\Leftrightarrow \mathcal{A} \models \varphi[e(\bar{x}/\bar{a}, \bar{y}/\bar{b})] \Leftrightarrow \mathcal{A} \models \varphi[(e \circ h)(\bar{x}/\bar{a}, \bar{y}/\bar{b})] \\ &\Leftrightarrow \mathcal{A} \models \varphi[e(\bar{x}/h(\bar{a}), \bar{y}/h(\bar{b}))] \Leftrightarrow \mathcal{A} \models \varphi[e(\bar{x}/h(\bar{a}), \bar{y}/\bar{b})] \Leftrightarrow h(\bar{a}) \in D. \end{aligned}$$

Ex.: the graph \mathcal{G} has exactly one nontrivial automorphism h that preserves 0.



$$h(0) = 0, \quad h(1) = 4, \quad h(2) = 3, \quad h(3) = 2, \quad h(4) = 1$$

$$\{0\} = (x = y)^{\mathcal{G}, 0}, \quad \{1, 4\} = (E(x, y))^{\mathcal{G}, 0}, \quad \{2, 3\} = (x \neq y \wedge \neg E(x, y))^{\mathcal{G}, 0}$$

Moreover, the sets $\{0\}$, $\{1, 4\}$, $\{2, 3\}$ are definable with parameter 0. Thus

$$\text{Df}^1(\mathcal{G}, \{0\}) = \{\emptyset, \{0\}, \{1, 4\}, \{2, 3\}, \{0, 1, 4\}, \{0, 2, 3\}, \{1, 4, 2, 3\}, \{0, 1, 2, 3, 4\}\}.$$

Finite models in language with equality

Proposition For every *finite* structures \mathcal{A}, \mathcal{B} of a language with *equality*,

$$\mathcal{A} \equiv \mathcal{B} \Rightarrow \mathcal{A} \simeq \mathcal{B}.$$

Proof It holds $|A| = |B|$ since we can express “there are exactly n elements”.

- Let \mathcal{A}' be expansion of \mathcal{A} to $L' = L \cup \{c_a\}_{a \in A}$ by **names of elements** of A .
- We show that \mathcal{B} has an expansion \mathcal{B}' to L' such that $\mathcal{A}' \equiv \mathcal{B}'$. Then clearly $h: a \mapsto c_a^{B'}$ is an isomorphism of \mathcal{A}' to \mathcal{B}' , and thus also of \mathcal{A} to \mathcal{B} .
- It suffices to find $b \in B$ for every $c_a^{A'} = a \in A$ such that $\langle \mathcal{A}, a \rangle \equiv \langle \mathcal{B}, b \rangle$.
- Let Ω be set of all formulas $\varphi(x)$ s.t. $\langle \mathcal{A}, a \rangle \models \varphi(x/c_a)$, i.e. $\mathcal{A} \models \varphi[e(x/a)]$.
- Since A is finite, there are finitely many formulas $\varphi_0(x), \dots, \varphi_m(x)$ such that for every $\varphi \in \Omega$ it holds $\mathcal{A} \models \varphi \leftrightarrow \varphi_i$ for some i .
- Since $\mathcal{B} \equiv \mathcal{A} \models (\exists x) \bigwedge_{i \leq m} \varphi_i$, there exists $b \in B$ s.t. $\mathcal{B} \models \bigwedge_{i \leq m} \varphi_i[e(x/b)]$.
- Hence for every $\varphi \in \Omega$ it holds $\mathcal{B} \models \varphi[e(x/b)]$, i.e. $\langle \mathcal{B}, b \rangle \models \varphi(x/c_a)$. \square

Corollary If a *complete* theory T in a language with equality has a *finite* model, then all models of T are *isomorphic*.

Categoricity

- An (isomorphism) *spectrum* of a theory T is given by the number $I(\kappa, T)$ of mutually nonisomorphic models of T for every **cardinality** κ .
- A theory T is *κ -categorical* if it has exactly one (up to isomorphism) model of cardinality κ , i.e. $I(\kappa, T) = 1$.

Proposition *The theory DeLO (i.e. “without ends”) is ω -categorical.*

Proof Let $\mathcal{A}, \mathcal{B} \models \text{DeLO}$ with $A = \{a_i\}_{i \in \mathbb{N}}$, $B = \{b_i\}_{i \in \mathbb{N}}$. By induction on n we can find injective **partial** functions $h_n \subseteq h_{n+1} \subset A \times B$ **preserving the ordering** s.t. $\{a_i\}_{i < n} \subseteq \text{dom}(h_n)$ and $\{b_i\}_{i < n} \subseteq \text{rng}(h_n)$. Then $\mathcal{A} \simeq \mathcal{B}$ via $h = \cup h_n$. \square

Similarly we obtain that (e.g.) $\mathcal{A} = \langle \mathbb{Q}, \leq \rangle$, $\mathcal{A} \upharpoonright (0, 1]$, $\mathcal{A} \upharpoonright [0, 1)$, $\mathcal{A} \upharpoonright [0, 1]$ are (up to isomorphism) all countable models of DeLO. Then*

$$I(\kappa, \text{DeLO}^*) = \begin{cases} 0 & \text{for } \kappa \in \mathbb{N}, \\ 4 & \text{for } \kappa = \omega. \end{cases}$$

ω -categorical criterium of completeness

Theorem *Let L be at most countable language.*

- (i) If a theory T in L without equality is ω -categorical, then it is complete.*
- (ii) If a theory T in L with equality is ω -categorical and without finite models, then it is complete.*

Proof Every model of T is elementarily equivalent with some countably infinite model of T , but such model is unique up to isomorphism. Thus all models of T are elementarily equivalent, i.e. T is complete. \square

For example, $DeLO$, $DeLO^+$, $DeLO^-$, $DeLO^\pm$ are complete and they are the all (mutually nonequivalent) simple complete extensions of $DeLO^$.*

Remark *A similar criterium holds also for cardinalities bigger than ω .*

Axiomatizability

We are interested if we can describe a class of models by given means.

