Propositional and Predicate Logic - I

Petr Gregor

KTIML MFF UK

WS 2014/2015

Conception of the course

- logic for computer science
  - + resolution in predicate logic, unification, “background” of Prolog
  - - less of model theory, ...
- tableau method instead of Hilbert-style calculi
  - + algorithmically more intuitive, (sometimes) more elegant proofs
  - - uncovered (much) in usual textbooks, restriction to countable languages
- propositional logic entirely before predicate logic
  - + ideal “playground” for comprehension of foundational concepts
  - - slower pace of lectures at the beginning
- undecidability and incompleteness less formally
  - + emphasis on principles
  - - a risk of impreciseness

Plan of the lectures 1/2

- Introduction
  1. Historical overview, “paradoxes”, logic as a language of mathematics, relation of syntax and semantics, preliminaries.
- Propositional logic
  2. Basic syntax and semantics, universality of logical connectives, normal forms, 2-SAT and Horn-SAT, semantics with respect to theories.
  3. Properties of theories, algebra of propositions, analysis of theories over finite set of propositional letters. Tableau method in propositional logic.
  4. Tableau method: systematic tableau, soundness, completeness, compactness.
  5. Resolution method, soundness and completeness, linear resolution, resolution in Prolog. Hilbert-style calculus.

Plan of the lectures 2/2

- Predicate logic
  6. Basic syntax and semantics, instances and variants. Structures and models of theories. Properties of theories.
  7. Substructures, open theories. Expansion and reduct. Boolean algebras. Tableau method in predicate logic.
  8. Tableau method: systematic tableau, soundness, completeness, compactness. Treatment of equality.
  9. Extensions by definitions. Prenex normal form, skolemisation, Herbrand's theorem.
  10. Resolution method: substitution, unification, soundness and completeness. Linear resolution and LI-resolution. Hilbert-style calculi.
- Model theory, incompleteness
  11. Elementary equivalence, completeness. Decidable theories. Undecidability of predicate logic. Incompleteness theorems. Undefinability of truth. Conclusion.

Recommended reading

- Books
  - A. Nerode, R.A. Shore, *Logic for Applications*, Springer, 2^{nd} edition, 1997.
  - P. Pudlák, *Logical Foundations of Mathematics and Computational Complexity - A Gentle Introduction*, Springer, 2013.
  - J.R. Shoenfield, *Mathematical Logic*, A. K. Peters, 2001.
  - W. Hodges, *Shorter Model Theory*, Cambridge University Press, 1997.
- Online resources
  - lecture slides
  - ...

Historical overview

- Aristotle (384-322 B.C.E.) - theory of syllogistic, e.g.

  from *'no Q is R'* and *'every P is Q'* infer *'no P is R'*.

- Euclid: *Elements* (about 330 B.C.E.) - axiomatic approach to geometry

  "There is at most one line that can be drawn parallel to another given one through an external point." (5th postulate)

- Descartes: *Geometry* (1637) - algebraic approach to geometry
- Leibniz - dream of *"lingua characteristica, calculus ratiocinator"* (1679-90)
- De Morgan - introduction of propositional connectives (1847)

$$\neg(p \vee q) \leftrightarrow \neg p \wedge \neg q$$
$$\neg(p \wedge q) \leftrightarrow \neg p \vee \neg q$$

- Boole - propositional functions, algebra of logic (1847)
- Schröder - semantics of predicate logic, concept of a model (1890-1905)

Historical overview - set theory

- Cantor - *intuitive* set theory (1878), e.g. the comprehension principle

  "For every property $\varphi(x)$ *there exists a set* $\{x \mid \varphi(x)\}$*."*

- Frege - first formal system with quantifiers and relations, concept of proofs based on inference, axiomatic set theory (1879, 1884)

- Russel - Frege's set theory is contradictory (1903)

  For a set $a = \{x \mid \neg(x \in x)\}$ *is* $a \in a$ *?*

- Russel, Whitehead - theory of types (1910-13)

- Zermelo (1908), Fraenkel (1922) - *standard* set theory ZFC, e.g.

