An Excursion Into Model Theory and Its Applications; Lectures 1

Ulla Karhumäki

University of Helsinki

LMS online course Fall 2020

Lecture 0

Introduction

What is model theory?

- Model theory concerns the interplay between mathematical structures (e.g. groups, fields, rings, graphs, ordered sets...) and the *first-order language* which is used to describe these structures.
  - A study of *definable sets* = *solution sets of first-order formulas* in a structure.
    - Example: $D = \{x \in \mathbb{Q} \mid x \neq 0 \wedge \exists y . y \cdot y = x\}$ is a definable set in $\mathbb{Q}$ defined by a first order formula $x \neq 0 \wedge \exists y . y \cdot y = x$.
- Benefit #1: transfer results across structures.
  - Some structures are indistinguishable by first order formulas (e.g. fields $\mathbb{Q}^{\mathrm{alg}}$, $\mathbb{C}$). Thus, if a result can be encoded in a formula, proving it in one structure also proves it in many others (e.g. Lefschetz principle).
- Benefit #2: results about definable sets can be very general.
  - Hope: describe *all* definable sets in a given structure.
    - Hopeless in general: a priori, definable sets can be *anything*. Instead: identify classes of 'tame' structures where definable sets can be controlled in some way.
  - Typical examples of tameness:
    1. Definable sets can be defined with simple formulas (e.g. no quantifiers).
    2. Definable sets have invariants (e.g. dimension).
    3. Existence of algorithms to decide (e.g. to decide whether a definable set is empty.)

Lecture 1

First-order languages and structures

Languages

- Not every formula makes sense in every structure (e.g. "$\exists y . y \cdot y = x$" makes sense in a field but not in a vector space).
- A language specifies which symbols are defined in a given structure and hence will appear in a formula.

Definition 1.1. A language is a set $L = \{R_1, R_2, \ldots, f_1, f_2, \ldots, c_1, c_2, \ldots\}$ of relation symbols R_i, function symbols f_j, and constant symbols c_k. Relation and function symbols have arities $n_i, m_j \in \mathbb{N}$.

Examples 1.2.

- $L_{\mathrm{group}} := \{1, \cdot, ^{-1}\}$, the language of *groups*: 1 is a constant symbol, $\cdot$ is a binary function symbol and $^{-1}$ is a unary function symbol.
- $L_{\mathrm{ag}} := \{0, +, -\}$, the language of *abelian groups*: 0 is a constant symbol, $+$ is a binary function symbol, $-$ is a unary function symbol.
- $L_{\mathrm{ring}} := L_{\mathrm{ag}} \cup \{1, \cdot\}$, the language of *rings*: 1 is a constant symbol, $\cdot$ is a binary function symbol.
- $L_{\mathrm{graph}} := \{E\}$, the language of *graphs*: E is a binary relation symbol.
- $L_{\mathrm{ord}} := \{<\}$, the language of *ordered sets*: $<$ is a binary relation symbol.
- $L_{\mathrm{oag}} := L_{\mathrm{ag}} \cup L_{\mathrm{ord}}$, the language of *ordered abelian groups*.
- $L_{\mathrm{oring}} := L_{\mathrm{ring}} \cup L_{\mathrm{ord}}$, the language of *ordered rings*.

Structures

- An L-structure specifies the *meaning* of the symbols in the language L.

Definition 1.3. An L-structure is a set M, (domain or universe), with:

- For each n-ary relation symbol R in L, a subset $R^M \subseteq M^n$.
- For each m-ary function symbol f in L, a function $f^M \colon M^m \to M$.
- For each constant symbol c in L, an element $c^M \in M$.

R^M, f^M, c^M are called the interpretations of R, f, c in M.
Most of the time, we write f and R instead of f^M and R^M.

Warning: we denote by M both the domain and the L-structure.

Example 1.4. Any group is naturally an L_{group}-structure, any ring with unit is naturally an L_{ring}-structure, etc.

