Logic for Computer Science

Summer semester
2019-2020

LECTURE 10:

Decidable theories & quantifier elimination

Lectures: LORENZO CLEMENTE
Tutorials: DARIA WALUKIEWICZ, JACEK CHRZĄSZCZ, JĘDRZEJ KOŁODZIEJSKI
Labs: DARIA, JACEK + PIOTR HOFMAN

SUMMARY

- logical theories (axiomatic theories, theory of a structure).
- The decision problem of a theory.
- Undecidability (next time).
- Decidable theories.
- Finite model property.
- Elimination of quantifiers.
  - Examples of theories with quantifier elimination.
  - Quantifier elimination for $(\mathbb{Q}, \leq)$.
  - Consequences of quantifier elimination.

THEORIES

A **theory** is a set of sentences Γ closed w.r.t. logical consequence:
$\Gamma \models \varphi$ implies $\varphi \in \Gamma$.

A theory Γ is **complete** if for every φ, $\varphi \in \Gamma$ or $\neg\varphi \in \Gamma$.

How to define a theory?

1) From syntax (formulas):
Axiomatic theory of a set of axioms Δ: $Th(\Delta) := \{\varphi \mid \Delta \models \varphi\}$.
Sometimes complete, sometimes incomplete.

2) From semantics (structures):
Theory of a structure $\mathcal{A}$: $Th(\mathcal{A}) = \{\varphi \mid \mathcal{A} \models \varphi\}$.
Always complete!

EXAMPLES: THEORIES from SYNTAX (AXIOMATIC TH.)

Theory of dense total orders with no endpoints (DLO). $\Sigma = \{\leq\}$.

(linear)

$\Delta_{DLO} = \{$ reflexivity, transitivity, density, no max/min $\}$.

Sometimes infinitely many axioms are required:

$\Delta_\infty = \{$ size ≥ 1, size ≥ 2, ... $\}$, $\Sigma = \{=\}$: Theory of infinite structures.

$\Delta_{RCF} = \{$ ordered fields, $\forall x \geq 0\ \exists y \cdot y^2 = x \} \cup \{\varphi_1, \varphi_3, \varphi_5, \dots\}$,

$\Sigma = \{0, 1, +, \cdot, \leq\}$, $\varphi_n \equiv$ every polynomial of degree n has a root: Theory of real closed fields.

$\Delta_{FO} = \{\varphi \mid \vdash \varphi\}$: sentences provable in Hilbert's proof system.

By soundness & completeness, $Th(\Delta_{FO}) = \Delta_{FO} = \{\varphi \mid \models \varphi\}$ valid sentences (true in every structure).

EXAMPLES: THEORIES from SEMANTICS (STRUCTURES)

$Th(\mathbb{A}, =)$: first order theory of an infinite set with equality. $= Th(\Delta_\infty)$

$Th(\mathbb{Q}, \leq)$: first-order theory of the rationals with order. $= Th(\Delta_{DLO})$

$Th(\mathbb{Q}, +)$: additive theory of the rationals.

$Th(\mathbb{Q}, \cdot)$: Skolem arithmetic.

$Th(\mathbb{N}, +)$: Presburger arithmetic.

$Th(\mathbb{R}, +, \cdot)$: Tarski algebra. $= Th(\Delta_{RCF})$

$Th(\Sigma^*, \cdot)$: Theory of the free monoid (finite words).

$\vdots$

(The theory of a structure is complete by definition.)

THE DECISION PROBLEM for a theory Γ over Σ.

(ENTSCHEIDUNGSPROBLEM)

INPUT: a sentence φ over vocabulary Σ.

OUTPUT: YES iff $\varphi \in \Gamma$.

$\Rightarrow$ The central problem in mathematical logic (Hilbert/Ackermann '28)

THEOREM (Church '36, Turing '37)
The validity problem for first-order logic is undecidable.
(but recursively enumerable thanks to Gödel's completeness theorem)

THEOREM (Trakhtenbrot '50)
The finite satisfiability problem is undecidable.
(but obviously recursively enumerable)

DECIDABLE THEORIES (φ valid $\Leftrightarrow$ unsatisfiable $\neg\varphi$)

Two techniques to obtain decidability:

1) Finite model property (satisfiable $\Rightarrow$ finitely satisfiable).

   Algorithm to decide validity of φ:

   Semiprocedure 1: enumerate proofs. } terminates thanks
   Semiprocedure 2: enumerate models. } to completeness + FMP.

2) Effective elimination of quantifiers.

   Idea: Convert φ to an equivalent quantifier-free ψ.

   If φ is a sentence (no free variables),
   then ψ is even variable free and can often be
   checked directly.