Let $K \subseteq M(L)$ be a class of structures of a language L . We say that K is

- **axiomatizable** if there is a theory T of language L with $M(T) = K$,
- **finitely axiomatizable** if K is axiomatizable by a **finite** theory,
- **openly axiomatizable** if K is axiomatizable by an **open** theory,
- a **theory** T if **finitely (openly) axiomatizable** if T is equivalent to a finite (resp. open) theory.

Observation *If K is axiomatizable, then it is closed under elem. equivalence.*

For example,

- linear orderings are both finitely and openly axiomatizable,*
- fields are finitely axiomatizable, but not openly,*
- infinite groups are axiomatizable, but not finitely.*

Application of compactness

Theorem *If a theory T has at least an n -element model for every $n \in \mathbb{N}$, then it also has an infinite model.*

Proof In a language without equality apply L.-S. theorem. Now assume we have a language with equality.

- Let $T' = T \cup \{c_i \neq c_j \mid \text{for } i \neq j\}$ be an extension of T in a language with additional countably infinitely many new constant symbols c_i .
- By the assumption, every finite part of T' has a model.
- By **compactness**, T' has a model, which clearly is infinite.
- Its reduct to the original language is an infinite model of T . \square

Corollary *If a theory T has at least an n -element model for each $n \in \mathbb{N}$, the class of all its finite models is not axiomatizable.*

For example, finite groups, finite fields, etc. are not axiomatizable. But infinite models of a theory T in language with equality are axiomatizable.

Finite axiomatizability

Theorem Let $K \subseteq M(L)$ and $\bar{K} = M(L) \setminus K$ where L is a language. Then K is *finitely axiomatizable* if and only if both K and \bar{K} are axiomatizable.

Proof (\Rightarrow) If T is a finite axiomatization of K is a **closed** form, then the theory with the only axiom $\bigvee_{\varphi \in T} \neg \varphi$ axiomatizes \bar{K} . Now we show (\Leftarrow).

- Let T, S be theories of language L such that $M(T) = K, M(S) = \bar{K}$.
- Then $M(T \cup S) = M(T) \cap M(S) = \emptyset$ and by the **compactness** there exist finite $T' \subseteq T$ and $S' \subseteq S$ such that $\emptyset = M(T' \cup S') = M(T') \cap M(S')$.
- Since

$$M(T) \subseteq M(T') \subseteq \overline{M(S')} \subseteq \overline{M(S)} = M(T),$$

we have $M(T) = M(T')$, i.e. a finite T' axiomatizes K . \square

Finite axiomatizability - example

Let T be the theory of fields. We say that a field $\mathcal{A} = \langle A, +, -, \cdot, 0, 1 \rangle$ has

- **characteristic 0** if there is no $p \in \mathbb{N}^+$ such that $\mathcal{A} \models p\mathbf{1} = \mathbf{0}$,
where $p\mathbf{1}$ denotes the term $1 + 1 + \dots + 1$ (+ applied $(p - 1)$ -times).
- **characteristic p** where p is prime, if p is the smallest s.t. $\mathcal{A} \models p\mathbf{1} = \mathbf{0}$.
- The class of fields of characteristic p for prime p is **finitely** axiomatized by the theory $T \cup \{p\mathbf{1} = \mathbf{0}\}$.
- The class K of fields of characteristic 0 is axiomatized by the (**infinite**) theory $T' = T \cup \{p\mathbf{1} \neq \mathbf{0} \mid p \in \mathbb{N}^+\}$.

Proposition K is not **finitely** axiomatizable.

Proof It suffices to show that \overline{K} is not axiomatizable. Suppose $M(S) = \overline{K}$. Then $S' = S \cup T'$ has a model \mathcal{B} since every finite $S^* \subseteq S'$ has a model (a field of prime characteristic larger than any p occurring in axioms of S^*), But then $\mathcal{B} \in M(S) = \overline{K}$ and $\mathcal{B} \in M(T') = K$, a contradiction. \square

Openly axiomatizable theories

Theorem *If a theory T is openly axiomatizable, then every substructure of a model of T is also a model of T .*

Proof Let T' be open axiomatization of $M(T)$, $\mathcal{A} \models T'$ and $\mathcal{B} \subseteq \mathcal{A}$. We know that $\mathcal{B} \models \varphi$ for every $\varphi \in T'$ since φ is open. Thus \mathcal{B} is a model of T' . \square

Remark *The other implication holds as well, i.e. if every substructure of every model of T is also a model of T , then T is openly axiomatizable.*

For example, the theory DeLO is not openly axiomatizable since e.g. any finite substructure of a model of DeLO is not a model DeLO.

At most n -element groups for a fixed $n > 1$ are openly axiomatized by

$$T \cup \left\{ \bigvee_{\substack{i,j \leq n \\ i \neq j}} x_i = x_j \right\},$$

where T is the (open) theory of groups.