Logic and Proof Hilary 2016

Decidable Theories

James Worrell

1 Theories

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

Fix a signature σ. A *theory* $\boldsymbol{T}$ is a set of sentences (closed formulas) that is closed under semantic entailment, i.e., if $\boldsymbol{T} \models F$ then $F \in \boldsymbol{T}$. 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 is *complete* if for any sentence F, either $F \in \mathrm{Th}(\mathcal{A})$ or $\neg F \in \mathrm{Th}(\mathcal{A})$. Clearly the theory of any particular structure is complete. The set of valid σ-formulas 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 $\boldsymbol{S}$, the set $\boldsymbol{T} = \{F : \boldsymbol{S} \models F\}$ is a theory. We call $\boldsymbol{S}$ a set of *axioms* for the theory $\boldsymbol{T}$. For example, if $\boldsymbol{S}$ comprises the group axioms then $\boldsymbol{T}$ 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 $\boldsymbol{T}_{UDLO}$ of *unbounded dense linear orders* is

the set of sentences entailed by the following set of axioms:

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

A theory $\boldsymbol{T}$ is *decidable* if there is an algorithm that, given a sentence F, determines whether or not $F \in \boldsymbol{T}$. 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 $\boldsymbol{T}$ 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 $\boldsymbol{T} \models \exists x \, F \leftrightarrow G$, that is, for any assignment $\mathcal{A}$ that is a model of $\boldsymbol{T}$, $\mathcal{A} \models \exists x \, F$ 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 $\boldsymbol{T}$ has a *quantifier elimination procedure* if there is an algorithm to obtain G given F.

Example 1. Let $\boldsymbol{T}$ 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 $\boldsymbol{T} \models F \leftrightarrow b^2 \geq 4ac$. 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 $\boldsymbol{T} \models \exists x_1 \exists x_2 \exists x_3 \exists x_4 F \leftrightarrow ad - bc = 0$.

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 $\boldsymbol{T}$ has quantifier elimination then we can find a quantifier-free formula G such that $\boldsymbol{T} \models \exists x \neg F \leftrightarrow G$. But then $\boldsymbol{T} \models \forall x \, F \leftrightarrow \neg G$.

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

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

2 Unbounded Dense Linear Orders

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

Proof. The main step of the proof is to show that $\boldsymbol{T}_{UDLO}$ 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 $\boldsymbol{T}_{UDLO}$, $\mathcal{A} \models \exists x\, F$ 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 $\boldsymbol{T}_{UDLO} \models \exists x\, F \leftrightarrow \mathbf{false}$. Otherwise, if F contains a conjunct $x = y$ for some other variable y then we have that $\boldsymbol{T}_{UDLO} \models \exists x\, F \leftrightarrow F[y/x]$.

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 $\boldsymbol{T}_{UDLO} \models \exists x\, F \leftrightarrow \mathbf{true}$ (since we're considering the theory of unbounded orders). Likewise if $n = 0$, i.e., there are no upper bounds on x, then $\boldsymbol{T}_{UDLO} \models \exists x\, F \leftrightarrow \mathbf{true}$. Otherwise, by density of the order relation, we have

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

Decidability of $\boldsymbol{T}_{UDLO}$ 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 $\boldsymbol{T} \models F \leftrightarrow G$. 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 $\boldsymbol{T}_{UDLO}$ 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 $\boldsymbol{T}_{UDLO} \models F \leftrightarrow \mathbf{true}$ or $\boldsymbol{T}_{UDLO} \models F \leftrightarrow \mathbf{false}$.) In particular, $(\mathbb{Q}, <)$ and $(\mathbb{R}, <)$ satisfy the same first-order sentences. (This finally answers Exercise 7 from the lecture introducing first-order logic.)

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.

The completeness of the theory $\boldsymbol{T}_{UDLO}$ is not surprising in view of the following result.

Proposition 3. Given two countable unbounded dense linear orderings $(A, <)$ and $(B, <)$, there is an order preserving bijection $f : A \to B$.

