

Logic for Computer Science

Summer Semester
2019-2020

LECTURE 10:

Decidable theories
&
quantifier elimination

Lectures : LORENZO CLEMENTE

Tutorials : DARIA WALUKIEWICZ, JACEK CHRZASZCZ,
JĘDRZEJ KOŁODZIEJSKI

Labs : DARIA, JACEK + PIOTR WOJTAN

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 : $\text{Th}(\Delta) := \{\varphi \mid \Delta \models \varphi\}$.

Sometimes complete, sometimes incomplete.

2) From semantics (structures):

Theory of a structure \mathcal{A} : $\text{Th}(\mathcal{A}) = \{\varphi \mid \mathcal{A} \models \varphi\}$.

Always complete!

EXAMPLES : THEORIES from SYNTAX (AXIOMATIC TH.)

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

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

Sometimes infinitely many axioms are required :

$\Delta_\infty = \{\text{size} >_1, \text{size} >_2, \dots\}, \Sigma = \{=\}$: Theory of infinite structures.

$\Delta_{\text{RCF}} = \{\text{ordered fields, } \forall x >_0 \exists y \cdot y^2 = x\} \cup \{\varphi_1, \varphi_3, \varphi_5, \dots\},$

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

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

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

EXAMPLES: THEORIES from SEMANTICS (STRUCTURES)

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

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

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

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

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

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

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

:

(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 (döwenheim'15)
(Only unary predicates; no equality, no functions).
- $\exists^* \forall^*$ fragment (Brouwer, 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 $\forall \exists$ is undecidable

without eq. (Sváeny '50; Kohn, Moon, Wang '62),

and $\exists^* \forall^2 \exists^*$ with eq. (Golomb '84).

- FO^2 : 2 variable fragment (Scott '62, Mortimer '75)

Tight: FO^3 undecidable

- Guarded fragment, guarded negation fragment, ...

FINITE
MODEL
PROPERTY

QUANTIFIER ELIMINATION

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

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

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

Tarski-Seidenberg

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

⇒ There are q.f. equivalents of (!)

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

EXAMPLES of THEORIES with QUANTIFIER ELIMINATION

(caveat: need to extend the signature sometimes)

- $\text{Th}(\mathbb{A}, =)$, \mathbb{A} infinite
 - $\text{Th}(\mathbb{Q}, \leq)$: dense total order.
 - Theory of the Erdős-Rényi random graph.
- :
- $\text{Th}(\mathbb{Z}, (\overset{\leftarrow}{+1}), \leq)$: discrete total order .
 - $\text{Th}(\mathbb{Q}, +, \leq)$: additive theory of rational numbers.
 - $\text{Th}(\mathbb{Z}, +, \leq)$: Presburger logic .
 - $\text{Th}(\mathbb{N}, \cdot)$: Skolem arithmetic .
 - $\text{Th}(\mathbb{R}, +, \cdot)$: Tarski algebra .
- :
- homogeneous
structures*

TOWARDS QUANTIFIER ELIMINATION

Claim: It suffices to consider formulas

~~conjunctional quant.~~

$\exists x \cdot \underbrace{\varphi_1 \wedge \dots \wedge \varphi_m}$

Or negation of atomic

atomic & quantifier-free & contains x

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

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

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

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

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

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

$$DNF(qe(\varphi)) \equiv \varphi_1 \vee \dots \vee \varphi_m \xleftarrow{\text{conjunctional}}$$

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

How does $\varphi \equiv \exists x . \psi_1 \wedge \dots \wedge \psi_m$ look like over $\Sigma = \{\leq\}$?

Case 1 : Some $\psi_i \equiv x < x$. Then $\psi \equiv \perp$

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

Case 3 : $\psi \equiv \exists x . \underbrace{y_1 < x \wedge \dots \wedge y_m < x}_{\text{lower bounds}} \wedge \underbrace{x < z_1 \wedge \dots \wedge x < z_m}_{\text{upper bounds}}$

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

- No constants + q.e. \Rightarrow completeness.

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

By q.e. there is φ q.f. s.t. $\Gamma \models \varphi \leftrightarrow \psi$.

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