Introductory Lectures
Model Theory I: Definability

David Marker

Mathematics, Statistics, and Computer Science
University of Illinois at Chicago

October 9, 2020

MSRI Program on Decidability, Definability and Computability in Number Theory

Khazdan on Model Theory

David Khazdan (2020 Abel Prize winner):

I don't know any mathematician who did not start as a logician and for whom it was easy and natural to learn model theory.

For a [short] while everything is so simple and so easily reformulated in familiar terms that there is nothing to learn but suddenly one finds himself in place when Model theoriticans "jump from a tussock to a hummock" while we mathematicians don't see where to put a foot down and are at a complete loss.

Khazdan on Model Theory continuted

So we have two questions.

a) Why is Model theory so useful in different areas of Mathematics?

b) Why is it so difficult for mathematicians to learn it ?

But really these two questions are almost the same–it is difficult to learn the Model theory since it appeals to different intuition. But exactly this new outlook leads to the successes of the Model Theory.

Model theory is the disappearance of the natural distinction between the formalism and the substance.

Outline

- Part I: Definability
  - Basic concepts from Logic & Model Theory
  - Definability
  - Interpretability
  - Completeness & Compactness (time permitting)
- Part II: Quantifier elimination & applications
- Part III: Tameness & fields

Mathematical structures

In Model Theory we use first order languages to study sets definable in mathematical structures.

Examples of Structures

- $(\mathbb{Z}, +, \cdot, 0, 1)$, the ring of integers;
- $(\mathbb{C}, +, \cdot, 0, 1)$, the field of complex numbers;
- $(\mathbb{R}, +, \cdot, <, 0, 1)$, the ordered field of real numbers;
- $\mathbb{R}_{\mathrm{exp}} = (\mathbb{R}, +, \cdot, \exp <, 0, 1)$, the ordered field of real numbers with exponentiation;
- $\mathbb{C}_{\mathrm{exp}} = (\mathbb{C}, +, \cdot, \exp, 0, 1)$, the field of complex numbers with exponentiation;
- $(\mathbb{C}((t)), +, \cdot, 0, 1)$;

Mathematical structures

Informally A *structure* is just a set with some distinguished functions, relations and elements.

For Example:
In $\mathbb{R}_{\text{exp}} = (\mathbb{R}, +, \cdot, \text{exp}, <, 0, 1)$ we have

- The set $\mathbb{R}$
- Binary functions $+$ and $\cdot$ and a unary function exp;
- Binary relation $<$;
- Distinguished elements 0 and 1.

In $(\mathbb{Z}, +, \cdot, 0, 1)$ we have

- The set $\mathbb{Z}$
- Binary functions $+$ and $\cdot$;
- No relations;
- Distinguished elements 0 and 1.

Multisorted Structures

We can also look at structures where we have more than one type of basic object.

Vector spaces over fields $(V, \oplus, F, +, \cdot, \lambda)$
Two sorts–vector space and field

- $(F, +, \cdot)$ is a field;
- $(V, \oplus)$ is an abelian group;
- $\lambda : F \times V \to V$ is scalar multiplication

Valued fields $(K, +_K, \cdot_K, \Gamma, +_\Gamma, <, \mathrm{k}, +_\mathrm{k}, \cdot_\mathrm{k})$
Three sorts home field, value group and residue field.

- $(K, +_K, \cdot_K)$ and $(\mathrm{k}, +_\mathrm{k}, \cdot_\mathrm{k})$ fields;
- $(\Gamma, +_\Gamma, <)$ an ordered abelian group;
- $v : K \to \Gamma$ the valuation;
- $r : K \to \mathrm{k}$ the residue map

First order languages

We fix a language to describe our structure.
For example, let's say we are studying $\mathbb{R}_{\exp}$. We would use the language $\mathcal{L}_{\exp}$ where we have special symbols $+, \cdot, \exp, <, 0, 1$.