Proof. Let $a_1, a_2, \ldots$ and $b_1, b_2, \ldots$ be enumerations of the elements of A and B. We define new enumerations $a'_1, a'_2, \ldots$ and $b'_1, b'_2, \ldots$ such that for any pair of indices i and j, $a'_i < a'_j$ if and only if $b'_i < b'_j$. Having done this we define the function f by $f(a'_i) = b'_i$ for each $i = 1, 2, \ldots$.

We define the a'_i and b'_i by strong induction via a *back and forth* construction. Suppose we have defined $a'_1, \ldots, a'_n$ and $b'_1, \ldots, b'_n$. If n is even then we define a'_{n+1} to be the first element of the original enumeration $a_1, a_2, \ldots$ that does not appear among $a'_1, \ldots, a'_n$. We then define b'_{n+1} such that $a'_i < a'_{n+1}$ if and only if $b'_i < b'_{n+1}$ for $1 \leq i \leq n$. We can do this because $(B, <)$ is a dense linear order. On the other hand, if n is odd then we define b'_{n+1} to be the first element of the original enumeration $b_1, b_2, \ldots$ that does not appear among $b'_1, \ldots, b'_n$. We then define a'_{n+1} such that $a'_i < a'_{n+1}$ if and only if $b'_i < b'_{n+1}$ for $1 \leq i \leq n$. We can do this because $(A, <)$ is a dense linear order. Proceeding in this way, we obtain new enumerations $a'_1, a'_2, \ldots$ and $b'_1, b'_2, \ldots$ with the desired properties. □

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 4. $\mathrm{Th}(\mathbb{Q}, 1, <, +, \{c\,\cdot\,\}_{c \in \mathbb{Q}})$ 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 $t_1 < t_2$ 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 concerns the theory of the structure $(\mathbb{N}, 0, 1, +, <)$, sometimes called *Presburger arithmetic*. In this case the proof of decidability does not proceed via quantifier elimination, but instead exploits closure properties of the class of regular languages. In fact $\mathrm{Th}(\mathbb{N}, 0, 1, +, <)$ does not have quantifier elimination since, e.g., the formula $\exists y\,(x = y + y)$ is not equivalent to a quantifier-free formula

Recall that a *regular language* is a language accepted by a *nondeterministic finite automaton (NFA)*. Recall also that the class of regular languages is closed under intersection and complementation, and under direct and inverse images with respect to renaming functions. Amplifying the last two closure properties, recall that a renaming function is a map $f : \Sigma \to \Gamma$ between two alphabets. We extend such a function pointwise to a map $f : \Sigma^* \to \Gamma^*$ by defining $f(\sigma_1 \dots \sigma_m) = f(\sigma_1) \dots f(\sigma_m)$. Then given a regular language $L \subseteq \Gamma^*$, its *inverse image* $f^{-1}(L) = \{w \in \Sigma^* : f(w) \in L\}$ is also regular. Likewise given a regular language $L \subseteq \Sigma^*$, its *direct image* $f(L) = \{f(w) : w \in L\}$ is also regular.

Importantly the above closure properties are all effective. For example, let $A = (\Gamma, Q, Q_0, \Delta, F)$ be a NFA for a given language $L \subseteq \Gamma^*$, with set of states Q, initial states Q_0, final states F, and transition relation $\Delta \subseteq Q \times \Gamma \times Q$. Then, given a renaming map $f : \Sigma \to \Gamma$, an NFA for the inverse image $f^{-1}(L)$ is $B = (\Sigma, Q, Q_0, \Delta', F)$, with transition relation Δ' given by $\Delta' = \{(p, \sigma, q) : (p, f(\sigma), q)\Delta\}$. We leave an an exercise the straightforward proof that this construction does the job.

Theorem 5. $\mathrm{Th}(\mathbb{N}, 0, 1, +, <)$ is decidable.

Proof. It will suffice to show that $\mathrm{Th}(\mathbb{N}, +)$ is decidable, since any formula over the richer signature can be rewritten to a formula using only $+$ (and equality) that defines the same property on $\mathbb{N}$. (We leave it as an exercise to check this.)

