Lecture 14

Decidable Theories

Logical theories, quantifier elimination, unbounded dense linear orders, linear arithmetic over the rationals, Presburger arithmetic

Dr Christoph Haase
University of Oxford
(with small changes by Javier Esparza)

Logical theories

- Fix a (finite or infinite) signature σ. We implicitly assume that all formulas are over σ. We call a closed formula a **sentence**.
- A **theory** $\mathcal{T}$ is a set of sentences closed under semantic entailment:
$$\mathcal{T} \models F \text{ implies } F \in \mathcal{T}$$
- Given a σ-structure $\mathcal{A}$, the **theory of** $\mathcal{A}$, denoted $\mathrm{Th}(\mathcal{A})$, is the theory containing all sentences F such that $\mathcal{A} \models F$.
- The **theory of a set** $\mathcal{S}$ of sentences is the set of sentences $\mathcal{T} = \{F : \mathcal{S} \models F\}$.
- If $\mathcal{T}$ is the theory of $\mathcal{S}$, then $\mathcal{S}$ is a set of **axioms** of $\mathcal{T}$.

Logical theories

A set $\mathcal{F}$ of formulas is **decidable** if there is an algorithm that decides for every formula F whether $F \in \mathcal{F}$ holds.

A theory $\mathcal{T}$ is

- **consistent** if for every sentence F, either $F \notin \mathcal{T}$ or $\neg F \notin \mathcal{T}$ (or both).
- **complete** if for every sentence F either $F \in \mathcal{T}$ or $\neg F \in \mathcal{T}$ (or both).
- **decidable** if $\mathcal{T}$ is decidable as a set of sentences.
- **(finitely) axiomatizable** if it is the theory of a (finite) decidable set of sentences.

Logical theories

Some easy facts:

- For every σ-structure $\mathcal{A}$, the theory $\mathrm{Th}(\mathcal{A})$ is consistent and complete.

Logical theories

Some easy facts:

- For every σ-structure $\mathcal{A}$, the theory $\mathrm{Th}(\mathcal{A})$ is consistent and complete.
- The only inconsistent theory is the theory of all sentences.

Logical theories

Some easy facts:

- For every σ-structure $\mathcal{A}$, the theory $\mathrm{Th}(\mathcal{A})$ is consistent and complete.
- The only inconsistent theory is the theory of all sentences.
- Theory consistent but not complete:

Logical theories

Some easy facts:

- For every σ-structure $\mathcal{A}$, the theory $\mathrm{Th}(\mathcal{A})$ is consistent and complete.
- The only inconsistent theory is the theory of all sentences.
- Theory consistent but not complete: theory of all valid sentences.

Logical theories

Some easy facts:

- For every σ-structure $\mathcal{A}$, the theory $\mathrm{Th}(\mathcal{A})$ is consistent and complete.
- The only inconsistent theory is the theory of all sentences.
- Theory consistent but not complete: theory of all valid sentences.
- For every theory $\mathcal{T}$, the set $\mathcal{T}$ is a set of axioms of $\mathcal{T}$.

Examples of logical theories

Example

Linear arithmetic over the rationals is the structure-based theory

$$\mathrm{Th}(\mathbb{Q}, 1, <, +, \{c\, \cdot\,\}_{c \in \mathbb{Q}})$$

It allows one to express

- the system of linear inequalities $A\boldsymbol{x} \leq \boldsymbol{b}$ has no solution
- every solution of $A\boldsymbol{x} \leq \boldsymbol{b}$ is also a solution of $C\boldsymbol{x} \leq \boldsymbol{d}$

Examples of logical theories

Example

Linear arithmetic over the rationals is the structure-based theory

$$\mathrm{Th}(\mathbb{Q}, 1, <, +, \{c\,\cdot\,\}_{c\in\mathbb{Q}})$$

It allows one to express

- the system of linear inequalities $A\boldsymbol{x} \leq \boldsymbol{b}$ has no solution
- every solution of $A\boldsymbol{x} \leq \boldsymbol{b}$ is also a solution of $C\boldsymbol{x} \leq \boldsymbol{d}$

Example

The theory $\mathcal{T}_{UDLO}$ of *unbounded dense linear orders* is the set of sentences entailed by the following set of axioms:

$$\begin{array}{ll}
F_1 & \forall x\,\forall y\,(x < y \rightarrow \neg(x = y \vee y < x)) \\
F_2 & \forall x\,\forall y\,\forall z\,(x < y \wedge y < z \rightarrow x < z) \\
F_3 & \forall x\,\forall y\,(x < y \vee y < x \vee x = y) \\
F_4 & \forall x\,\forall y\,(x < y \rightarrow \exists z\,(x < z \wedge z < y)) \\
F_5 & \forall x\,\exists y\,\exists z\,(y < x < z)\,.
\end{array}$$

Decidable theories

- Quantifier-elimination is a technique to show decidability
- A theory $\mathcal{T}$ **admits quantifier-elimination** if for any formula (not necessarily a sentence!) $\exists x\, F$ with F quantifier-free, there is a quantifier-free formula G such that

$$\mathcal{T} \models \exists x\, F \leftrightarrow G$$

- A **quantifier-elimination procedure** for $\mathcal{T}$ is an algorithm that on input $\exists x\, F$ computes such a formula G.
- If $\mathcal{T}$ has
  - a quantifier elimination procedure, and
  - a procedure for deciding $F \in \mathcal{T}$ for variable-free atomic formulas F,

  then $\mathcal{T}$ is decidable.

