Lecture 14

Decidable Theories

Logical theories, quantifier elimination, unbounded dense linear orders, linear rational arithmetic, Presburger arithmetic

Print version of the lecture in *Introduction to Logic for Computer Science*

presented by Prof Hongseok Yang

These lecture notes are very minor variants of the ones made by Prof James Worrell and Dr Christoph Haase for their 'Logic and Proof' course at Oxford.

1 Logical Theories

In this lecture we work exclusively with first-order logic with equality.

Fix a signature σ. A **theory** $\mathcal{T}$ is a set of sentences (closed formulas) that is closed under semantic entailment, i.e., if $\mathcal{T} \models F$ then $F \in \mathcal{T}$. Given a σ-structure $\mathcal{A}$ it is clear that the set of sentences that hold in $\mathcal{A}$ is a theory. We denote this theory by $\mathrm{Th}(\mathcal{A})$ and call it the **theory of** $\mathcal{A}$. We say that a theory $\mathcal{T}$ is **complete** if for any sentence F, either $F \in \mathcal{T}$ or $\neg F \in \mathcal{T}$. Clearly the theory of any particular structure is complete. The set of valid σ-sentences is an example of a theory that is not complete.

An example of a structure-based theory is $\mathrm{Th}(\mathbb{Q}, 1, <, +, \{c\,\cdot\,\}_{c\in\mathbb{Q}})$, linear arithmetic over the rationals. Here, $+$ is the binary addition function and $c\,\cdot$ denotes the unary function "multiply by c" for each $c \in \mathbb{Q}$. The theory is defined over a signature σ that has symbols for each component of the structure $(\mathbb{Q}, 1, <, +, \{c\cdot\}_{c\in\mathbb{Q}})$. Specifically, σ has a constant symbol 1, binary function symbol $+$, binary relation symbol $<$, and an infinite family of unary function symbols $c\,\cdot$, indexed by $c \in \mathbb{Q}$.

Note that having a family of unary multiplication functions $\{c\,\cdot\,\}_{c\in\mathbb{Q}}$ is completely different from having a single binary multiplication function. Under the above definition σ-terms are essentially linear combinations of the the first-order variables, e.g., $\frac{1}{2}x + \frac{1}{3}y + z + \frac{5}{9}$ is a σ-term. On the other hand, incorporating binary multiplication in σ would lead to polynomial terms, such as $x^2y + z^4$.

Atomic formulas have the form $t_1 = t_2$ or $t_1 < t_2$ for σ-terms. Here are some assertions that can be formalized in linear arithmetic (where A denotes a matrix of rationals, $\boldsymbol{x}$ a vector of variables, and $\boldsymbol{b}$ a vector of rationals):

- 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 $C\boldsymbol{x} \leq \boldsymbol{d}$.

The statements above have a natural geometric interpretation. For example, the second statement asserts that the polygon $\{\boldsymbol{x} \in \mathbb{Q}^n : A\boldsymbol{x} \leq \boldsymbol{b}\}$ is a subset of the polygon $\{\boldsymbol{x} \in \mathbb{Q}^n : C\boldsymbol{x} \leq \boldsymbol{d}\}$.

Another important source of theories is from sets of axioms. Given a set of sentences $\mathcal{S}$, the set $\mathcal{T} = \{F : \mathcal{S} \models F\}$ is a theory. We call $\mathcal{S}$ a set of **axioms** for the theory $\mathcal{T}$. For example, if $\mathcal{S}$ comprises the group axioms then $\mathcal{T}$ is the theory of groups. Observe that the theory of groups is not complete: if m denotes the binary

multiplication operation then the theory of groups neither contains the sentence $\forall x\, \forall y\, (m(x,y) = m(y,x))$ nor its negation (some groups are abelian and other groups are non-abelian).

Here, in more detail, is another axiomatic theory, which we will explore below. Consider a signature with a single binary relation $<$. The theory $\mathcal{T}_{UDLO}$ of *unbounded dense linear orders* is the set of sentences entailed by the following set of axioms:

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

A theory $\mathcal{T}$ is **decidable** if there is an algorithm that, given a sentence F, determines whether or not $F \in \mathcal{T}$. We will show that the theory of unbounded dense linear orders and the theory of linear arithmetic over the rationals are both decidable.