  "For every property $\varphi(x)$ *and a set* y *there is a set* $\{x \in y \mid \varphi(x)\}$*."*

- Bernays (1937), Gödel (1940) - set theory based on classes, e.g.

  "For every property of sets $\varphi(x)$ *there exists a class* $\{x \mid \varphi(x)\}$*."*

Historical overview - algorithmization

- Hilbert - complete axiomatizaton of Euclidean geometry (1899),
  formalism - strict divorce from the intended meanings

  "It could be shown that all of mathematics follows from a correctly chosen finite system of axioms."

- Brouwer - intuitionism, emphasis on explicit constructive proofs

  "A mathematical statement corresponds to a mental construction, and its validity is verified by intuition."

- Post - completeness of propositional (and Gödel - predicate) logic
- Gödel - incompleteness theorems (1931)
- Kleene, Post, Church, Turing - formalizations of the notion of algorithm, an existence of algorithmically undecidable problems (1936)
- Robinson - resolution method (1965)
- Kowalski; Colmerauer, Roussel - Prolog (1972)

Levels of language

We will formalize the notion of proof and validity of mathematical statements.

We distinguish different levels of logic according to the means of language, in particular to which level of quantification is admitted.

- propositional connectives *propositional logic*
  This allows to form combined propositions from the basic ones.
- variables for objects, symbols for relations and functions, quantifiers *first-order logic*
  This allows to form statements on objects, their properties and relations.
  The (standard) set theory is also described by a first-order language.

In higher-order languages we have, in addition,

- variables for sets of objects (also relations, functions) *second-order logic*
- variables for sets of sets of objects, *etc.* *third-order logic*
- ...

Examples of statements of various orders

- *"If it will not rain, we will not get wet. And if it will rain, we will get wet, but then we will get dry on the sun."* *proposition*

$$(\neg r \to \neg w) \land (r \to (w \land d))$$

- *"There exists the smallest element."* *first-order*

$$\exists x\, \forall y\, (x \leq y)$$

- The axiom of induction. *second-order*

$$\forall X\, ((X(0) \land \forall y(X(y) \to X(y+1))) \to \forall y\, X(y))$$

- *"Every union of open sets is an open set."* *third-order*

$$\forall \mathcal{X} \forall Y ((\forall X(\mathcal{X}(X) \to \mathcal{O}(X)) \land \forall z(Y(z) \leftrightarrow \exists X(\mathcal{X}(X) \land X(z)))) \to \mathcal{O}(Y))$$

Syntax and semantics

We will consider relations between syntax and semantics:

- *syntax*: language, rules for formation of formulas, interference rules, formal proof system, proof, provability,
- *semantics*: interpreted meaning, structures, models, satisfiability, validity.

We will introduce the notion of proof as a well-defined syntactical object.

A formal proof system is

- *sound*, if every provable formula is valid,
- *complete*, if every valid formula is provable.

We will show that predicate logic (first-order logic) has formal proof systems that are both sound and complete. This does not hold for higher order logics.

Paradoxes

"Paradoxes" show us the need of precise definitions of foundational concepts.

- *Cretan paradox*

  Cretan said: "All Cretans are liars."
- *Barber paradox*

  There is a barber in a town who shaves all that do not shave themselves. Does he shave himself?
- *Liar paradox*

  This sentence is false.
- *Berry paradox*

  The expression "The smallest positive integer not definable in under eleven words" defines it in ten words.

Set-theoretical notions

All notions are introduced within a set theory using only the membership predicate and equality (and means of logic).