Consider a quantifier-free formula F that mentions variables $x_1, \dots, x_n$. We show how to define an automaton A_F over the alphabet of n-dimensional bit vectors

$$\Sigma_n = \left\{ \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \dots, \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} \right\}$$

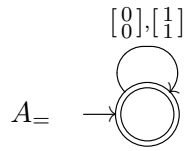
whose language is in one-to-one correspondence with the set of values of the free variables $x_1, \dots, x_n$ that satisfy F. Here each natural number is encoded in binary, with the value for x_i represented in the i-th component of each tuple in Σ_n. For example, the valuation $x_1 = 1, x_2 = 4, x_3 = 9$ is encoded by the word

$$\begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

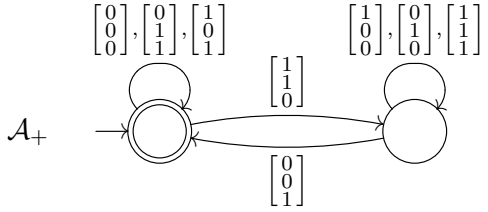
where the least significant bits occur on the left. Note that Σ_0 is a singleton set consisting of the empty vector $\{[]\}$ (the only 0-dimensional bit vector).

The construction of A_F is predicated on the following two *basic automata*.

We have the following one-state automaton $A_=$ over the alphabet Σ_2, corresponding to the equality relation $x_1 = x_2$:



And we have the a two-state automata A_+ over the alphabet Σ_3, corresponding to the addition function $x_1 + x_2 = x_3$:



We now define the automaton A_F by induction on the structure of the formula F. The construction proceeds from the atoms $A_=$ and A_+ using only the closure properties of the class of regular languages.

Base cases: Suppose F is the formula $x_i = x_j$. Then the automaton A_F is defined to be automaton whose language is $\pi^{-1}(L(A_=))$, where $\pi : \Sigma_n \to \Sigma_2$ is the projection map

$$\pi : \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \mapsto \begin{bmatrix} x_i \\ x_j \end{bmatrix}$$

Likewise, if F is the formula $x_i + x_j = x_k$, then A_F is defined to be an automaton whose language is $\pi^{-1}(L(A_+))$, where $\pi : \Sigma_n \to \Sigma_3$ is the projection map

$$\pi : \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \mapsto \begin{bmatrix} x_i \\ x_j \\ x_k \end{bmatrix}$$

Case: $F = F_1 \wedge F_2$. Then we define A_F to be an automaton whose language is $L(A_{F_1}) \cap L(A_{F_2})$.

Case: $F = \neg G$. Then we define A_F to be the automaton with language $\Sigma_n^* \setminus L(A_G)$.

This completes the definition of the automaton A_F corresponding to a quantifier-free formula F. Now consider a sentence $Q_1 x_1 \dots Q_n x_n F$ in prenex form. For $k = 0, \dots, n$, we write $F_k := Q_{k+1} x_{k+1} \dots Q_n x_n F^*$ and define a corresponding automaton A_k over alphabet Σ_k such that A_k accepts the set of values of the variables $x_1, \dots, x_k$ that satisfy F_k. In particular, an invariant of this construction is that A_k has non-empty language if and only if formula F_k is satisfiable.

We start by defining A_n to be the automaton A_F, as constructed above.

Now suppose that $F_{k-1} = \exists x_k F_k$. By induction we have an automaton A_k on alphabet Σ_k corresponding to F_k. Then we define A_{k-1} to be an automaton whose language is $\pi(L(A_k))$, where $\pi : \Sigma_k \to \Sigma_{k-1}$ is the map the projects out the k-th coordinate of each tuple in Σ_k.

Finally we handle the universal quantifier $\forall x_k$ by treating it as shorthand for $\neg \exists x_k \neg$.

We end up with an automaton A_0 for the sentence F_0 (which is $Q_1 x_1 \dots Q_n x_n F$) over the alphabet Σ_0. This automaton has non-empty language if and only if $(\mathbb{N}, +)$ satisfies F_0. $\square$