Unbounded Dense Linear Orders

Theorem

The theory $\mathcal{T}_{UDLO}$ of unbounded dense linear orders is decidable.

Unbounded Dense Linear Orders

Theorem

The theory $\mathcal{T}_{UDLO}$ of unbounded dense linear orders is decidable.

Proof.

Suffices to give quantifier-elimination procedure for $\exists x\, F$, where F is conjunction of atomic formulas $x = y$, $x < y$ or $y < x$ for some variable y.

Unbounded Dense Linear Orders

Theorem

The theory $\mathcal{T}_{UDLO}$ of unbounded dense linear orders is decidable.

Proof.

Suffices to give quantifier-elimination procedure for $\exists x\, F$, where F is conjunction of atomic formulas $x = y$, $x < y$ or $y < x$ for some variable y.
Excluding trivial cases, we have

$$F = \bigwedge_{i=1}^{m} l_i < x \wedge \bigwedge_{j=1}^{n} x < u_j.$$

Unbounded Dense Linear Orders

Theorem

The theory $\mathcal{T}_{UDLO}$ of unbounded dense linear orders is decidable.

Proof.

Suffices to give quantifier-elimination procedure for $\exists x\, F$, where F is conjunction of atomic formulas $x = y$, $x < y$ or $y < x$ for some variable y.
Excluding trivial cases, we have

$$F = \bigwedge_{i=1}^{m} l_i < x \wedge \bigwedge_{j=1}^{n} x < u_j.$$

If $m = 0$ or $n = 0$ then $\mathcal{T}_{UDLO} \models \exists F \leftrightarrow$ **true**. Otherwise

$$\mathcal{T}_{UDLO} \models \exists x F \leftrightarrow \bigwedge_{i=1}^{m} \bigwedge_{j=1}^{n} l_i < u_j.$$

Unbounded Dense Linear Orders

Theorem

The theory $\mathcal{T}_{UDLO}$ of unbounded dense linear orders is decidable.

Proof.

Suffices to give quantifier-elimination procedure for $\exists x\, F$, where F is conjunction of atomic formulas $x = y$, $x < y$ or $y < x$ for some variable y.
Excluding trivial cases, we have

$$F = \bigwedge_{i=1}^{m} l_i < x \wedge \bigwedge_{j=1}^{n} x < u_j.$$

If $m = 0$ or $n = 0$ then $\mathcal{T}_{UDLO} \models \exists F \leftrightarrow$ **true**. Otherwise

$$\mathcal{T}_{UDLO} \models \exists x F \leftrightarrow \bigwedge_{i=1}^{m} \bigwedge_{j=1}^{n} l_i < u_j.$$

After eliminating all quantifiers, end up with Boolean combination of **true** and **false** whose truth value can easily be computed. □

Presburger arithmetic

Figure: Mojzesz Presburger (1904 - 1943)

$\mathrm{Th}(\mathbb{N}, 0, 1, +, <)$ is commonly known as **Presburger arithmetic**.

Simple number theory in Presburger arithmetic

Example

Every natural number is odd or even:

$$\forall x \, \exists y \, (x = y + y \vee x = y + y + 1) \, .$$

Simple number theory in Presburger arithmetic

Example

Every natural number is odd or even:

$$\forall x \, \exists y \, (x = y + y \vee x = y + y + 1)\,.$$

Example

Consider the Chicken McNugget problem: Given $a_1, \ldots, a_n \in \mathbb{N}$, is there some $c \in \mathbb{N}$ such that all numbers greater than c can be represented as a non-negative linear combination of $a_1, \ldots, a_n$:

Simple number theory in Presburger arithmetic

Example

Every natural number is odd or even:

$$\forall x \, \exists y \, (x = y + y \lor x = y + y + 1) \, .$$

Example

Consider the Chicken McNugget problem: Given $a_1, \ldots, a_n \in \mathbb{N}$, is there some $c \in \mathbb{N}$ such that all numbers greater than c can be represented as a non-negative linear combination of $a_1, \ldots, a_n$:

$$\exists x \, \forall y \, (x < y \to (\exists z_1 \ldots \exists z_n \, (y = a_1 \cdot z_1 + \cdots + a_n \cdot z_n)))$$