- A property of sets $\varphi(x)$ defines a *class* $\{x \mid \varphi(x)\}$. A class that is not a set is called a *proper* class, eg. $\{x \mid x = x\}$,
- $x \notin y$, $x \neq y$ are shortcuts for $\neg(x \in y)$, $\neg(x = y)$,
- $\{x_0, \ldots, x_{n-1}\}$ denotes the set containing exactly $x_0, \ldots, x_{n-1}$, $\{x\}$ is called a *singleton*, $\{x, y\}$ is called an *unordered pair*,
- $\emptyset$, $\cup$, $\cap$, $\setminus$, $\triangle$ stand for *empty set*, *union*, *intersection*, *difference*, *symmetric difference* of sets, e.g.
$$x \triangle y = (x \setminus y) \cup (y \setminus x) = \{z \mid (z \in x \wedge z \notin y) \vee (z \notin x \wedge z \in y)\}$$
- x, y are *disjoint* if $x \cap y = \emptyset$, we denote by $x \subseteq y$ that x is a *subset* of y,
- the *power set* of x is $\mathcal{P}(x) = \{y \mid y \subseteq x\}$,
- the *union* of x is $\bigcup x = \{z \mid \exists y(z \in y \wedge y \in x)\}$,
- a *cover* of a set x is a set $y \subseteq \mathcal{P}(x) \setminus \{\emptyset\}$ with $\bigcup y = x$. If, moreover, all sets in y are mutually disjoint, then y is a *partition* of x.

Relations

- An *ordered pair* is $(x, y) = \{x, \{x, y\}\}$, so $(x, x) = \{x, \{x\}\}$, an *ordered n-tuple* is $(x_0, \ldots, x_{n-1}) = ((x_0, \ldots, x_{n-2}), x_{n-1})$ for $n > 2$,
- the *Cartesian product* of a and b is $a \times b = \{(x, y) \mid x \in a, y \in b\}$, the *Cartesian power* of x is $x^0 = \{\emptyset\}$, $x^1 = x$, $x^n = x^{n-1} \times x$ for $n > 1$,
- the *disjoint union* of x and y is $x \uplus y = (\{\emptyset\} \times x) \cup (\{\{\emptyset\}\} \times y)$,
- a *relation* is a set R of ordered pairs, instead of $(x, y) \in R$ we usually write $R(x, y)$ or $x\, R\, y$,

  the *domain* of R is $\mathrm{dom}(R) = \{x \mid \exists y\, (x, y) \in R\}$,

  the *range* of R is $\mathrm{rng}(R) = \{y \mid \exists x\, (x, y) \in R\}$,

  the *extension* of x in R is $R[x] = \{y \mid (x, y) \in R\}$,

  the *inverse relation* to R is $R^{-1} = \{(y, x) \mid (x, y) \in R\}$,

  the *restriction* of R to the set z is $R \restriction z = \{(x, y) \in R \mid x \in z\}$,
- the *composition* of relations R and S is the relation
  $$R \circ S = \{(x, z) \mid \exists y\, ((x, y) \in R \wedge (y, z) \in S)\},$$
- the *identity* on a set z is the relation $\mathrm{Id}_z = \{(x, x) \mid x \in z\}$.

Equivalences

- A relation R on X is an *equivalence* if for every $x, y, z \in X$

$$R(x,x) \qquad \text{(reflexivity)}$$
$$R(x,y) \rightarrow R(y,x) \qquad \text{(symmetry)}$$
$$R(x,y) \wedge R(y,z) \rightarrow R(x,z) \qquad \text{(transitivity)}$$

- $R[x]$ is called the *equivalence class* of x in R, denoted also $[x]_R$.
- $X/R = \{R[x] \mid x \in X\}$ is the *quotient set* of X by R.
- It holds that X/R is a partition of X since the equivalence classes are mutually disjoint and cover X.
- On the other hand, a partition S of X determines the equivalence (on X)

$$\{(x,y) \mid x \in z, y \in z \text{ for some } z \in S\}.$$

Orders

Let $\leq$ be a relation on a set X. We say that $\leq$ is

- a *partial order* (of the set X) if for every $x, y, z \in X$

$$x \leq x \qquad \text{(reflexivity)}$$
$$x \leq y \;\wedge\; y \leq x \;\rightarrow\; x = y \qquad \text{(antisymmetry)}$$
$$x \leq y \;\wedge\; y \leq z \;\rightarrow\; x \leq z \qquad \text{(transitivity)}$$

- a *linear* (*total*) *order* if, moreover, for every $x, y \in X$

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

- a *well-order* if, moreover, every non-empty subset of X has a *least* element.