Example 1.5. $\mathbb{Z}$ is naturally an $L_{\mathrm{oag}} = \{0, +, -, <\}$-structure:

- The interpretation $0^{\mathbb{Z}}$ of the symbol $0 \in L_{\mathrm{ag}}$ is the usual 0 of $\mathbb{Z}$.
- The interpretation $+^{\mathbb{Z}}$ of $+ \in L_{\mathrm{oag}}$ is addition, i.e. $(x, y) \mapsto x + y$ for $x, y \in \mathbb{Z}$.
- The interpretation $-^{\mathbb{Z}}$ of $- \in L_{\mathrm{oag}}$ is the map $x \mapsto -x$.
- The interpretation $<^{\mathbb{Z}}$ of $<$ is the set $\{(a, b) \in \mathbb{Z}^2 \mid a < b\}$.

Warning: do not confuse $+$ the *symbol* in L_{oag} with $+$ the *function* $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$.

Substructures

Definition 1.6. Let L be a language and M be an L-structure. A subset $N \subseteq M$ is an L-substructure if it contains c^M for all constant symbols $c \in L$ and if it is closed under f^M for all function symbols $f \in L$.
Note: such an N is an L-structure in a natural way.
Most of the time we simply write substructure instead of L-substructure.

Note: if the language L has no constant symbol, then the empty set is the domain of a substructure of an L-structure M.

Examples 1.7.
- A substructure of a group G, seen as an L_{group}-structure, is a subgroup. Remember that the notion of substructure is sensitive to the language! E.g. an $L = \{1, \cdot\}$-substructure of a group G, seen as an L-structure, is a submonoid of G containing 1^G and an $L = \{\cdot\}$-substructure of a group G, seen as an L-structure, can be empty.
- A substructure of a field F, seen as an L_{ring}-structure, is a subring.

Example 1.8. Let $L_{\mathrm{nuring}} = L_{\mathrm{ring}} \setminus \{1\}$ and look at $\mathbb{Z}$ as an L_{nuring}-structure. Its substructures are $k\mathbb{Z}$ for $k \in \mathbb{Z}$: they contain 0 and are closed under $+, -, \cdot$.

Homomorphisms & embeddings

Definition 1.9. Map $h : M \to N$ between two L-structures is a homomorphism if

1. $h(c^M) = c^N$ for all constant symbols $c \in L$,
2. $h(f^M(a_1, \dots, a_n)) = f^N(h(a_1), \dots, h(a_n))$ for all function symbols $f \in L$ and $a_1, \dots, a_n \in M$,
3. if $(a_1, \dots, a_m) \in R^M$ then $(h(a_1), \dots, h(a_m)) \in R^N$ for all relation symbols $R \in L$ and $a_1, ..., a_m \in M$.

An injective homomorphism $\eta : M \to N$ is an L-embedding if in addition $(a_1, \dots, a_m) \in R^M \Leftrightarrow (\eta(a_1), \dots, \eta(a_m)) \in R^N$.
A bijective L-embedding is an L-isomorphism and an L-isomorphism $i : M \to M$ is an L-automorphism.
We often drop the L-prefix and just write embedding, isomorphism, etc.

Examples 1.10.
- An L_{group}-homomorphism of groups G and H, seen as L_{group}-structures, is just a homomorphism of groups.
- An L_{ord}-homomorphism of L_{ord}-structures M and N is an order-preserving map.

Example 1.11. If $N \subseteq M$ and the inclusion map is an L-embedding then N is a substructure of M.

Formulas, informally

- Examples:
  1. "$x = 0 \vee \neg\exists y : y + y = x$" is an L_{ag}-formula on x (e.g. in $\mathbb{Z}$ it says "x is either 0 or x is odd".
  2. "$\forall x : (x > 0 \to \exists y : y \cdot y = x)$" is an L_{oring}-formula which does not depend on a variable. Therefore it is either true or false in a structure (e.g. true in $\mathbb{R}$ but false in $\mathbb{Q}$).
- Informally, a first order L-formula is a syntactically correct finite string build using:
  1. symbols of the language L,
  2. symbols for variables,
  3. equality symbol $=$; logical connectives $\vee$, $\wedge$ and $\neg$; quantifiers $\forall$ and $\exists$ and parentheses $($, $)$.

