# Propositional and Predicate Logic - XI

Petr Gregor

KTIML MFF UK

WS 2015/2016

# Basic algebraic theories

- theory of *groups* in the language $L = \langle +, -, 0 \rangle$ with equality has axioms

$$x + (y + z) = (x + y) + z \qquad \text{(associativity of } +\text{)}$$
$$0 + x = x = x + 0 \qquad \text{(0 is neutral to } +\text{)}$$
$$x + (-x) = 0 = (-x) + x \qquad (-x \text{ is inverse of } x)$$

- theory of *Abelian groups* has moreover ax. $x + y = y + x$ (commutativity)
- theory of *rings* in $L = \langle +, -, \cdot, 0, 1 \rangle$ with equality has moreover axioms

$$1 \cdot x = x = x \cdot 1 \qquad \text{(1 is neutral to } \cdot\text{)}$$
$$x \cdot (y \cdot z) = (x \cdot y) \cdot z \qquad \text{(associativity of } \cdot\text{)}$$
$$x \cdot (y + z) = x \cdot y + x \cdot z,\ (x + y) \cdot z = x \cdot z + y \cdot z \qquad \text{(distributivity)}$$

- theory of *commutative rings* has moreover ax. $x \cdot y = y \cdot x$ (commutativity)
- theory of *fields* in the same language has additional axioms

$$x \neq 0 \rightarrow (\exists y)(x \cdot y = 1) \qquad \text{(existence of inverses to } \cdot\text{)}$$
$$0 \neq 1 \qquad \text{(nontriviality)}$$

# Theories of structures

*What holds in particular structures?*

The *theory of a structure* $\mathcal{A}$ is the set $\mathrm{Th}(\mathcal{A})$ 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 $L$,*

$(i)$ $\mathrm{Th}(\mathcal{A})$ *is a complete theory,*

$(ii)$ *if $\mathcal{A} \models T$, then $\mathrm{Th}(\mathcal{A})$ is a simple (complete) extension of $T$,*

$(iii)$ *if $\mathcal{A} \models T$ and $T$ is complete, then $\mathrm{Th}(\mathcal{A})$ is equivalent with $T$, i.e. $\theta^L(T) = \mathrm{Th}(\mathcal{A})$.*

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

Remark *Later, we will see that $\mathrm{Th}(\underline{\mathbb{N}})$ 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. $\mathrm{Th}(\mathcal{A}) = \mathrm{Th}(\mathcal{B})$.

  *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 $\mathrm{Th}(\mathcal{A})$, $\mathrm{Th}(\mathcal{B})$ 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

$$x \leq x \qquad \text{(reflexivity)}$$
$$x \leq y \ \wedge \ y \leq x \ \rightarrow \ x = y \qquad \text{(antisymmetry)}$$
$$x \leq y \ \wedge \ y \leq z \ \rightarrow \ x \leq z \qquad \text{(transitivity)}$$
$$x \leq y \ \vee \ y \leq x \qquad \text{(dichotomy)}$$
$$x < y \ \rightarrow \ (\exists z)\,(x < z \ \wedge \ z < y) \qquad \text{(density)}$$
$$(\exists x)(\exists y)(x \neq y) \qquad \text{(nontriviality)}$$

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

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

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

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

# Corollary of the theorem on countable models

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

**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 $B$ is infinite. □

# 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

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

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

*For example, the field $\underline{\mathbb{C}} = \langle \mathbb{C}, +, -, \cdot, 0, 1 \rangle$ is algebraically closed, whereas the fields $\underline{\mathbb{R}}$ and $\underline{\mathbb{Q}}$ 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 $\underline{\mathbb{C}}$. Hence it is algebraically closed as well. □

# Isomorphisms of structures

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

- A bijection $h\colon A \to B$ is an *isomorphism* of structures $\mathcal{A}$ and $\mathcal{B}$ if both
  - $(i)$ $h(f^A(a_1, \ldots, a_n)) = f^B(h(a_1), \ldots, h(a_n))$
    for every $n$-ary function symbol $f \in \mathcal{F}$ and every $a_1, \ldots, a_n \in A$,
  - $(ii)$ $R^A(a_1, \ldots, a_n) \Leftrightarrow R^B(h(a_1), \ldots, h(a_n))$
    for every $n$-ary relation symbol $R \in \mathcal{R}$ and every $a_1, \ldots, a_n \in A$.
- $\mathcal{A}$ 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 $\underline{{}^n2} = \langle {}^n2, -_n, \wedge_n, \vee_n, 0_n, 1_n \rangle$ via $h : A \mapsto \chi_A$ where $\chi_A$ 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 $h\colon A \to B$ is an isomorphism of $\mathcal{A}$ and $\mathcal{B}$ if and only if both*