Let us write '$x < y$' for '$x \leq y \wedge x \neq y$'. A linear order $\leq$ on X is

- a *dense order* if X is not a singleton and for every $x, y \in X$

$$x < y \;\rightarrow\; \exists z\, (x < z \wedge z < y) \qquad \text{(density)}$$

Functions

A relation f is a function if every $x \in \mathrm{dom}(f)$ has exactly one y with $(x, y) \in f$.

- We say that y is the *value* of the function f at x, denoted by $f(x) = y$,
- $f\colon X \to Y$ denotes that f is a function with $\mathrm{dom}(f) = X$ and $\mathrm{rng}(f) \subseteq Y$,
- a function f is a *surjection* (*onto* Y) if $\mathrm{rng}(f) = Y$,
- a function f is *injection* (*one-to-one*) if for every $x, y \in \mathrm{dom}(f)$

$$x \neq y \quad \to \quad f(x) \neq f(y)$$

- $f\colon X \to Y$ is *bijection* from X to Y if it is both injection and surjection,
- if $f\colon X \to Y$ is injective, then $f^{-1} = \{(y, x) \mid (x, y) \in f\}$ is its *inverse*,
- the *image* of the set A under f is $f[A] = \{y \mid (x, y) \in f$ for some $x \in A\}$,
- if $f\colon X \to Y$ and $g\colon Y \to Z$, their composition $(f \circ g)\colon X \to Z$ satisfies

$$(f \circ g)(x) = g(f(x))$$

- ${}^{X}Y$ denotes the set of all functions from X to Y.

Numbers

We give examples of standard formal constructions.

- The natural numbers are defined inductively by $n = \{0, \ldots, n-1\}$, thus
$$0 = \emptyset, \quad 1 = \{0\} = \{\emptyset\}, \quad 2 = \{0, 1\} = \{\emptyset, \{\emptyset\}\}, \quad \ldots$$
- the sef of *natural* numbers $\mathbb{N}$ is defined as the smallest set containing $\emptyset$ which is closed under $S(x) := x \cup \{x\}$ (successor),
- the set of *integers* is $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\sim$, where $\sim$ is the equivalence
$$(a, b) \sim (c, d) \text{ if and only if } a + d = b + c$$
- the set of *rational* numbers is $\mathbb{Q} = (\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}))/\approx$, where $\approx$ is given by
$$(a, b) \approx (c, d) \text{ if and only if } a.d = b.c$$
- the set of *real* numbers $\mathbb{R}$ is the set of *cuts* of rational numbers, that is non-trivial downwards closed subsets of $\mathbb{Q}$ with no greatest element. ($A \subset \mathbb{Q}$ is *downwards closed* if $y < x \in A$ implies $y \in A$.)

Cardinalities

- x has *cardinality smaller or equal* to the cardinality of y if there is an injective function $f\colon x \to y$, $(x \preccurlyeq y)$
- x has *same cardinality* as y if there is a bijection $f\colon x \to y$, $(x \approx y)$
- x has *cardinality strictly smaller* than y if $x \preccurlyeq y$ but not $x \approx y$, $(x \prec y)$

Theorem (Cantor) $x \prec \mathcal{P}(x)$ *for every set* x.

