Model Theory, Quantifier Elimination and Differential Algebra

David Marker

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

June 1, 2020

www.math.uic.edu/∼marker/Banff

Khazdan on Model Theory

David Khazdan (2020 Able 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

- Today
  - Basic concepts from Logic & Model Theory
  - Quantifier Elimination & Applications
- Wednesday
  - A test for quantifier elimination
  - Differentially Closed Fields
  - Quantifier Elimination for Differentially Closed Fields
  - Other useful model theoretic concepts (if time permits)

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;
- $\mathbb{R}_{\exp} = (\mathbb{R}, +, \cdot, \exp <, 0, 1)$, the ordered field of real numbers with exponentiation;
- $\mathbb{C}_{\exp} = (\mathbb{C}, +, \cdot, \exp, 0, 1)$, the field of complex numbers with exponentiation;
- $(\mathcal{M}, +, \cdot, D, 0, 1)$, the field of meromorphic functions with the derivation $D(f) = \frac{df}{dz}$.

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

Mathematical structures

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

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

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. $\exp(x) > 1 + x$;
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 $\mathbb{C}$

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.

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

- $\leq$ is definable in $(\mathbb{Z}, +, \cdot)$ by Lagrange's Theorem

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

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

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

- If $X \subset \mathbb{R}^n$ is definable, so is it's closure $\overline{X}$. Let $\phi(v)$ define X. Then $x \in \overline{X}$ if and only if

$$\forall \epsilon > 0 \exists y \; [\phi(y) \wedge \sum_{i=1}^{n} (x_i - y_i)^2 < \epsilon].$$

Fundamental Problem 2

A deeper example

- (J. Robinson) $\mathbb{Z}$ is definable in $(\mathbb{Q}, +, \cdot)$.

Fundamental Problem 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?

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 $\mathrm{Th}(\mathbb{Z})$.

So we can not easily understand $\mathrm{Th}(\mathbb{Z})$.

Hilbert's 10th Problem

Fix a coding of computer programs by integers.

Theorem (Matiyasevich-J. Robinson-Davis-Putnam)

There is an integer polynomial $p(X, Y, Z_1, \ldots, Z_9)$ *such that: The program coded by* e *halts on input* i *if and only if*

$$\mathbb{Z} \models \exists z_1 \ldots \exists z_9 \; p(e, i, z_1, \ldots, z_9) = 0.$$

Thus the Halting Problem, an undecidable set, is definable in $(\mathbb{Z}, +, \cdot)$ This is the first sign that there is no good theory for definable sets.

Lesson: Quantifiers lead to complexity

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.

What is $\mathrm{Th}(\mathbb{R})$?

We start by some giving axioms (RCF) in the language $\mathcal{L}_{or} = \{+, \cdot, <, , 0, 1\}$ that we know are true in $\mathbb{R}$.
We say that $(K, +, \cdot, <)$ is a *real closed field* if

- K is an ordered field;
- (sign change) If $f \in K[X]$, $a < b$ and $f(a)f(b) < 0$, there is $c \in (a, b)$ such that $f(c) = 0$.

Sign change can be expressed by axioms $\phi_1, \phi_2, \ldots$ where ϕ_n is

$$\forall \alpha_0 \ldots \forall \alpha_n \left[\forall a \forall b \left(a < b \wedge \left(\sum_{i=0}^{n} \alpha_i a^i \right) \left(\sum_{i=0}^{n} \alpha_i b^i \right) < 0 \right) \rightarrow \right.$$

$$\left. \exists c \; a < c < b \wedge \sum_{i=0}^{n} \alpha_i c^i = 0. \right]$$

Quantifier Elimination for Real Closed Fields

Theorem (Tarski)

RCF has quantifier elimination, i.e., for any $\mathcal{L}_{or}$-formula $\phi(v_1, \ldots, v_n)$, there is an $\mathcal{L}_{or}$ formula $\psi(v_1, \ldots, v_n)$ without quantifiers such that

$$\mathrm{RCF} \models \forall v_1, \ldots, \forall v_n \ (\phi(v_1, \ldots, v_n) \leftrightarrow \psi(v_1, \ldots, v_n)).$$

In particular any definable set is definable by a quantifier free formula.

What are the quantifier free definable sets in a real closed field K?
Boolean combinations of

$$p(x_1, \ldots, x_n) = 0 \text{ and } q(x_1, \ldots, x_n) > 0$$

for $p, q \in K[X_1, \ldots, X_n]$.
In real algebraic geometry these are known as the *semialgebraic sets*.

Semialgebraic sets and QE

Corollary (Tarski–Seidenberg Theorem)

The image of a semialgebraic set under a semialgebraic function is semialgebraic.

Corollary

The closure of a semialgebraic set is semialgebriac.

Corollary (o-minimality)

Any definable subset of $\mathbb{R}$ is a finite union of points and intervals. In particular, $\mathbb{Z}$ is not definable in $\mathbb{R}$.

Remarkable Fact: o-minimality captures many of the good geometric and topological properties of semialgebraic sets.