Following some simple rules we build up the collection of $\mathcal{L}_{\exp}$-formulas using the special symbols and the logical symbols

- $=$;
- Logical connectives $\wedge$ (and), $\vee$ (or), $\neg$(not);
- Quantifiers $\exists$ (exists) and $\forall$ (for all);
- Variables $v_0, v_1, \ldots$; (often we use $x, y, z \ldots$)
- Parenthesis;

Examples of $\mathcal{L}_{\exp}$-formulas

1. $1 + x < \exp(x)$;
2. $\exists y \; y \cdot y = x$ *x is a square*
3. $\forall x \; (0 < x \to \exists y \; y^2 = x)$ *every positive element is a square*
4. $\exists y \; \exp(y) = x$ *x has a logarithm*
5. $\forall \epsilon > 0 \; \exists \delta > 0 \; \forall x \; ((x-2)^2 < \delta \to (x^2 - 4)^2 < \epsilon)$

$$\lim_{x \to 2} x^2 = 4$$

(here 2 and 4 are abbreviations for $1+1$ and $1 + 1 + 1 + 1$ and $(x-2)^2 < \delta$ is an abbreviation for $x \cdot x + 1 + 1 + 1 + 1 < \delta + x + x$.

Definition

A formula is a *sentence* if every variable is in the scope of a quantifier.

Here 3) and 5) are sentences.

Sentences

Sentences are declarative statements. In any particular structure they are either true or false.

- $\exists x \forall y \; x \cdot y = y$
  - True in $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ (take $x = 1$).
- $\forall x \; (x = 0 \vee \exists y \; x \cdot y = 1)$
  - False in $\mathbb{Z}$ (take $x = 2$)
  - True in $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.
- $\forall x \exists y \; y^2 = x$
  - False in $\mathbb{Z}$, $\mathbb{R}$ (no $\sqrt{-1}$)
  - True in $\mathbb{C}$

What we can't do

- Sentences are finite.
- We can only quantify over elements of our structure not subsets, functions,. . . .

We don't have sentences expressing.

- a group is torsion
  $\forall x\ (x^2 = 1 \vee x^3 = 1 \vee x^4 = 1 \vee \dots)$
- an ordering is complete
  $\forall X$ if X is nonempty and bounded above, then there is a least upper bound

Theories

An $\mathcal{L}$-theory T is just a set of $\mathcal{L}$-sentences.
For example T could be the set of axioms for fields.

If ϕ is an $\mathcal{L}$-sentence we write $\mathcal{M} \models \phi$ if ϕ is true in $\mathcal{M}$.

If T is an $\mathcal{L}$-theory we write $\mathcal{M} \models T$ if $\mathcal{M} \models \phi$ for all $\phi \in T$ and say $\mathcal{M}$ is a *model* of T.

The *Theory* of a structure $\mathcal{M}$ is the set of all sentences true in $\mathcal{M}$ and denoted $\mathrm{Th}(\mathcal{M})$.

Fundamental Problem 1

Given a structure $\mathcal{M}$ can we understand $\mathrm{Th}(\mathcal{M})$?

- Is there an algorithm to decide for ϕ an $\mathcal{L}$-sentence if $\mathcal{M} \models \phi$?
  If there is we say $\mathrm{Th}(\mathcal{M})$ is *decidable*.
- Can we give a simple axiomatization of $\mathrm{Th}(\mathcal{M})$?
  i.e., can we write down a simple set of $\mathcal{L}$-sentences T_0 such that $\mathcal{M} \models T_0$ whenever $\mathcal{N} \models T_0$, then $\mathcal{N} \models \mathrm{Th}(\mathcal{M})$.

If the last condition holds, then

$$\mathcal{M} \models \phi \Leftrightarrow \mathcal{N} \models \phi$$

for all $\mathcal{L}$-sentences ϕ. We say $\mathcal{M}$ and $\mathcal{N}$ are *elementarily equivalent* and write $\mathcal{M} \equiv \mathcal{N}$.

We say T is *complete* if any two models are elementarily equivalent.

Definable Sets

Formulas with free variable assert a property of the free variables.

$\exists y\ y^2 = x$ asserts x is a square

- in $\mathbb{Z}$ or $\mathbb{Q}$ it is true for $x = 9$, but false for $x = 3$
- in $\mathbb{R}$ it is true of any $x \geq 0$ but false for $x = -3$
- in $\mathbb{C}$ it is true for every x.

Suppose $\phi(x_1, \ldots, x_n)$ is a formula with free variables $x_1, \ldots, x_n$ and $\mathcal{M}$ is a structure. We say that

$$\{(a_1, \ldots, a_n) \in \mathcal{M}^n : \mathcal{M} \models \phi(a_1, \ldots, a_n)\}$$

is *definable*.