$(i)$ $h(t^A[e]) = t^B[he]$ *for every term $t$ and $e\colon \mathrm{Var} \to A$,*

$(ii)$ $\mathcal{A} \models \varphi[e] \;\Leftrightarrow\; \mathcal{B} \models \varphi[he]$ *for every formula $\varphi$ and $e\colon \mathrm{Var} \to A$.*

*Proof* $(\Rightarrow)$ By induction on the structure of the term $t$, resp. the formula $\varphi$.
$(\Leftarrow)$ By applying $(i)$ for each term $f(x_1, \ldots, x_n)$ or $(ii)$ for each atomic formula $R(x_1, \ldots, x_n)$ 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 $\langle \mathbb{Q}, \leq \rangle \not\simeq \langle \mathbb{R}, \leq \rangle$ since $|\mathbb{Q}| = \omega$ and $|\mathbb{R}| = 2^\omega$.*

# Finite models in language with equality

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

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

*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 $h\colon a \mapsto c_a^{B'}$ is an isomorfism of $\mathcal{A}'$ to $\mathcal{B}'$, and thus also of $\mathcal{A}$ to $\mathcal{B}$.
- If 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 $\Omega$ 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 $\varphi_0(x), \ldots, \varphi_m(x)$ 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 $\kappa$.
- A theory $T$ is *$\kappa$-categorical* if it has exactly one (up to isomorphism) model of cardinality $\kappa$, i.e. $I(\kappa, T) = 1$.

**Proposition** *The theory $DeLO$ (i.e. "without ends") is $\omega$-categorical.*

*Proof* Let $\mathcal{A}, \mathcal{B} \models DeLO$ 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. $\{a_i\}_{i<n} \subseteq \mathrm{dom}(h_n)$ and $\{b_i\}_{i<n} \subseteq \mathrm{rng}(h_n)$. Then $\mathcal{A} \simeq \mathcal{B}$ via $h = \cup h_n$. $\square$

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

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

# $\omega$-categorical criterium of completeness

**Theorem** *Let $L$ be at most countable language.*

$(i)$ *If a theory $T$ in $L$ without equality is $\omega$-categorical, then it is complete.*

$(ii)$ *If a theory $T$ in $L$ with equality is $\omega$-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, $\mathrm{DeLO}$, $\mathrm{DeLO}^+$, $\mathrm{DeLO}^-$, $\mathrm{DeLO}^\pm$ are complete and they are the all (mutually nonequivalent) simple complete extensions of $\mathrm{DeLO}^*$.*

*Remark* *A similar criterium holds also for cardinalities bigger than $\omega$.*

# Recursive and recursively enumerable sets

*Which problems are algorithmically solvable?*

- The notion of *"algorithm"* can be rigorously formalized (e.g. by TM).
- We may encode decision problems into sets of natural numbers corresponding to the positive instances (with answer $\mathtt{yes}$). For example,
$$SAT = \{\lceil\varphi\rceil \mid \varphi \text{ is a satisfiable proposition in CNF}\}.$$
- A set $A \subseteq \mathbb{N}$ is *recursive* if there is an algorithm that for every input $x \in \mathbb{N}$ halts and correctly tells whether or not $x \in A$. We say that such algorithm decides $x \in A$.
- A set $A \subseteq \mathbb{N}$ is *recursively enumerable* (*r. e.*) if there is an algorithm that for every input $x \in \mathbb{N}$ halts if and only if $x \in A$. We say that such algorithm recognizes $x \in A$. Equivalently, $A$ is recursively enumerable if there is an algorithm that generates (i.e. *enumerates*) all elements of $A$.

**Observation** *For every $A \subseteq \mathbb{N}$ it holds that $A$ is recursive $\Leftrightarrow$ $A$, $\overline{A}$ are r. e.*

# Decidable theories

*Is the truth in a given theory algorithmically decidable?*

We (always) assume that the language $L$ is recursive. A theory $T$ of $L$ is *decidable* if $\mathit{Thm}(T)$ is recursive; otherwise, $T$ is *undecidable*.

**Proposition** *For every theory $T$ of $L$ with recursively enumerable axioms,*

- $(i)$ *$\mathit{Thm}(T)$ is recursively enumerable,*
- $(ii)$ *if $T$ is complete, then $\mathit{Thm}(T)$ is recursive, i.e. $T$ is decidable.*

*Proof* The construction of systematic tableau from $T$ with a root $F\varphi$ assumes a given enumeration of axioms of $T$. Since $T$ has recursively enumerable axioms, the construction provides an algorithm that recognizes $T \vdash \varphi$.

