MATHEMATICAL LOGIC FOR COMPUTER SCIENCE (A.Y. 20/21)

HANDOUT N. 5

Abstract. Theories. Logical consequence. The theory of dense linear orders without end-points. The Back-and-Forth method. All countable dense linear orders without end-points are isomorphic to $(\mathbb{Q}, \leq)$.

1. Theories, Logical Consequence

If we look back at the proof of quantifier elimination for $Th(\mathcal{Q})$ we can observe that we used a handful of particular properties of the rationals along with a handful of specific logical laws. In particular, regarding $(\mathbb{Q}, \leq)$ we only used the following:

- $(\mathbb{Q}, \leq)$ has no left or right endpoint.
- $(\mathbb{Q}, \leq)$ is a dense linear ordering.

If happens that these properties can be easily expressed in the very language of orders, i.e., in $\mathcal{L} = \{\leq\}$. This can be done as follows, where we use $x < y$ as an abbreviation for $(x \leq y \land \neg(x = y))$.

(1) (A1 - Reflexivity) $\forall x(x \leq x)$.
(2) (A2 - Transitivity) $\forall x\forall y\forall z(x \leq y \land y \leq z \to x \leq z)$.
(3) (A3 - Antisimmetry) $\forall x\forall y((x \leq y \land y \leq x) \to y = x)$.
(4) (A4 - Totality) $\forall x\forall y(x \leq y \lor x \leq y)$.
(5) (A4 - No right end-point) $\forall x\exists y(x < y)$.
(6) (A5 - No left end-point) $\forall x\exists y(y < x)$.
(7) (A6 - Density) $\forall x\forall y(x < y \to \exists z(x < z \land z < y))$.

Let's call this finite set of sentences **DLO**.

Definition 1.1 (Theory)**.** A set of sentences is called a *theory*.

Looking back at the quantifier-elimination proof for $Th(\mathcal{Q})$ it is very easy to realize that everything we did worked not only for the particular structure $\mathcal{Q}$ but, more generally, for any structure $\mathfrak{A} = (A, \leq^{\mathfrak{A}})$ such that $\mathfrak{A} \models$ **DLO** (we call any such structure a *model of* **DLO**). This intrinsic generality of the proof is a ubiquitous phenomenon in Maths and CS.

To be precise, the proof works if we replace $\mathcal{Q}$-equivalence with the following notion of **DLO**-equivalence:

We say that two formulas F and G are **DLO**-equivalent (or equivalent modulo **DLO**) if they are equivalent in all models of **DLO**, i.e., for any $\mathfrak{A}$, if $\mathfrak{A} \models$ **DLO** then $\mathfrak{A} \models F \leftrightarrow G$.

Thus, the quantifier-elimination proof actually shows the following.

Notes by Lorenzo Carlucci, please report typos or errors to lorenzo.carlucci@uniroma1.it.

Quantifier Elimination for DLO

There exists an algorithm for transforming any formula $F(x_1, \ldots, x_n)$ in a **DLO**-equivalent quantifier-free formula $F'(x_1, \ldots, x_n)$ with no new free variables.

1.1. **Logical Consequence.** It is obvious that the notion of **DLO**-equivalence relates the set of sentences **DLO** with the formula $(F \leftrightarrow G)$, since it is based on a universal quantification over all models of **DLO**. So it makes sense to express it in this way. This motivates the following very basic definition.

Definition 1.2 (Logical Consequence - for sentences)**.** Let T be a a theory and S be a sentence, both in a given language $\mathcal{L}$. We say that T *logically implies* S if for all structures $\mathfrak{A}$ adequate for $\mathcal{L}$, if $\mathfrak{A} \models T$ then $\mathfrak{A} \models S$. We write in this case

$$T \models S$$

and say that S is a *logical consequence* of T.