An important technique to show that a theory is decidable is **quantifier elimination**. We say that a theory $\mathcal{T}$ admits quantifier elimination if for any formula $\exists x\, F$, with F quantifier-free, there exists a quantifier-free formula G with the same free variables as $\exists x\, F$ such that $\mathcal{T} \models \exists x\, F \leftrightarrow G$, that is, for any assignment $\mathcal{A}$ that is a model of $\mathcal{T}$, $\mathcal{A} \models \exists x\, F$ if and only if $\mathcal{A} \models G$. (It is worth emphasizing that quantifier elimination is defined on formulas that may have free variables.) We furthermore say that $\mathcal{T}$ has a **quantifier elimination procedure** if there is an algorithm to obtain G given F.

Example 1. Let $\mathcal{T}$ denote the theory of the structure $(\mathbb{R}, +, \cdot, 0, 1)$ and consider the formula $F := \exists x\, (ax^2 + bx + c = 0)$ in free variables a, b, c. This formula asserts that the quadratic equation $ax^2+bx+c = 0$ has a real solution. By the quadratic formula we have $\mathcal{T} \models F \leftrightarrow b^2 \geq 4ac$. As another example, consider the formula

$$F := (x_1 a + x_2 c = 1) \wedge (x_1 b + x_2 d = 0) \wedge (x_3 a + x_4 c = 0) \wedge (x_3 b + x_4 d = 1)\,.$$

F can be written

$$\begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

in matrix notation. Thus $\exists x_1 \exists x_2 \exists x_3 \exists x_4 F$ asserts that the matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

has a multiplicative inverse. Thus $\mathcal{T} \models \exists x_1 \exists x_2 \exists x_3 \exists x_4 F \leftrightarrow ad - bc \neq 0$.

The definition of quantifier elimination refers only to the existential quantifier. The universal quantifier can be handled using duality. Consider a formula $\forall x\, F$ with F quantifier-free. If a theory $\mathcal{T}$ has quantifier elimination then we can find a quantifier-free formula G such that $\mathcal{T} \models \exists x\, \neg F \leftrightarrow G$. But then $\mathcal{T} \models \forall x\, F \leftrightarrow \neg G$.

A theory $\mathcal{T}$ is decidable if it has a quantifier elimination-procedure and a procedure for determining whether or not $F \in \mathcal{T}$ for a variable-free quantifier-free formula F. Given an arbitrary sentence F, to determine whether $F \in \mathcal{T}$, first convert F to an equivalent formula in prenex normal form, and eliminate quantifiers from the inside out. In particular, if $\mathcal{T} \models \exists x\, F^* \leftrightarrow G$ then $\mathcal{T} \models Q_1 x_1 \ldots Q_n x_n Q x\, F^* \leftrightarrow Q_1 x_1 \ldots Q_n x_n\, G$, where $Q_i, Q \in \{\exists, \forall\}$.

Eventually one obtains a sentence F' such that $\mathcal{T} \models F \leftrightarrow F'$. Thus $F \in \mathcal{T}$ if and only if $F' \in \mathcal{T}$. But by assumption we have a procedure to decide this last membership query.

2 Unbounded Dense Linear Orders

Theorem 2. *The theory $\mathcal{T}_{UDLO}$ of unbounded dense linear orders is decidable.*

Proof. The main step of the proof is to show that $\mathcal{T}_{UDLO}$ has a quantifier-elimination procedure.

Consider a formula $\exists x\, F$, with F quantifier-free. We give a quantifier-free formula G with the same free variables as $\exists x\, F$ such that for any assignment $\mathcal{A}$ that is a model of $\mathcal{T}_{UDLO}$, $\mathcal{A} \models \exists x\, F$ if and only if $\mathcal{A} \models G$. The quantifier-elimination procedure has two phases: first we simplify the formula F through logical manipulations and then we show how to eliminate quantifiers within formulas in simplified form.

As a first step, we can convert F into a logically equivalent formula in DNF. We can moreover eliminate negative literals by replacing the subformula $\neg(x_i < x_j)$ with $x_i = x_j \vee x_j < x_i$ and replacing the subformula $\neg(x_i = x_j)$ with $x_i < x_j \vee x_j < x_i$.

Henceforth we assume that F is in DNF and negation-free. Now using the equivalence $\exists x\, (F_1 \vee F_2) \equiv \exists x\, F_1 \vee \exists x\, F_2$ it suffices that we be able to eliminate the quantifier $\exists x$ in case F is a conjunction of atomic formulas. Finally, using the equivalence $\exists x\, (F_1 \wedge F_2) \equiv \exists x\, F_1 \wedge F_2$ in case x is not free in F_2, it suffices that we be able to eliminate the quantifier $\exists x$ in case F is a conjunction of atomic formulas all of which mention x. Such formulas have the form $x = y$, $x < y$ or $y < x$ for some variable y.