Terms & formulas

Let L be a language and $\overline{x} = (x_1, \ldots, x_n)$ be a tuple of variables.

Definition 1.12. An L-term in $\overline{x}$ is one of the following:

- a variable x_i for some $i = 1, \ldots, n$;
- a constant symbol $c \in L$;
- $f(t_1, \ldots, t_m)$ where $f \in L$ is an m-ary function symbol and t_1, …, t_m are L-terms in $\overline{x}$.

Example 1.13. $0 + x$ is an L_{ag}-term in x; $1 + (x \cdot y)$ is an L_{ring}-term in (x, y).

Definition 1.14. An L-formula in $\overline{x}$ is one of the following:

- atomic: $t_1 = t_2$ where t_1, t_2 are L-terms in $\overline{x}$, or $R(t_1, \ldots, t_n)$ where $R \in L$ is an n-ary relation symbol and t_1, …, t_n are L-terms in $\overline{x}$;
- $\phi \wedge \psi$, $\phi \vee \psi$, $\neg\phi$ where ϕ, ψ are L-formulas in $\overline{x}$;
- $\exists y.\phi$, $\forall y.\phi$ where y is a variable and ϕ is an L-formula in $\overline{x}y$.

An L-formula is an L-sentence if $\overline{x} = \varnothing$ (i.e. $n = 0$).

Examples 1.15. $x + y < 1$ is an atomic L_{oring}-formula in (x, y); $\forall x.x = x$ is a sentence (in any language!); $\forall x.\exists y.y \cdot y = x$ is an L_{ring}-sentence.

Some notation about terms & formulas

- If ϕ is a formula in $\overline{x}$ we often write $\phi(\overline{x})$; similarly for terms.
- We shall often use many abbreviations in notation:
  - $\phi \to \psi$ in place of $(\neg\phi) \vee \psi$;
  - $\phi \leftrightarrow \psi$ in place of $(\phi \to \psi) \wedge (\psi \to \phi)$;
  - $t_1 \neq t_2$ in place of $\neg t_1 = t_2$;
  - $\top$ is any formula which is always true (e.g. $\forall x : x = x$).
  - $\bot = \neg\top$ is always false.
  - for well understood symbols:
    - $t_1 \leq t_2$ in place of $t_1 < t_2 \vee t_1 = t_2$;
    - $t_1 + t_2$ in place of the more accurate "$+(t_1, t_2)$";
    - $t_1 \not< t_2$ in place of $\neg t_1 < t_2$ ...
- We add parentheses where appropriate to prevent ambiguities:
  - $(1 + x) \cdot x$ and $1 + (x \cdot x)$ are different terms;
  - $(\bot \vee \top) \wedge x = y$ and $\bot \vee (\top \wedge x = y)$ are different formulas.
- Some more dangerous shortcuts:
  - if $\cdot \in L$, xy in place of $x \cdot y$, x^2 in place of $x \cdot x$, and similarly $x^3 \ldots$ (but not x^y!);
  - if $+ \in L$ and $\cdot \notin L$, $2x$ in place of $x + x$, and similarly $3x \ldots$ (but not xy!).

Interpretation of formulas

An L-formula can be naturally interpreted in an L-structure M. E.g. interpreting L_{ag}-formula $\psi(x) = \exists y : 2y = x$ in $\mathbb{Z}$, we may ask for which $n \in \mathbb{Z}$ it is true.

Definition 1.16. Given an L-term $t(x_1, \ldots, x_n)$, its interpretation $t^M(\bar{a})$ is:

- $t^M(\bar{a}) := a_i$, if $t = x_i$;
- $t^M(\bar{a}) := c^M$, if $t = c$ for some constant $c \in L$;
- $t^M(\bar{a}) := f^M(t_1^M(\bar{a}), \ldots, t_m^M(\bar{a}))$, if t is $f(t_1, \ldots, t_m)$.

Example 1.17. Let t be $x + y$: then $t^{\mathbb{Q}}(2, 4) = 6$, $t^{\mathbb{Z}/5\mathbb{Z}}(\bar{2}, \bar{4}) = \bar{1}$.