In the particular case that $T = \{G_1, \ldots, G_n\}$ we write $T_1, \ldots, T_n \models S$ instead of $\{T_1, \ldots, T_n\} \models S$. We denote the set of logical consequences of a given theory T by $Th(T)$ or $Conseq(T)$.

Logical consequence is a crucial notion in Logic. It captures any situation in which we have an initial body of knowledge (expressed by a set of sentences – i.e., a theory) and a sentence containing new information that is necessarily implied by assuming the given body of knowledge. This idea captures a large number of mathematical, scientific and practical situations.

The notion of logical consequence can be defined also for formulas rather than sentences and is in some cases useful.

Definition 1.3 (Logical Consequence - for formulas)**.** Let Γ be a set (finite or infinite) of formulas and F be a formula. We say that Γ logically implies F if for all adequate structures $\mathfrak{A}$, for all assignment α in $\mathfrak{A}$, we have that if $\mathfrak{A} \models \Gamma[\alpha]$ then $\mathfrak{A} \models F[\alpha]$. We write $\Gamma \models F$ in this case and say that F is a logical consequence of Γ.

It is very easy to observe that the definition of logical consequence for sentences is a particular case of the definition of logical consequence for formulas.

1.2. **Complete theories.** Since $\mathcal{Q}$ is a single structure, the theory $Th(\mathcal{Q})$ has a particularly interesting property: for any sentence S, either $S \in Th(\mathcal{Q})$ or $\neg S \in Th(\mathcal{Q})$, and not both. This is so since being in $Th(\mathcal{Q})$ just means being true in $\mathcal{Q}$ and for any sentence S we have either $\mathcal{Q} \models S$ or $\mathcal{Q} \models \neg S$, and not both.

It we generalize this notion to any theory T we obtain the concept of a (semantically) **complete theory**.

For example, let's consider $Th(\mathbf{DLO}) := \{S : \mathbf{DLO} \models S\}$, that is the set of all and only the logical consequences of the axioms **DLO**. To say that this theory is complete means that for any sentence S, either $S \in Th(\mathbf{DLO})$ or else $\neg S \in Th(\mathbf{DLO})$ (and not both). Unwinding the definition this means: For any sentence S,

(1) Either S is true in **all models** of **DLO**, or else
(2) $\neg S$ is true in **all models** of **DLO**.

This in general is not a dichotomy, since it is conceivable that for some sentence S there exists a model $\mathfrak{A}$ of **DLO** such that $\mathfrak{A} \models S$ and another model $\mathfrak{B}$ of **DLO** such that $\mathfrak{B} \models \neg S$.

In general an incomplete theory is not a problem – for example we don't even expect that the theory of groups is complete, since some groups are commutative and others are not. But we can reasonable expect to get a complete theory if our aim is that of describing a particular structure, as, for example, $\mathcal{Q}$. So it's reasonable to ask how good **DLO** is in this respect.

In the particular case at hand, the quantifier elimination proof for **DLO** answers the question, showing that $Th(\mathbf{DLO})$ is both decidable and complete.

The point is that our quantifier-elimination procedure transformed an arbitrary sentence into a **DLO**-equivalent quantifier-free sentence in the language of orders, and formulas of the latter type are Boolean combinations of $\perp$ and $\top$. Such formulas are true or false independently of the model in which we evaluate them. Therefore any sentence S in the language of order is a logical consequence of **DLO** if and only if the quantifier-free equivalent S' obtained by our procedure is true (absolutely).

This implies that all models of **DLO** satisfy exactly the same sentences, i.e. all and only those that are transformed to a true boolean combination of $\top$ and $\perp$ by our quantifier-elimination procedure! The fancy name for two models satisfying exactly the same sentences is that they are **elementarily equivalent**. In particular we have that

$$\mathsf{DLO} \models S \text{ if and only if } \mathcal{Q} \models S.$$

Therefore the theories $Th(\mathcal{Q})$ and $Th(\mathsf{DLO})$ coincide.

