Introductory Lectures
Model Theory II: Quantifier Elimination

David Marker

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

October 14, 2020

MSRI Program on Decidability, Definability and Computability in Number Theory

Loose End

Last time I pointed out that the natural way to express that a field F is orderable would be quantifying over subsets of F^2

$$\exists R \subset F^2 \text{ [}R\text{ is a linear order compatible with } + \text{ and } \cdot \text{]}$$

which we can't do in a first order sentence.

BUT..
Using the Artin–Schrier theory of ordered fields

F is orderable if and only if -1 is not a sum of squares.

This can be expressed in the theory: field axioms + $\{\forall x_1 \forall x_2\ x_1^2+x_2^2+1 \neq 0, \ldots, \forall x_1, \ldots, \forall x_n\ x_1^2+\cdots+x_n^2+1 \neq 0, \ldots\}$.

Recap

Fundamental Problems for a mathematical structure $\mathcal{M}$

- Understand $\mathrm{Th}(\mathcal{M})$.
  - Is it decidable?
  - Find an axiomatization.
- Understand the definable subsets of $\mathcal{M}^n$.
  - Give more natural description
  - Prove they have good properties.

Lesson: Quantifiers lead to complexity

Algebraically Closed Fields

$\mathcal{L} = \{+, \cdot, -, 0, 1\}$.

The theory of algebraically closed fields (ACF) is axiomatized by:

- the field axioms;
- $\forall y_0 \forall y_{n-1} \exists x \; x^n + y_{n-1}x^{n-1} + \cdots + y_0 = 0$, $n = 2, 3, \ldots$.

Theorem (Tarski)

ACF has quantifier elimination, i.e., for any formula $\phi(v_1, \ldots, v_n)$ there is a formula $\psi(v_1, \ldots, v_n)$ with no quantifiers such that

$$\mathrm{ACF} \models \forall \mathsf{v} \; [\phi(\mathsf{v}) \leftrightarrow \psi(\mathsf{v})].$$

Definable Sets

Let K be an algebraically closed field and suppose $X \subseteq K^n$ is definable.

By quantifier elimination X has a quantifier free definition.

What can we say without quantifiers?
Finite boolean combinations of $p(x_1, \ldots, x_n) = 0$,
$p \in K[X_1, \ldots, X_n]$

definable $=$ boolean combination of varieties$=$ **constructible** sets

Corollary (strong minimality)

If K is algebraically closed and $X \subset K$ is definable then either X or $K \setminus X$ is finite.

Any definable subset of K is a Boolean combination of sets $p(x) = 0$ which are finite unless p is constant.

Corollary (Chevalley)

If $X \subseteq K^{n+m}$ is constructible and π is the projection onto first n-coordinates, then the image $\pi(X)$ is construcible.

$$\mathrm{x} \in \pi(X) \Leftrightarrow \exists y_1 \ldots \exists y_m \ (\mathrm{x}, \mathrm{y}) \in X$$

and by quantifier elimination we can find an equivalent quantifier free formula.

Model Completeness

In any language $\mathcal{L}$ if we have structures $\mathcal{M} \subset \mathcal{N}$, we say that $\mathcal{N}$ is an *elementary extension* of $\mathcal{M}$ if for any formula $\phi(x_1, \ldots, x_n)$ and any a $\in \mathcal{M}^n$

$$\mathcal{M} \models \phi(\mathrm{a}) \Leftrightarrow \mathcal{N} \models \phi(\mathrm{a}).$$

We write $\mathcal{M} \prec \mathcal{N}$.

Corollary (Model Completeness of ACF)

If $K \subset L$ are algebraically closed fields, then $K \prec L$.

Proof Let $\phi(x_1, \ldots, x_n)$ be a formula and a $\in K^n$.
There is a quantifier free ψ such that $ACF \models \forall \mathrm{x}\, [\phi(\mathrm{x}) \leftrightarrow \psi(\mathrm{x})]$
An easy induction shows that for quantifier free ψ,

$$K \models \psi(\mathrm{a}) \Leftrightarrow L \models \psi(\mathrm{a}).$$

Corollary

Let K be algebraically closed and let $P \subseteq K[X_1, \ldots, X_n]$ be a prime ideal and $g \in K[\mathrm{X}] \setminus P$. There there is $\mathrm{x} \in K^n$ such that $f(\mathrm{x}) = 0$ for $f \in P$ but $g(\mathrm{x}) \neq 0$.

Let $f_1, \ldots, f_m$ generate P.

Let $L = (K[\mathrm{X}]/P)^{\mathrm{alg}}$.

$$L \models \exists x_1 \ldots \exists x_n \ f_1(\mathrm{x}) = \cdots = f_m(\mathrm{x}) = 0 \wedge g(\mathrm{x}) \neq 0$$

Namely take $x_1 = X_1/P, \ldots x_n = X_n/P$.
By model completeness

$$L \models \exists x_1 \ldots \exists x_n \ f_1(\mathrm{x}) = \cdots = f_m(\mathrm{x}) = 0 \wedge g(\mathrm{x}) \neq 0$$

Skip Bounds

Corollary

For any d, m, n there is k (depending only on d, m, n) such that in any algebraically closed field K if $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$ have degree at most d, then $f_1(\mathrm{X}) = \cdots = f_m(\mathrm{X}) = 0$ has a solution in K if and only if

$$1 \neq \sum_{i=1}^{m} g_i f_i$$

where each g_i has degree at most k.