If $T$ is complete, then $T \nvdash \varphi$ if and only if $T \vdash \neg\varphi$ for every sentence $\varphi$. Hence, the parallel construction of systematic tableaux from $T$ with roots $F\varphi$ resp. $T\varphi$ provides an algorithm that decides $T \vdash \varphi$. $\square$

# Recursively enumerable complete extensions

*What happens if we are able to describe all simple complete extensions?*

We say that the set of all (up to equivalence) simple complete extensions of a theory $T$ is *recursively enumerable* if there exists an algorithm $\alpha(i, j)$ that generates $i$-th axiom of $j$-th extension (in some enumeration) or announces that it (such an axiom or an extension) does not exist.

**Proposition** *If a theory $T$ has recursively enumerable axioms and the set of all (up to equivalence) simple complete extensions of $T$ is recursively enumerable, then $T$ is decidable.*

*Proof* By the previous proposition there is an algorithm to recognize $T \vdash \varphi$. On the other hand, if $T \nvdash \varphi$ then $T' \vdash \neg\varphi$ is some simple complete extension $T'$ of $T$. This can be recognized by parallel construction of systematic tableaux with root $T\varphi$ from all extensions. In the $i$-th step we construct tableaux up to $i$ levels for the first $i$ extensions. □

# Examples of decidable theories

The following theories are decidable although not complete.

- the theory of pure equality; with no axioms, in $L = \langle\rangle$ with equality,
- the theory of unary predicate; with no axioms, in $L = \langle U \rangle$ with equality, where $U$ is a unary relation symbol,
- the theory of dense linear orders $DeLO^*$,
- the theory of algebraically closed fields in $L = \langle +, -, \cdot, 0, 1 \rangle$ with equality, with the axioms of fields, and moreover the axioms for all $n \geq 1$,
$$(\forall x_{n-1}) \dots (\forall x_0)(\exists y)(y^n + x_{n-1} \cdot y^{n-1} + \dots + x_1 \cdot y + x_0 = 0),$$
where $y^k$ is a shortcut for the term $y \cdot y \cdot \ \cdots \ \cdot y$ ( $\cdot$ applied $(k-1)$-times).
- the theory of Abelian groups,
- the theory of Boolean algebras.

# Recursive axiomatizability

*Can we "effectively" describe common mathematical structures?*

- A class $K \subseteq M(L)$ is *recursively axiomatizable* if there exists a recursive theory $T$ of language $L$ with $M(T) = K$.
- A theory $T$ is recursively axiomatizable if $M(T)$ is recursively axiomatizable, i.e. there is an equivalent recursive theory.

**Proposition** *For every finite structure $\mathcal{A}$ of a finite language with equality the theory $\mathrm{Th}(\mathcal{A})$ is recursively axiomatizable. Thus, $\mathrm{Th}(\mathcal{A})$ is decidable.*

*Proof* Let $A = \{a_1, \ldots, a_n\}$. $\mathrm{Th}(\mathcal{A})$ can be axiomatized by a single sentence (thus recursively) that describes $\mathcal{A}$. It is of the form *"there are exactly $n$ elements $a_1, \ldots, a_n$ satisfying exactly those atomic formulas on function values and relations that are valid in the structure $\mathcal{A}$."* $\square$

# Examples of recursive axiomatizability

The following structures $\mathcal{A}$ have recursively axiomatizable $\mathrm{Th}(\mathcal{A})$.

- $\langle \mathbb{Z}, \leq \rangle$, by the theory of discrete linear orderings,
- $\langle \mathbb{Q}, \leq \rangle$, by the theory of dense linear orderings without ends (*DeLO*),
- $\langle \mathbb{N}, S, 0 \rangle$, by the theory of successor with zero,
- $\langle \mathbb{N}, S, +, 0 \rangle$, by so called Presburger arithmetic,
- $\langle \mathbb{R}, +, -, \cdot, 0, 1 \rangle$, by the theory of real closed fields,
- $\langle \mathbb{C}, +, -, \cdot, 0, 1 \rangle$, by the theory of algebraically closed fields with characteristic $0$.

**Corollary** *For all the above structures $\mathcal{A}$ the theory $\mathrm{Th}(\mathcal{A})$ is decidable.*

*Remark* *However, $\underline{\mathbb{N}} = \langle \mathbb{N}, S, +, \cdot, 0, \leq \rangle$ is not recursively axiomatizable. (This follows from the Gödel's incompleteness theorem).*