Corollary 1.4. $Th(\mathcal{Q}) = Th(\mathsf{DLO})$. *The theory is both decidable and complete.*

Note however that this is not a general situation! The theory of all consequences of some theory T can have effective quantifier elimination without this implying that T is complete. This is because the truth of the quantifier-free sentences to which we reduce arbitrary sentences can vary with the model we consider.

2. Isomorphic Structures. Back-and-Forth method.

Isomorphism is a fundamental concept in Mathematics and Computer Science. Essentially it captures the idea that two structures are the same, except for a renaming of their objects and relations.

If two structures are similar in this sense, then we essentially identify them, because they are undistinguishable in all respects of interest.

The formal definition is as follows.

Definition 2.1 (Isomorphism)**.** Let $\mathfrak{A}, \mathfrak{B}$ be structures for the same language $\mathcal{L}$. $\mathfrak{A}$ is isomorphic to $\mathfrak{B}$ (denoted $\mathfrak{A} \simeq \mathfrak{B}$ if and only if There exists a map $h : A \to B$ such that h is a bijection, such that the following points hold:

(1) For each n-ary relation symbol R in the language, for each $(a_1, \ldots, a_n) \in A^n$,

$$\mathfrak{A} \models R(x_1, \ldots, x_n)[a_1, \ldots, a_n] \Leftrightarrow \mathfrak{B} \models R(x_1, \ldots, x_n)[h(a_1), \ldots, h(a_n)],$$

i.e.

$$(a_1, \ldots, a_n) \in R^{\mathfrak{A}} \Leftrightarrow (h(a_1), \ldots, h(a_n)) \in R^{\mathfrak{B}}.$$

(2) For each constant symbol c in the language,

$$h(c^{\mathfrak{A}}) = c^{\mathfrak{B}},$$

(3) For each n-ary function symbol f in the language, for every $(a_1, \ldots, a_n) \in A^n$,

$$h(f^{\mathfrak{A}}(a_1, \ldots, a_n)) = f^{\mathfrak{B}}(h(a_1), \ldots, h(a_n)).$$

(We say in this case that h commutes with the function symbol f).

For example two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ (with $E_i \subseteq V_i^2$) are isomorphic as structures for the language of graphs iff there existsd a bijections between the set of vertices V_1 of G_1 and the set of vertices V_2 of G_2 such that for all $(a, b) \in V_1^2$,

$$(a, b) \in E_1 \Leftrightarrow (h(a), h(b)) \in E_2,$$

i.e. any pair of vertices is connected by an edge in G_1 iff its image under h is connected by an edge in G_2.

It is easily observed that the structure $\mathcal{Q} = (\mathbf{Q}, <)$ where $\mathbf{Q}$ are the rationals and $<$ is the natural order on the rationals is a model of **DLO**. Similarly, $\mathcal{R} = (\mathbf{R}, <)$ is a model of **DLO**, where $\mathbf{R}$ is the set of real numbers and $<$ is the usual ordering of $\mathbf{R}$. This tells us right away that **DLO** does not characterize $\mathcal{Q}$ up to isomorphism, since $\mathbf{R}$ is uncountable while $\mathbf{Q}$ is countable. So we cannot say, by reasons of cardinality, that any two models of **DLO** are isomorphic.

We will see that, however, cardinality is the only reason why **DLO** fails to capture $\mathcal{Q}$ up to isomorphism. In fact, we will prove that all *countable* models of **DLO** are *isomorphic*. That is, if $\mathfrak{A} \models \mathsf{DLO}$ and $\mathfrak{B} \models \mathsf{DLO}$ and $\mathfrak{A}$ and $\mathfrak{B}$ are countable structures, then there exists a bijection f between A and B such that for every $a, a' \in A$,

$$\mathfrak{A} \models a < a' \Leftrightarrow \mathfrak{B} \models f(a) < f(a').$$

It is easily observed that two isomorphic models satisfy the same set of sentences (Exercise).

The proof is established by a method called Back-and-Forth, which is quite general.