Proof of Bounds

Write down generic polynomials $F_1, \ldots, F_m$ of degree d
i.e. $F_i = \sum_{|j| \leq d} c_{i,j} X^j$ (j a multi-index, $c_{i,j}$ new variables)

For each l there is a sentence Φ_l saying that

$$1 \neq \sum_{i \neq 1}^{m} g_i F_i$$

where each g_i has degree at most l.

Let $T = \mathrm{ACF} \cup \{\forall x \neg \bigwedge_{i=1}^{n} F_i(x) = 0\} \cup \{\Phi_l : l = 1, 2, \ldots\}$.

T is not satisfiable. If we had a model of T, we would have a contradiction to Hilbert's Nullstellensatz.

By the Compactness Theorem. Some finite subset of T is not satisfiable. But then there is a k such that if $F_1 = \cdots = F_m = 0$ has no solution, then we can find 1 using polynomials of degree at most k.

Completeness

Recall that a theory T is *complete* if for all sentences ϕ either $T \models \phi$ or $T \models \neg\phi$.

ACF is not complete

For each n, let ψ_n be the sentence $\underbrace{1+1+\cdots+1}_{n-\text{times}} = 0$

Then ACF$\not\models \psi_n$ and ACF$\not\models \neg\psi_n$.

For p prime let $\mathrm{ACF}_p = \mathrm{ACF}+\psi_p$

Let $\mathrm{ACF}_0 = \mathrm{ACF} \cup \{\neg\psi_n : n = 2, 3, \ldots\}$.

Corollary

If $p = 0$ or $p > 0$ is prime, the ACF_p is complete.

Proof of Completeness

To show ACF_0 is complete. Suppose $K, L \models \mathrm{ACF}_0$ and ϕ is a sentence.
We must show $K \models \phi \Leftrightarrow L \models \phi$. By quantifier elimination there is a quantifier free sentence ψ such that $\mathrm{ACF} \models \phi \leftrightarrow \psi$.
Quantifier free sentences can't say much.

$$K \models \psi \Leftrightarrow \mathbb{Q} \models \psi \Leftrightarrow L \models \psi$$

Thus

$$K \models \phi \Leftrightarrow L \models \phi.$$

The proof for ACF_p is similar using $\mathbb{F}_p$ instead of $\mathbb{Q}$.

Corollary

ACF_0 axiomatizes $\mathrm{Th}(\mathbb{C})$.

Corollary

The following are equivalent:

1. *ϕ is true in some $K \models ACF_0$;*
2. *ϕ is true in every $K \models ACF_0$;*
3. *For all sufficiently large primes p ϕ is true in every $K \models ACF_p$;*
4. *For infinitely many p, ϕ is true in some $K \models ACF_p$.*

2) $\Rightarrow$ 3) By the Completeness Theorem, there is a proof of ϕ from ACF_0. That proof uses only finitely many sentences $\neg\Psi_n$ and thus work in ACF_p for large p.

4) $\Rightarrow$ 1) If not that $\mathrm{ACF}_0 \models \neg\phi$, and by the above $\mathrm{ACF}_p \models \neg\phi$ for all sufficiently large primes.

Ax–Grothendieck Theorem

Corollary

If $f : \mathbb{C}^n \to \mathbb{C}^n$ is an injective polynomial map, then f is surjective.

There are sentences $\Phi_{n,d}$ saying that if $f : K^n \to K^n$ is an injective polynomial map where all polynomials have degree at most d from $K^n \to K^n$, then f is surjective.

$\Phi_{n,d}$ is true in all finite fields

$\Phi_{n,d}$ is true in $\mathbb{F}_p^{\mathrm{alg}}$.
If there was a counterexample f it would already be a counterexample in some $\mathbb{F}_{p^n}$.

Thus $\mathrm{ACF}_0 \models \Phi_{n,d}$

Decidability

Corollary

For $p = 0$ or $p > 0$ prime ACF_p is decidable.

To decide if $\mathrm{ACF}_p \models \phi$ search for a proof of ϕ or $\neg\phi$.

Corollary

ACF is also decidable.

To decide if $\mathrm{ACF} \models \phi$ search for either a proof of ϕ from ACF or a prime p and a proof of $\neg\phi$ from ACF_p.