For the final case above, we proceed as follows. If F contains a conjunct $x < x$ then we have $\mathcal{T}_{UDLO} \models \exists x\, F \leftrightarrow$ **false**. Otherwise, if F contains a conjunct $x = y$ for some other variable y then we have that $\mathcal{T}_{UDLO} \models \exists x\, F \leftrightarrow F[y/x]$.

If neither of the above applies then (after deleting conjuncts of the form $x = x$ if present) we can write F in the form

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

where the l_i and u_j are variables different from x. Now if $m = 0$, i.e., there are no lower bounds on x, then $\mathcal{T}_{UDLO} \models \exists x\, F \leftrightarrow$ **true** (since we're considering the theory of unbounded orders). Likewise if $n = 0$, i.e., there are no upper bounds on x, then $\mathcal{T}_{UDLO} \models \exists x\, F \leftrightarrow$ **true**. Otherwise, by density of the order relation, we have

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

Decidability of $\mathcal{T}_{UDLO}$ follows straightforwardly from the existence of a quantifier-elimination procedure. Starting from a sentence F, after eliminating all quantifiers from F we are left with a variable-free formula G such that $\mathcal{T} \models F \leftrightarrow G$. But G must be a propositional combination of **true** or **false**, and therefore logically equivalent to either **true** or **false**. □

The proof of Theorem 2 shows *inter alia* that $\mathcal{T}_{UDLO}$ is complete: given a sentence F, either F holds on all unbounded dense linear orders, or its negation holds on all unbounded dense linear orders. (After eliminating all quantifiers from a closed formula F one obtains either $\mathcal{T}_{UDLO} \models F \leftrightarrow$ **true** or $\mathcal{T}_{UDLO} \models F \leftrightarrow$ **false**.) In particular, $(\mathbb{Q}, <)$ and $(\mathbb{R}, <)$ satisfy the same first-order sentences.

You may recall that $(\mathbb{R}, <)$ is *Dedekind complete*: any non-empty set of reals that is bounded above has a least upper bound. This property fails for the rationals since, e.g., $\{x \in \mathbb{Q} : x^2 < 2\}$ has no least upper bound in the rationals. Evidently Dedekind completeness cannot be expressed in first-order logic in the language of linear orders.

3 Linear Rational Arithmetic

In the previous section we showed decidability of an axiomatic theory by quantifier elimination. In this section we use quantifier elimination to show decidability of the theory of a certain structure.

Theorem 3. $\mathrm{Th}(\mathbb{Q}, 1, <, +, \{c\,\cdot\,\}_{c\in\mathbb{Q}})$ *is decidable.*

Proof. We show that the above theory has a quantifier-elimination procedure. In this context quantifier elimination is sometimes called *Fourier-Motzkin elimination*.

Following the proof of Theorem 2, it suffices to show how to eliminate the quantifier $\exists x$ in $\exists x\, F$, where F is a conjunction of atomic formulas all of which mention x. Each such atomic formula has the form $t_1 = t_2$ or $t_1 < t_2$ for terms t_1 and t_2, where at least one of t_1 or t_2 mentions x. Using the multiplication operations $c\,\cdot$ we can equivalently render each atomic formula in the form $x = t$, $x < t$ or $t < x$ for some term t that does not mention x. For example, $5x + y < 2x - y + z$ is equivalent to $x < -\frac{2}{3}y + \frac{1}{3}z$.

Thus we can assume that F is written in the form

$$F = \bigwedge_{i=1}^{m} t_i < x \wedge \bigwedge_{j=1}^{n} x < s_j$$

where the terms t_i and s_j do not mention x.

If $m = 0$ or $n = 0$ then the formula $\exists x\, F$ is equivalent to **true** on the given structure (since $\mathbb{Q}$ is unbounded). Otherwise $\exists x\, F$ can equivalently be written

$$\bigwedge_{i=1}^{m} \bigwedge_{j=1}^{n} t_i < s_j\,.$$

This concludes the description of the quantifier elimination procedure.

Finally note that it is straightforward that any variable-free formula, which is a Boolean combination of formulas $t_1 = t_2$ and t_1, t_2 for closed terms t_1, t_2, simplifies to **true** or **false** on the structure in question. □

4 Presburger arithmetic

Our final decidability result in this lecture concerns the theory of the structure $(\mathbb{N}, 0, 1, +, <)$, which is commonly known as *Presburger arithmetic*.