DECIDABLE FRAGMENTS ZOO (with equality)

- Monadic first-order logic (Löwenheim '15)
  (only unary predicates; no equality, no functions).
- $\exists^* \forall^*$ fragment (Bernays, Schönfinkel '28; Ramsey '30 with eq.)
- $\exists^* \forall \exists^*$ fragment (no eq. Ackermann '28; '54 with eq.)
- $\exists^* \forall^2 \exists^*$ fragment, no equality (Gödel '32)
  Tight: SAT for $\forall\exists\forall$ and $\forall^3\exists$ is undecidable without eq. (Surányi '50; Kahr, Moor, Wang '62), and $\exists^* \forall^2 \exists^*$ with eq. (Goldfarb '84).
- FO^2: 2 variable fragment (Scott '62, Mortimer '75)
  Tight: FO^3 undecidable
- Guarded fragment, guarded negation fragment, ...

} FINITE MODEL PROPERTY

QUANTIFIER ELIMINATION

$$\varphi(a,b,c) \equiv \exists x \cdot ax^2 + bx + c = 0 \quad (\text{over } \mathbb{R})$$

Can we find a quantifier-free formula $\psi(a,b,c)$ equivalent to φ?

$$\psi(a,b,c) \equiv \big(a = 0 \wedge (c = 0 \vee b \neq 0)\big) \vee \big(a \neq 0 \wedge b^2 - 4ac \geq 0\big)$$

Tarski-Seidenberg
$Th(\mathbb{R}, +, \cdot, 0, 1, \leq)$ has effective elimination of quantifiers.

$\Rightarrow$ There are q.f. equivalents of (!)

$$\exists x \cdot ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$$

EXAMPLES of THEORIES with QUANTIFIER ELIMINATION

(caveat: need to extend the signature sometimes)

- $Th(\mathbb{A}, =)$, $\mathbb{A}$ infinite
- $Th(\mathbb{Q}, \leq)$: dense total order.
- Theory of the Erdős-Rényi random graph.

} homogeneous structures

⋮

- $Th(\mathbb{Z}, (+1), \leq)$: discrete total order. (successor function)
- $Th(\mathbb{Q}, +, \leq)$: additive theory of rational numbers.
- $Th(\mathbb{Z}, +, \leq)$: Presburger logic.
- $Th(\mathbb{N}, \cdot)$: Skolem arithmetic.
- $Th(\mathbb{R}, +, \cdot)$: Tarski algebra.

⋮

TOWARDS QUANTIFIER ELIMINATION

Claim: It suffices to consider formulas "conjunctive query" $\exists x \cdot \underbrace{\varphi_1 \wedge \cdots \wedge \varphi_n}$

atomic & quantifier-free & contains x

$$qe(\neg\varphi) = \neg qe(\varphi)$$

$$qe(\varphi \vee \psi) = qe(\varphi) \vee qe(\psi)$$

$$qe(\varphi \wedge \psi) = qe(\varphi) \wedge qe(\psi)$$

$$qe(\forall x \cdot \varphi) = qe(\neg \exists x \cdot \neg\varphi)$$

$$qe(\exists x \cdot \varphi) = qe(\varphi) \text{ if } x \notin fv(\varphi)$$

$$qe(\exists x \cdot \varphi) = qe(\exists x \cdot \varphi_1) \vee \cdots \vee qe(\exists x \cdot \varphi_n), \text{ where}$$

$$DNF(qe(\varphi)) \equiv \varphi_1 \vee \cdots \vee \varphi_n$$ ← conjunctive

EXAMPLE: QUANTIFIER ELIMINATION for $(\mathbb{Q}, \leq)$

How does $\varphi \equiv \exists x \cdot \varphi_1 \wedge \cdots \wedge \varphi_m$ look like over $\Sigma = \{\leq\}$?

Case 1: Some $\varphi_i \equiv x < x$. Then $\psi \equiv \bot$

Case 2: Some $\varphi_i \equiv x = y$. Replace x with y everywhere.

Case 3: $\varphi \equiv \exists x \cdot \underbrace{y_1 < x \wedge \cdots \wedge y_m < x}_{\text{lower bounds}} \wedge \underbrace{x < z_1 \wedge \cdots \wedge x < z_n}_{\text{upper bounds}}$

Take $\psi \equiv \bigwedge_{i,j} y_i < z_j$.

Correctness by density.

CONSEQUENCES of QUANTIFIER ELIMINATION

- If effective and the q.f. fragment is decidable $\Rightarrow$ decidability.

Ex.: $\exists x.\, ax^2+bx+c=0 \rightsquigarrow (a=0 \wedge (c=0 \vee b\neq 0)) \vee (a\neq 0 \wedge b^2-4ac \geq 0)$.

CONSEQUENCES of QUANTIFIER ELIMINATION

- If effective and the q.f. fragment is decidable $\Rightarrow$ decidability.

  Ex.: $\exists x.\, ax^2+bx+c=0 \rightsquigarrow (a=0 \wedge (c=0 \vee b\neq 0)) \vee (a\neq 0 \wedge b^2-4ac \geq 0)$.

- no constants + q.e. $\Rightarrow$ completeness.

  Proof: let Γ be a theory and φ a sentence (no free variables)

  By q.e. there is ψ q.f. s.t. $\Gamma \vdash \varphi \leftrightarrow \psi$.

  Since no constants, ψ is equivalent to either $\top$ (and thus $\varphi \in \Gamma$) or $\bot$ (and thus $\neg\varphi \in \Gamma$).