Model Theoretic test for QE

Theorem

Let T be a theory. Suppose that for all quantifier free formulas $\phi(x_1, y_1, \ldots, y_m)$, all $\mathcal{M}, \mathcal{N} \models T$, all $\mathcal{A} \subset \mathcal{M}, \mathcal{N}$ and all $a_1, \ldots, a_m \in \mathcal{A}$

(*) if $\mathcal{M} \models \exists x\ \phi(x, a_1, \ldots, a_n)$, then $\mathcal{N} \models \exists x\ \phi(x, a_1, \ldots, a_n)$.

Then T has quantifier elimination

QE for Algebraically Closed Fields

Let ACF be the axioms for algebraically closed fields

Theorem (Tarski)

ACF has quantifier elimination.

Suppose K, L are algebraically closed fields and $\mathcal{A} \subset K \cap L$ is a domain.
$\phi(v)$ is a quantifier free formula with parameters from $\mathcal{A}$ such that there is $b \in K$ with $K \models \phi(b)$.
$\phi(v)$ is a Boolean combination of formulas of the form $p(v) = 0$ where $p(X) \in \mathcal{A}[X]$.
Without loss of generality $\phi(v)$ is

$$\bigwedge_{i=1}^{n} f_i(v) = 0 \wedge g(v) \neq 0$$

where $f_1, \ldots, f_n, g \in \mathcal{A}[X]$

QE for Algebraically Closed Fields

$$\bigwedge_{i=0}^{n} f_i(v) = 0 \wedge g(v) \neq 0$$

case 1 There are no nonzero f_i, in this case $\phi(v)$ is just $g(v) \neq 0$. We can find $c \in L$ such that $g(c) \neq 0$.

case 2 For some i, f_i is nonzero and $f_i(b) = 0$.
Let K_0 be the algebraic closure of $\mathcal{A}$ in K. Then $b \in K_0$

There is a field embedding $\sigma : K_0 \to L$ fixing $\mathcal{A}$ and $L \models \phi(\sigma(b))$.

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.

The proof closely follows the proof for algebraically closed fields.

The key algebraic fact needed is that every ordered field $(F, <)$ has a unique real closure.

Semialgebraic sets

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*.

definable=quantifier free definable=semialgebraic

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 $\mathbb{R}$.

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.

We say closures of definable sets are definable.
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.

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

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

V is a finite system of equations like

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

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

Corollary

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

Wilkie's result shows model completeness. van den Dries, Macintyre and I showed quantifier elimination in an expanded language adding restrictions of analytic functions and ln.

Open Questions

- Is $\mathrm{Th}(\mathbb{R}_{\mathrm{exp}})$-decidable? Macintyre–Wilkie: Yes assuming Schanuel's Conjecture
- Find a natural axiomatization. Find a $\forall\exists$-axiomatization.
- What's the right language for quantifier elimination?

Quantifier Elimination for $\mathbb{Q}_p$

Recall that $\mathbb{Z}_p$ is definable in $\mathbb{Q}_p$. Thus we can also define

$$x|y \leftrightarrow \exists z \in \mathbb{Z}_p\ xz = y. \text{ i.e., } v(x) \leq v(y).$$

Let P_n be a predicate for the n^{th}-powers in $\mathbb{Q}_p$.
Consider the language $\mathcal{L}_{\mathrm{Mac}} = \{+, \cdot, 0, 1, |, \mathbb{Z}_p, P_2, P_3, \ldots\}$.
Any subset of $\mathbb{Q}_p^n$ definable using the $\mathcal{L}_{\mathrm{Mac}}$-language is already definable in the field language.

Theorem (Macintyre)

$\mathrm{Th}(\mathbb{Q}_p)$ *has quantifier elimination in the* $\mathcal{L}_{\mathrm{Mac}}$.

Corollary

Any infinite definable subset of $\mathbb{Q}_p$ *has interior.*

Quantifier Elimination in the Pas Langugage

Consider a valued field as a three sorted structure (K, Γ, k) with $v : K^\times \to \Gamma$ and $r : O \to k$.

Add a *angular component* $\mathrm{ac} : K^\times \to k$ a multiplicative homomorphism that agrees with the residue map on the units.

For example: In $K((t))$ and $f = \sum_{n=m}^{\infty} a_n t^n$ with $a_m \neq 0$ we could let $\mathrm{ac}(f) = a_m$.

angular components need not exist (but will in saturated enough models)

adding the angular component map adds new definable sets

Theorem (Pas)

Suppose K is a henselian field with residue field k of characteristic 0. Roughly, any formula is equivalent to a boolean combination of:
i) quantifier free field formulas about K;
ii) formulas about the residue field and value group

Ax–Kochen

Theorem

Let (K,v) and (L,v) be henselian valued fields with characteristic zero residue fields k and l. Then $K \equiv L$ if and only if
i) $v(K) \equiv v(L)$;
ii) $k \equiv l$.

If D is a non-principle ultrafilter on the primes

$$\prod_D \mathbb{Q}_p \equiv \prod_D \mathbb{F}_p((t))$$

Corollary

If $\mathbb{F}_p((t)) \models \phi$ for all primes p, then $\mathbb{Q}_p \models \phi$ for all sufficiently large primes.