We also allow parameters. Given $\phi(x_1, \ldots, x_{n+m})$ and $b_1, \ldots, b_m \in \mathcal{M}$

$$\{(a_1, \ldots, a_n) \in \mathcal{M}^n : \mathcal{M} \models \phi(a_1, \ldots, a_n, b_1, \ldots, b_m)\}$$

is *definable* using parameters $b_1, \ldots, b_m$.

For example $\{x \in \mathbb{R} : x > \pi\}$ is definable using parameter π.

Examples of Definable sets

- In $\mathbb{C}$ any algebraic variety V is definable using parameters.

$$\mathrm{x} \in \mathrm{V} \Leftrightarrow p_1(\mathrm{x}) = 0 \wedge \cdots \wedge p_m(\mathrm{x}) = 0.$$

- $\mathbb{Z}$ is definable in $\mathbb{C}_{\mathrm{exp}}$.

$$\mathbb{Z} = \{n : \forall z\ (\exp(z) = 1 \rightarrow \exp(nz) = 1\}.]$$

- $\leq$ is definable in $(\mathbb{Z}, +, \cdot)$

$$x \leq y \Leftrightarrow \exists z_1 \exists z_2 \exists z_3 \exists z_4\ x + z_1^2 + z_2^2 + z_3^2 + z_4^2 = y$$

Examples of Definable sets

- If $X \subset \mathbb{R}^n$ is definable, so is it's closure $\overline{X}$.
  Let $\phi(\mathrm{v}, \mathrm{a})$ define X.

$$\mathrm{x} \in \overline{X} \Leftrightarrow \forall \epsilon \left[\epsilon > 0 \rightarrow \exists \mathrm{y} \ \left(\phi(\mathrm{y}, \mathrm{a}) \wedge \sum (x_i - y_i)^2 < \epsilon \right) \right].$$

- $\mathbb{C}$ is definable in the field $\mathbb{C}(t)$

$$x \in C \Leftrightarrow \exists y \ y^2 = x^3 + 1$$

  Because $y^2 = x^3 + 1$ has genus 1, there are no nonconstant rational functions f, g such that $f^2 = g^3 + 1$.

Examples of Definable sets

- The valuation ring $\mathbb{Z}_p$ is definable in the p-adic field $\mathbb{Q}_p$. Assume $p \neq 2$.

$$x \in \mathbb{Z}_p \Leftrightarrow \exists y \ y^2 = px + 1$$

If $v(x) < 0$¡ then $v(px + 1)$ is odd while $v(y^2)$ is even
If $v(x) \geq 0$, we can solve $y^2 = px + 1$ by Hensel's Lemma.

- (J. Robinson) $\mathbb{Z}$ is definable in the field $\mathbb{Q}$.

Some undefinability results

- $\mathbb{R}$ is not definable in $\mathbb{C}$.
  Suppose $\phi(x, \mathrm{a})$ is a formula.

  Let k be the subfield of $\mathbb{C}$ generated by a and let $r \in \mathbb{R}$, $s \in \mathbb{C} \setminus \mathbb{R}$ be transcendental over k.

  There is an automorphism σ of $\mathbb{C}$ fixing k with $\sigma(r) = s$. But then

  $$\phi(r, \mathrm{a}) \Leftrightarrow \phi(\sigma(r), \sigma(\mathrm{a})) \Leftrightarrow \phi(s, \mathrm{a}).$$

  Thus $\phi(x, \mathrm{a})$ does not define $\mathbb{R}$.
- In $\mathbb{C}(t)$ we can't define $\{t\}$ using only parameters from $\mathbb{C}$.
  Consider an automorphism of $\mathbb{C}(t)$ fixing $\mathbb{C}$ but sending $t \mapsto t + 1$.

We were lucky here as the structures have many automorphisms. In general to prove undefinability results we need to develop a good theory of the definable sets.

Interpretability

We can interpret $\mathbb{C}$ in the field $\mathbb{R}$.

Identify $\mathbb{C}$ with $\mathbb{R}^2$ and define

$$(x, y) \oplus (u, v) = (x + u, y + v) \text{ and } (x, y) \odot (u, v) = (xu - yv, xv + yu).$$

In a similar way for any field F and any finite algebraic extension K/F we can interpret K in F.