Theorem 4. $\mathrm{Th}(\mathbb{N}, 0, 1, +, <)$ *is decidable.*

We show decidability of Presburger arithmetic by providing a quantifier-elimination procedure. In fact, $\mathrm{Th}(\mathbb{N}, 0, 1, +, <)$ as such does not have quantifier elimination since, e.g., the formula $\exists y\,(x = y + y)$ is not equivalent to a quantifier-free formula since it expresses that x is divisible by two, and we cannot express this property using only Boolean combinations of the atomic formulas of the structure $(\mathbb{N}, 0, 1, +, <)$. This motivates the extension of this structure by unary divisibility predicates $c \mid \cdot$ for any $c > 0$ such that $c \mid n$ is true if there exists a $k \in \mathbb{N}$ such that $n = k \cdot c$. Consequently, we will in the following show that the theory $(\mathbb{N}, 0, 1, +, <, \{c \mid \cdot\}_{c\in\mathbb{N}})$ admits quantifier elimination. In the following, we will write $a \cdot x$ in order to abbreviate the a-fold application of $+$.

As discussed above, it suffices to provide a quantifier elimination procedure for existential formulas whose matrix is a conjunction of atomic formulas. For Presburger arithmetic, we henceforth consider formulas of the form

$$F = \exists x \bigwedge_{i\in G} q_i(\vec{y}) < a_i \cdot x \wedge \bigwedge_{j\in L} a_j \cdot x < p_j(\vec{y}) \wedge \bigwedge_{k\in D} c_k \mid a_k \cdot x + r_k(\vec{y}) \wedge J, \tag{1}$$

where L, G, D are finite index sets, and q_i, p_j, r_k are linear polynomials in $\vec{y}$, e.g., $2 \cdot y_1 - 4 \cdot y_2 + 3$, and x does not occur in J. Strictly speaking, subtraction is not present in our theory, but we may use it intermediately since any formula involving subtraction of variables is equivalent to one which does not (since e.g. $2 \cdot y_1 - 4 \cdot y_2 + 3 < y_3$ is equivalent to $2 \cdot y_1 + 3 < y_3 + 4 \cdot y_2$). For simplicity, in the following we will assume that J is equivalent to *true*, i.e., that x occurs in all conjuncts of F.

Note that x occurs isolated in (1), but with different coefficients. Now set

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

where $b := 1$ if $G \cup L \cup D = \emptyset$. We have that F in (1) is equivalent to

$$H = \exists x \bigwedge_{i \in G} \frac{b}{a_i} \cdot q_i(\vec{y}) < x \wedge \bigwedge_{j \in L} x < \frac{b}{a_j} \cdot p_j(\vec{y}) \wedge \bigwedge_{k \in D} \frac{b}{a_k} \cdot c_k \mid x + \frac{b}{a_k} \cdot r_k(\vec{y}) \wedge b \mid x. \tag{2}$$

To see this, suppose $x \in \mathbb{N}$ is such that it satisfies (1). We claim that $b \cdot x$ satisfies (2). This is indeed easily seen for all atomic formulas except for the divisibility constraints in (1). But note that $c \mid a \cdot x + r$ for some $c, r \in \mathbb{N}$ if and only if there exists $k \in \mathbb{N}$ such that

$$\begin{aligned} & k \cdot c = a \cdot x + r \\ \iff & b \cdot k \cdot c = b \cdot a \cdot x + b \cdot r \\ \iff & \frac{b}{a} \cdot k \cdot c = b \cdot x + \frac{b}{a} \cdot r \\ \iff & \frac{b}{a} \cdot c \mid b \cdot x + \frac{b}{a} \cdot r. \end{aligned}$$

By the same argument, if x satisfies (2) then x/b satisfies (1). Let

$$c := \mathrm{lcm}\left\{b, \frac{b}{a_k} \cdot c_k : k \in D\right\}^{1},$$

where $c := 1$ if $D = \emptyset$. Let H' be H without $\exists x$. That is, $H = \exists x\, H'$. We now claim that H in (2) is equivalent to the following formula:

$$H'' = \begin{cases} \bigvee_{0 \le m < c} H'[m/x] & \text{if } G = \emptyset \\ \bigvee_{j \in G} \bigvee_{1 \le m \le c} H'[((b/a_j) \cdot q_j(\vec{y}) + m)/x] & \text{otherwise} \end{cases} \tag{3}$$