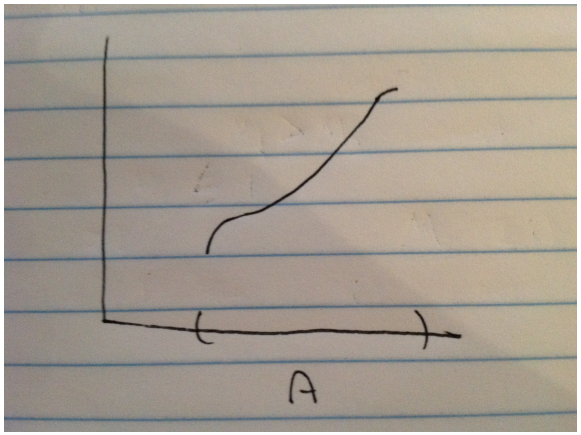
o-minimality

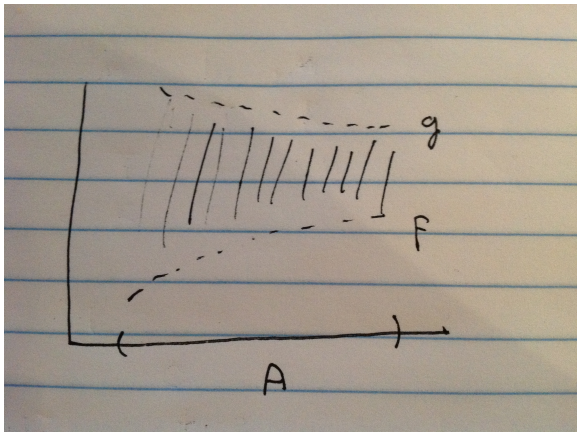
Theorem

If $f : \mathbb{R}^n \to \mathbb{R}$ is definable, then we can partition $\mathbb{R}$ into definable sets $X_1 \cup \cdots \cup X_n$ such that f is continuous (or even $\mathcal{C}^m$) on each X_i.

Theorem (Cell Decomposition)

If $X \subseteq \mathbb{R}^n$ is definable, then X can be partitioned into finitely many disjoint cells, $X = C_1 \cup \cdots \cup C_m$.
In particular, X has finitely many connected components.





What about $\mathrm{Th}(\mathbb{R})$?

Corollary

RCF axiomatizes $\mathrm{Th}(\mathbb{R})$, *i.e., if* K *is a real closed field, then* $K \models \mathrm{Th}(\mathbb{R})$.

Let ϕ be a sentence such that $\mathbb{R} \models \phi$.

By quantifier elimination there is a quantifier free sentence ψ such that in any real closed field F

$$F \models \phi \leftrightarrow \psi.$$

But quantifier free sentences are trivial.
$(1+1)\cdot(1+1) = 1+1+1+1$

For a quantifier free sentence ψ

$$\mathbb{R} \models \psi \Leftrightarrow \mathbb{Q} \models \psi \Leftrightarrow K \models \psi.$$

Thus

$$\mathbb{R} \models \phi \Leftrightarrow \mathbb{R} \models \psi \Leftrightarrow K \models \psi \Leftrightarrow K \models \phi.$$

Decidability–A Logician's Algorithm

Corollary

$\mathrm{Th}(\mathbb{R})$ *is decidable.*

Let ϕ be any sentence.

One of ϕ and $\neg\phi$ is true in $\mathbb{R}$ and hence in every real closed field. Thus

$$\mathrm{RCF} \models \phi \text{ or } \mathrm{RCF} \models \neg\phi.$$

By Gödel's Completeness Theorem, there is proof from the RCF axioms of one of ϕ or $\neg\phi$

One by one generate all possible finite sequence of symbols in our language. Check each one to see if it a proof of ϕ or of $\neg\phi$. Checking each proof is "easy". Eventually we will find one or the other and be able to answer if $\mathbb{R} \models \phi$.

QE algorithm

Corollary

There is an algorithm to transform any formula ϕ into an equivalent (in $\mathbb{R}$) quantifier free formula ψ

Start with ϕ, search for a proof of $\phi \leftrightarrow \psi$ for some quantifier free ψ.

In fact Tarski gave an explicit algorithm to transform $\phi \mapsto \psi$ and this gave an explicit decision procedure for $\mathrm{Th}(\mathbb{R})$.

Namely, start with a sentence ϕ.
Eliminate quantifiers to find an equivalent quantifier free sentence ψ.
Check to see if ψ is true in $\mathbb{Q}$.

Theorem (Wilkie)

For any $X \subset \mathbb{R}^n$ definable in $\mathbb{R}_{\exp}$ there is an exponential algebraic variety $V \subset \mathbb{R}^{n+m}$ such that

$$x \in V \Leftrightarrow \exists y \in \mathbb{R}^m (x, y) \in V.$$

V is a finite system of equations like

$$e^{x+y} - ye^{e^z} = 0$$

Khovanskii's proved that any such V has finitely many connected components.

Corollary

$\mathbb{R}_{\exp}$ *is o-minimal.*

Open Question Is $\mathrm{Th}(\mathbb{R}_{\exp})$-decidable? Macintyre–Wilkie: Yes assuming Schanuel's Conjecture