Quantifier-elimination for Presburger arithmetic

- $\mathrm{Th}(\mathbb{N}, 0, 1, +, <)$ does not have quantifier elimination: y cannot be eliminated from $\exists y\, x = y + y$

Quantifier-elimination for Presburger arithmetic

- $\mathrm{Th}(\mathbb{N}, 0, 1, +, <)$ does not have quantifier elimination: y cannot be eliminated from $\exists y\, x = y + y$
- Solution: extend signature with unary divisibility relations $c \mid \cdot$ for all $c > 0$ such that

$$c \mid n \text{ iff there is } k \in \mathbb{N} \text{ such that } n = k \cdot c$$

- $\mathrm{Th}(\mathbb{N}, 0, 1, +, <, \{c \mid \cdot\}_{c>0})$ has quantifier elimination

Quantifier-elimination for Presburger arithmetic

- Suffices to consider eliminating x from $F = \exists x \bigwedge_{1 \leq i \leq n} F_i$

Quantifier-elimination for Presburger arithmetic

- Suffices to consider eliminating x from $F = \exists x \bigwedge_{1 \leq i \leq n} F_i$
- Rearrange matrix of F so that x is isolated:

$$F \equiv \exists x \bigwedge_{i \in G} q_i(\vec{y}) < a_i \cdot x \wedge \bigwedge_{j \in L} a_j \cdot x < p_j(\vec{y}) \wedge \bigwedge_{k \in D} c_k \mid a_k \cdot x + r_k(\vec{y}).$$

Quantifier-elimination for Presburger arithmetic

- Suffices to consider eliminating x from $F = \exists x \bigwedge_{1 \le i \le n} F_i$
- Rearrange matrix of F so that x is isolated:

$$F \equiv \exists x \bigwedge_{i \in G} q_i(\vec{y}) < a_i \cdot x \wedge \bigwedge_{j \in L} a_j \cdot x < p_j(\vec{y}) \wedge \bigwedge_{k \in D} c_k \mid a_k \cdot x + r_k(\vec{y}).$$

- Let $b = \mathrm{lcm}\{a_i \mid i \in G \cup L \cup D\}$

Quantifier-elimination for Presburger arithmetic

- Suffices to consider eliminating x from $F = \exists x \bigwedge_{1 \le i \le n} F_i$
- Rearrange matrix of F so that x is isolated:

$$F \equiv \exists x \bigwedge_{i \in G} q_i(\vec{y}) < a_i \cdot x \wedge \bigwedge_{j \in L} a_j \cdot x < p_j(\vec{y}) \wedge \bigwedge_{k \in D} c_k \mid a_k \cdot x + r_k(\vec{y}).$$

- Let $b = \mathrm{lcm}\{a_i \mid i \in G \cup L \cup D\}$, then F is equi-satisfiable with

$$\begin{aligned} H = \exists x \bigwedge_{i \in G} \frac{b}{a_i} \cdot q_i(\vec{y}) < x \wedge \bigwedge_{j \in L} x < \frac{b}{a_j} \cdot p_j(\vec{y}) \wedge \\ \wedge \bigwedge_{k \in D} \frac{b}{a_k} \cdot c_k \mid x + \frac{b}{a_k} \cdot r_k(\vec{y}) \wedge b \mid x. \end{aligned}$$

Quantifier-elimination for Presburger arithmetic

- Suffices to consider eliminating x from $F = \exists x \bigwedge_{1\leq i\leq n} F_i$
- Rearrange matrix of F so that x is isolated:

$$F \equiv \exists x \bigwedge_{i\in G} q_i(\vec{y}) < a_i \cdot x \wedge \bigwedge_{j\in L} a_j \cdot x < p_j(\vec{y}) \wedge \bigwedge_{k\in D} c_k \mid a_k \cdot x + r_k(\vec{y}).$$

- Let $b = \mathrm{lcm}\{a_i \mid i \in G \cup L \cup D\}$, then F is equi-satisfiable with

$$H = \exists x \bigwedge_{i\in G} \frac{b}{a_i} \cdot q_i(\vec{y}) < x \wedge \bigwedge_{j\in L} x < \frac{b}{a_j} \cdot p_j(\vec{y}) \wedge \bigwedge_{k\in D} \frac{b}{a_k} \cdot c_k \mid x + \frac{b}{a_k} \cdot r_k(\vec{y}) \wedge b \mid x.$$

- Define $c = \mathrm{lcm}\{b, b \cdot c_k/a_k : k \in D\}$, then H is equivalent to

$$\begin{cases} \bigvee_{0\leq m<c} H[m/x] & \text{if } G = \emptyset \\ \bigvee_{j\in G} \bigvee_{1\leq m\leq c} H[((b/a_j) \cdot q_j(\vec{y}) + m)/x] & \text{otherwise} \end{cases}$$

Quantifier-elimination for Presburger arithmetic

Theorem (Oppen)

Presburger arithmetic is decidable in time $2^{2^{2^{O(n)}}}$.