Definition 1.18. Given an L-formula $\phi(x_1, \ldots, x_n)$, we write $M \models \phi(\bar{a})$ when:

- ϕ is $t_1 = t_2$ and $t_1^M(\bar{a}) = t_2^M(\bar{a})$;
- ϕ is $R(t_1, \ldots, t_m)$ and $(t_1^M(\bar{a}), \ldots, t_m^M(\bar{a})) \in R^M$;
- ϕ is $\neg\psi$ and $M \not\models \psi(\bar{a})$; ϕ is $\psi_1 \wedge \psi_2$ and $M \models \psi_i(\bar{a})$ for both $i = 1, 2$; similarly for $\psi_1 \vee \psi_2$
- ϕ is $\exists y.\psi(\bar{x}, y)$ and there is $b \in M$ with $M \models \psi(\bar{a}, b)$; similarly for $\forall y.\psi(\bar{x}, y)$.

$M \models \phi(\bar{a})$ says "$\phi(\bar{a})$ holds in M" and, if ϕ is a sentence, "M is a model of ϕ".

Example 1.19. Let ϕ be $\exists y.(y \cdot y = x)$. Then $\mathbb{Z} \models \phi(9)$ but $\mathbb{Z} \not\models \phi(8)$; Let ψ be $\forall x.(x = 0 \vee \exists y.xy = 1)$. Then $\mathbb{Z} \not\models \psi$ and $\mathbb{Q} \models \psi$.

Definable sets and parameters

Definition 1.20. Let M be an L-structure. A set $D \subseteq M^n$ is said to be definable if there is an L-formula $\phi(\bar{x}, \bar{y})$ and parameters $\bar{b}$ from M such that

$$D = \phi(M, \bar{b}) := \{\bar{a} \in M^n : M \models \phi(\bar{a}, \bar{b})\}.$$

If $\bar{b}$ may be taken from $B \subseteq M$, we say that D is B-definable. In particular, $\emptyset$-definable (or L-definable) means that there are no parameters. Convenient to add parameters, passing to $L_B := L \cup \{c_b : b \in B\}$ (L plus new constant symbols c_b).Then M_B is M seen as an L_B-structure and L_B-definable sets in M_B are B-definable in M.

Example 1.21. Consider $\mathbb{R}$ as an L_{ring}-structure. The set $\mathbb{R}_{\geqslant 0}$ is $\emptyset$-definable by the formula $\phi(x) := \exists y.y^2 = x$.

Example 1.22. Fix a group G, seen as an L_{group}-structure.

- The centraliser $C_G(g)$ of a given element $g \in G$ is definable, using the parameter g, by the formula $\phi(x, g) := xg = gx$.
- The center $Z(G)$ of G is $\emptyset$-definable by the formula $\psi(y) := \forall x \phi(x, y)$.

More examples of definable sets

Example 1.23. Fix a graph Γ, seen as an L_{graph}-structure.

- The set of elements of Γ connected by an edge to at least two distinct elements is $\emptyset$-definable by the formula $\phi(x) := \exists y_1, y_2(y_1 \neq y_2 \wedge E(x, y_1) \wedge E(x, y_2))$.
- Given an element $a \in \Gamma$, the set of elements of Γ at distance $\leqslant n$ from a is definable by the formula

$$\psi(x, a) := \exists y_1, \ldots, y_{n-1}(\bigwedge_{i=1}^{n-2} E(y_i, y_{i+1}) \wedge E(a, y_1) \wedge E(y_{n-1}, x)).$$

Example 1.24. Fix a field K, seen as an L_{ring}-structure.

- Some L_{ring}-definable sets in K:
  - The zero set $\{\overline{a} \in K^n \mid f(\overline{a}) = 0\}$ of a polynomial $f \in \mathbb{Z}[\overline{x}]$. (Note that $n \in \mathbb{N}$ can be written as the L_{ring}-term $\underbrace{1 + \ldots + 1}_{n}$.)
  - Boolean combinations of the above.

Note: These are *all* sets that are L_{ring}-definable without quantifiers.