Theorem 2.2. *Let $\mathfrak{A}$ and $\mathfrak{B}$ be countable models of* DLO*. Then $\mathfrak{A} \simeq \mathfrak{B}$..*

Proof. Let $\mathfrak{A} = (A, \leq^{\mathfrak{A}})$ and $\mathfrak{B} = (B, \leq^{\mathfrak{B}})$ with A and B countable. Fix a list with no repetitions of A, $(a_0, a_1, a_2, a_3, \dots)$ and a list with no repetitions of B, $(b_0, b_1, b_2, b_3, \dots)$. We define recursively a list $(p_0, p_1, p_2, \dots)$ with no repetition and a list $(q_0, q_1, q_2, \dots)$ with no repetition such that the map

$$p_i \mapsto q_i$$

is an isomorphism between $\mathfrak{A}$ and $\mathfrak{B}$.

We start by setting $p_0 = a_0$ and $q_0 = b_0$.

For the inductive step consider a generic n and assume that $p_0, p_1, \dots, p_n$ and $q_0, q_1, \dots, q_n$ have been defined. The exact inductive hypothesis we need on these values will be clear from the proof.

We distinguish two cases.

(Case 1) n is even. Pick an element p_{n+1} in $A \setminus \{p_0, \dots, p_n\}$ with least index in the list $(a_0, a_1, a_2, \dots)$. We compare this element to the elements already picked. We have three cases.

(Case 1.1) For all $m \leq n$, $p_{n+1} <^{\mathfrak{A}} p_m$. In this case pick a q_{n+1} in B such that for all $m \leq n$ we have $q_{n+1} <^{\mathfrak{B}} q_m$. This element exists because $\mathfrak{B}$ satisfies the axioms saying that there are no left end-points.

(Case 1.2) For all $m \leq n$, $p_{n+1} >^{\mathfrak{A}} p_m$. In this case pick a q_{n+1} in B such that for all $m \leq n$ we have $q_{n+1} >^{\mathfrak{B}} q_m$. Such an element exists because $\mathfrak{B}$ satisfies the axioms saying that there are no right end-points.

(Case 1.3) The first two cases do not apply. Then there exist $i, j \leq n$, $i \neq j$ such that $p_i <^{\mathfrak{A}} p_{n+1} <^{\mathfrak{A}} p_j$ and there are no other elements of $\{p_0, p_1, \dots, p_n\}$ in the interval $[p_i, p_j]$ in $\mathfrak{A}$. Then pick an element q_{n+1} in B such that $q_i <^{\mathfrak{B}} q_{n+1} <^{\mathfrak{B}} q_j$. Such an element exists since $\mathfrak{B}$ satisfies the density axiom. In particular: So $\mathfrak{B} \models (x < y \to \exists z(x < z \land z < y)[\binom{x,y}{q_i,q_j}]$. By inductive hypothesis we can be sure that $q_i <^{\mathfrak{B}} q_j$, so that $\mathfrak{B} \models \exists z(x < z \land z < y)[\binom{x,y}{q_i,q_j}]$ and therefore there exists a $q \in B$ witnessing the existential. This q is necessarily distinct from the previously chosen $q_0, \dots, q_n$ and we can select it as our q_{n+1}.

(Case 2) n is odd. In this case we do the same thing but starting with an element $q_{n+1} \in B \setminus \{q_0, \dots, q_n\}$.

It is easy to show that the map defined by $p_i \mapsto q_i$ is an isomorphism between $\mathfrak{A}$ and $\mathfrak{B}$.

□

Corollary 2.3. *Any countable model of* DLO *is isomorphic to $\mathcal{Q} = (\mathbf{Q}, \leq)$.*

Corollary 2.4. *The theory of countable dense linear orders without end-points is complete.*

The fancy name to express the fact that all countable models of DLO are isomorphic is to say that DLO is an ω-categorical (or $\aleph_0$-categorical) theory.