Proof $f(y) = \{y\}$ for $y \in x$ is an injective function $f\colon x \to \mathcal{P}(x)$, so $x \preccurlyeq \mathcal{P}(x)$.
Suppose for a contradiction that there is an injective $g\colon \mathcal{P}(x) \to x$. Define

$$y = \{g(z) \mid z \subseteq x \wedge g(z) \notin z\}$$

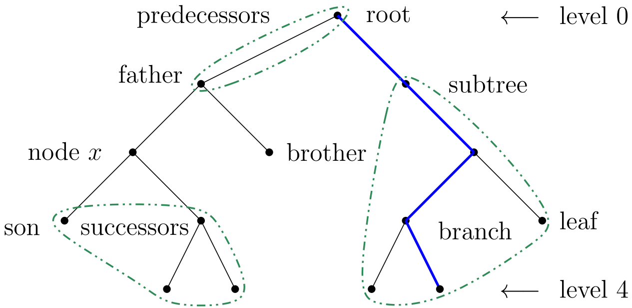
By definition, $g(y) \in y$ if and only if $g(y) \notin y$, a contradiction. $\square$

- for every x there is *cardinal number* κ with $x \approx \kappa$, denoted by $|x| = \kappa$,
- x is *finite* if $|x| = n$ for some $n \in \mathbb{N}$, x is *countable* if $|x| = |\mathbb{N}| = \omega$,
- x is *uncountable* if it is neither finite nor countable,
- x has *cardinality of the continuum* if $|x| = |\mathcal{P}(\mathbb{N})| = \mathfrak{c}$.

n-ary relations and functions

- A relation of *arity* $n \in \mathbb{N}$ on X is any set $R \subseteq X^n$, so for $n = 0$ we have either $R = \emptyset = 0$ or $R = \{\emptyset\} = 1$, and for $n = 1$ we have $R \subseteq X$,
- A (partial) function of *arity* $n \in \mathbb{N}$ from X to Y is any function $f \subseteq X^n \times Y$. We say that f is *total* on X^n if $\mathrm{dom}(f) = X^n$, denoted by $f\colon X^n \to Y$. If, moreover, $Y = X$, we say that f is an *operation* on X.
- A function $f\colon X^n \to Y$ is *constant* if $\mathrm{rng}(f) = \{y\}$ for some $y \in Y$, for $n = 0$ we have $f = \{(\emptyset, y)\}$ and we identify f with the *constant* y.
- The arity of a relation or function is denoted by $\mathrm{ar}(R)$ or $\mathrm{ar}(f)$ and we speak about *nullary*, *unary*, *binary*, etc. relations and functions.

Trees



- A *tree* is a set T with a partial order $<_T$ in which there is a unique least element, called the *root*, and the set of predecessors of any element is well ordered by $<_T$,
- a *branch* of a tree T is a maximal linearly ordered subset of T,
- we adopt standard terminology on trees from the graph theory, e.g.

a branch in a finite tree is a path from the root to a leaf.

König's lemma

We will consider *(for simplicity)* usually finitely branching trees in which every node except the root has an immediate predecessor (*father*).

- *n-th level* of a tree T for $n \in \mathbb{N}$ is given by induction, it is the set of sons of nodes from the $(n-1)$-th level, 0-th level containing exactly the root,
- the *depth* of T is the maximal $n \in \mathbb{N}$ of non-empty level; if T has infinite branch, then it has *infinite depth* ω.
- a tree T is *n-ary* for $n \in \mathbb{N}$ if every node has at most n sons. It is *finitely branching*, if every node has only finitely many sons.

Lemma (König) *Every infinite, finitely branching tree contains an infinite branch.*

Proof We start in the root. Since it has only finitely many sons, there exists a son with infinitely many successors. We *choose* him and continue in his subtree. In this way we construct an infinite branch. □

Ordered trees

- An *ordered tree* is a tree T with a linear order of sons at each node. These orders are called *left-right orders* and are denoted by $<_L$. In comparison with $<_L$, the order $<_T$ is called the *tree order*.
- A *labeled tree* is a tree T with an arbitrary function (a *labeling function*), that assigns to each node some object (a *label*).
- Labeled ordered trees represent, for example, structure of formulas.