Definition

We say that an $\mathcal{L}_0$-structure $\mathcal{N}$ is *interpretable* in an $\mathcal{L}$-structure $\mathcal{M}$ if there is a definable $X \subseteq \mathcal{M}^n$, a definable equivalence relation E on X, and for each symbol of $\mathcal{L}_0$ we can find definable E-invariant sets on X (where "definable" means definable in $\mathcal{L}$) such that X/E with the induced structure is isomorphic to $\mathcal{N}$.

Examples of Interpretations

- $\mathbb{P}^{(n)}(k)$ is interpretable in k

  Define $\sim$ in $k^{n+1} - \{0\}$, by $(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n)$ if and only if there is $\lambda \in k^\times$ such that $\lambda x_i = y_i$ for all i.

  Alternatively. define $\mathbb{P}^1(k)$ by taking $X = k \times \{0, 1\}$ and identify (x, i) with $(1/x, 1 - i)$ for $x \neq 0$,

Examples of Interpretations

- If $(G, \cdot)$ is a definable group definable in $\mathcal{M}$ and $H \subset G$ is a definable normal subgroup, then we can interpret G/H in $\mathcal{M}$.
- If K is a valued field with valuation ring O, then the value group is interpretable in $(K, O, +, \cdot)$.

  Let $U = \{x \in O : \exists y \in O \ xy = 1\}$ be the units.

  Let $\Gamma = K^\times/U$.

  $x/U \leq y/U$ if $\exists z \in O \ y = xz$.

  Similarly, the residue field is interpretable.
- Any structure in a finite language can be interpreted in a graph.

Fundamental Problem 2

Fundamental Problem For a particular structure $\mathcal{M}$, can we understand the definable sets?

- Can we give a simpler description of the definable sets?
- Can we prove the definable sets have good properties?
- Can we understand what structures are interpretable in $\mathcal{M}$?

So our two fundamental problems are to try to understand the $\mathrm{Th}(\mathcal{M})$ and the sets definable in $\mathcal{M}$.

Bad Cases: Gödel Phenomena

These problems are hopeless for $(\mathbb{Z}, +, \cdot)$.

Theorem (Gödel's Incompleteness Theorem)

$\mathrm{Th}(\mathbb{Z})$ *is far from decidable.*
In particular, no decidable theory can axiomatize $\mathrm{Th}(\mathbb{Z})$.

The definable subset of $\mathbb{Z}^n$ are exactly the arithmetic sets from computability theory.

MRDP showed that for any recursively enumerable set A there is an integer polynomial $p(X, Y_1, \ldots, Y_9)$ such that

$$n \in A \Leftrightarrow \exists \mathrm{y} \in \mathbb{Z}^9 \; p(n, \mathrm{y}) = 0$$

Lesson: Quantifiers lead to complexity

It could be worse

Consider $(\mathbb{R}, \mathbb{Z}, +, \cdot)$. The real field with a predicate for $\mathbb{Z}$.

In this case the definable sets are the projective sets of descriptive set theory.

Even questions like "is every definable set Lebesgue measurable" depend on set theoretic assumptions.

Digression: Completeness Theorem

For an $\mathcal{L}$-theory T we write $T \models \phi$ (ϕ is a *consequence* of T) if

$$\text{for all } \mathcal{M} \models T \Rightarrow \mathcal{M} \models \phi.$$

Theorem (Gödel's Completeness Theorem)

$T \models \phi$ if and only if there is a finite proof of ϕ assuming T.

We say T is *satisfiable* if there is some $\mathcal{M} \models T$.

Corollary

T is satisfiable if and only there is no proof of a contradiction from T.

Digression: Compactness Theorem

Corollary (Compactness Theorem)

T is satisfiable if and only if every finite subset of T is satisfiable.

Proof Any proof of a contradiction from T uses only finitely many of the sentences in ϕ.

Sample Application (Nonstandard models)
There is $K \models \mathrm{Th}(\mathbb{R})$ with $a \in K$ an infinite.
Let $\mathcal{L} = \{+, \cdot, <, 0, 1, a\}$. Let
$T = \mathrm{Th}(\mathbb{R}) \cup \{a > 1, a > 1 + 1, a > 1 + 1 + 1, \dots\}$.
If Δ is a finite subset of T then there is a maximum n such that "$a > n$" $\in \Delta$.
We can find a model of Δ by taking $\mathbb{R}$ and interpreting a as $n + 1$. So Δ is satisfiable.
Thus, by the Compactness Theorem, T is satisfiable.