Let us consider the case $G = \emptyset$ first. If the divisibility constraints in H have a solution x, then they have a solution amongst $\{0, \ldots, c-1\}$. (Exercise: convince yourself that this is the case.) Since G is empty, such a solution is only constrained from above by the less-than constraints indexed by L in H', and hence we can just try out by brute-force all values for x between $\{0, \ldots, c-1\}$ in order to obtain an equivalent formula. Otherwise if $G \neq \emptyset$, then x can additionally be constrained from below by some greater-than constraint indexed by G. But then some term $((b/a_j) \cdot q_j(\vec{y}) + m)$ will be the largest amongst all others in a satisfying assignment, and hence we can use a long disjunction in order to "simulate" guessing which assignment is going to be the largest, and then additionally add some number in $\{1, \ldots, c\}$ giving the smallest solution, if it exists.

We close this lecture with an example showing that we can prove some elementary number theoretic statements in Presburger arithmetic.

Example 5. Let us consider the formula $F = \forall x\, \exists y\, (x = 2 \cdot y \vee x = 2 \cdot y + 1)$ expressing that every natural number is odd or even. We rewrite F as

$$F \equiv \forall x\, \exists y\, ((x < 2 \cdot y + 1 \wedge 2 \cdot y < x + 1) \vee (x < 2 \cdot y + 2 \wedge 2 \cdot y < x)).$$

[1] Thanks to Long Pham (Keble) who spotted a glitch in an earlier version of these notes, and in particular pointed out that $\mathrm{lcm}(m, n) \neq \mathrm{lcm}(m \cdot n, n)$ for arbitrary $m, n \in \mathbb{N}$.

We now eliminate y from the two disjuncts, call them F_1 and F_2, separately. We first isolate y and obtain

$$F_1 \equiv \exists y\,(x-1 < 2\cdot y \wedge 2\cdot y < x+1).$$

Let $b = \mathrm{lcm}(2,2) = 2$. We now have F_1 is equivalent to G_1 defined as

$$\begin{aligned} G_1 &= \exists y\,(\frac{2}{2}(x-1) < y \wedge y < \frac{2}{2}(x+1) \wedge 2 \mid y) \\ &\equiv \exists y\,(x-1 < y \wedge y < x+1 \wedge 2 \mid y). \end{aligned}$$

We can now eliminate y from G_1 and obtain an equivalent H_1 as follows (noting that there were no divisibility constraints in F_1 and hence $c = 2$):

$$\begin{aligned} H_1 &= ((x-1 < x-1+1) \wedge (x-1+1 < x+1) \wedge 2 \mid x-1+1) \\ &\qquad \vee ((x-1 < x-1+2) \wedge (x-1+2 < x+1) \wedge 2 \mid x-1+2) \\ &\equiv 2 \mid x \end{aligned}$$

Likewise, from F_2 we obtain $H_2 = 2 \mid x-1$. Consequently, F is equivalent to $H = \forall x\,((2 \mid x) \vee (2 \mid x-1))$. Now observe that $\neg(m \mid n) \equiv \bigvee_{1\le i<m} m \mid n+i$. Hence,

$$\forall x(2 \mid x \vee 2 \mid x-1) \equiv \neg\exists x\,(\neg(2 \mid x) \wedge \neg(2 \mid x-1)) \equiv \neg\exists x\,((2 \mid x+1) \wedge (2 \mid x)).$$

We now eliminate x from $(2 \mid x+1) \wedge (2 \mid x)$. This is immediate by replacing x by 0 and 1 according to the quantifier elimination procedure:

$$\begin{aligned} &\Big((2 \mid x+1) \wedge (2 \mid x)\Big)[0/x] \vee \Big((2 \mid x+1) \wedge (2 \mid x)\Big)[1/x] \\ &\quad \equiv \Big((2 \mid 0+1) \wedge (2 \mid 0)\Big) \vee \Big((2 \mid 1+1) \wedge (2 \mid 1)\Big) \\ &\quad \equiv \Big((2 \mid 1) \wedge (2 \mid 0)\Big) \vee \Big((2 \mid 2) \wedge (2 \mid 1)\Big) \\ &\quad \equiv \textbf{false}. \end{aligned}$$

Now $\neg$**false** $\equiv$ **true**, which shows that F is valid.

Admittedly, this is a lengthy proof for the simple statement that every natural number is odd or even. Still, the interesting part about it is that it goes through by mechanically following the rules of the quantifier elimination procedure for Presburger arithmetic.