- Let $f \in K[\overline{x}]$. Then $\{\overline{a} \in K^n \mid f(\overline{a}) = 0\}$ is K-definable.

Exercises 1.25. ■ Describe a language for structures in your research. Multiple sorts (i.e. several domains) may be helpful; see the example of vector spaces on Wikipedia.

1. Let R be a ring, seen as an L_{nuring}-structure. Is it true that $S \subseteq R$ is a substructure $\Leftrightarrow$ S is an ideal?
2. Look at $\mathbb{C}$ as an L_{ring}-structure. Is $\mathbb{Z} \subseteq \mathbb{C}$ a substructure? Write a language L_{field} interpret its symbols in $\mathbb{C}$ so that the substructures of $\mathbb{C}$ are exactly the subfields of $\mathbb{C}$.
3. Consider $\mathbb{R}$ as an L_{ring}-structure. Are sentences $\exists x. x + x = x \cdot x$, $\forall x. \exists y. x + y = x \cdot y$ true in $\mathbb{R}$? Is there an L_{ring}-formula $\phi(x, y)$ such that $\mathbb{R} \models \phi(a, b)$ iff $a < b$?
4. Write down an L_{group}-sentence σ such that $G \models \sigma$ iff G is abelian.
5. Find a sentence σ in a language with only a unary function symbol f such that σ has infinite but no finite models.
6. Let G be a group, seen as an L_{group}-structure. Express "G is divisible". (Hint: you need infinitely many sentences.)
7. Express "there are exactly two y's s.t. $M \models \phi(y)$" (abbreviated as $\exists^{=2}$).
8. Let G be a group, seen as an L_{group}-structure. Assume that there is a finite bound on the length of any chain of centralisers in G. Prove: $C_G(A)$ is definable for *any* $A \subseteq G$.
9. Let $L = L_{\mathrm{oring}} \cup \{f\}$, where f is a unary function symbol. Write an L-sentence σ such that $M \models \sigma$ if and only if f is continuous at 0.
10. Prove: For any L_{oring}-formula $\phi(\overline{x})$, there is an L_{ring}-formula $\psi(\overline{x})$ such that $\mathbb{R} \models \forall \overline{x}. \phi(\overline{x}) \leftrightarrow \psi(\overline{x})$.

Further examples of structures

- We have seen graphs, groups, rings, ordered sets, ordered groups and rings.
- Vector spaces over K: $L_{K\text{-vect}} = L_{\mathrm{ag}} \cup \{\lambda_r\}_{r \in K}$, where each λ_r is a unary function symbol representing "scalar multiplication by r".
- Action of G on a set: $L_G = \{\lambda_g\}_{g \in G}$, where each λ_g is a unary function.
- If G is finitely generated by $S \subseteq G$: $L_S = \{\lambda_g\}_{g \in S}$. Note how we can now talk about e.g. actions of $\mathrm{SL}_2(\mathbb{F}_p)$ but with *p not fixed*.
- Group acting on a set: two sorts G and X, language L_{ag} on the sort G, plus function symbol $\rho : G \times X \to X$.
- Group with representation: two sorts G and V, language L_{ag} on G, language $L_{K\text{-vect}}$ on V, plus function symbol $\rho : G \times V \to V$. Since the two languages overlap, we need to write $\{0_G, +_G, -_G, 0_V, +_V, -_V, \rho\}$ to distinguish the symbols on the sort G from the symbols on the sort V.
- Vector spaces: sorts K and V, language L_{ring} on K, L_{ag} on V, plus function symbol $\lambda : K \times V \to V$. Again $\{0_K, 1_K, +_K, \dots, 0_V, +_V, \dots, \lambda\}$.
- Profinite groups: one sort of each $n \in \mathbb{N}$ representing "cosets of open normal subgroups of index $\leq n$"; binary relations $\leq_{n,m}$ (inclusion of underlying subgroup); binary functions $\cdot_n$ (product inside underlying subgroup); binary relations $C_{n,m}$ (coset inclusion). Note how this is *dual* to groups: a substructure H of a profinite group G corresponds to an epimorphism $G \to H$.