ACFs are simple as much as infinite sets: An introduction to quantifier elimination

Junguk Lee

KAIST

January, 14th, 2022

- My goal is to convince that algebraically closed fields are simple as much as infinite sets (in the view of their syntax).
- I will introduce a notion of **quantifier elimination** (QE) from model theory.
- In the term of QE, the syntax of an algebraically closed field, as a field, is simple as like
  - an infinite set as a structure equipped with equality only,
  - a real closed field as an ordered field,
  - a differentially closed fields as a differential field.

- Fix a first order language $\mathcal{L}$, which is countable for simplicity. Let T be a complete $\mathcal{L}$-theory.
- Write $x, y, z, \ldots$ for tuples of variables.
- Let ω be the set of natural numbers.
- We say that a formula $\varphi(x)$ is **quantifier-free** if it has no quantifiers in φ.
- We say that T has **quantifier elimination** (QE) if for any formula $\varphi(x)$, there is a quantifier-free formula $\psi(x)$ such that

$$T \models \forall x(\varphi(x) \leftrightarrow \psi(x)),$$

that is, any formula is equivalent to a quantifier-free formula modulo T.

Example

Let T be the theory of real closed fields in the ordered ring language. Let

$$\varphi(a, b, c) \equiv a \neq 0 \wedge \exists x(ax^2 + bx + c = 0).$$

Then, φ is equivalent (modulo T) to the following quantifier-free formula

$$\psi(a, b, c) \equiv b^2 - 4ac \geq 0.$$

- Even though QE is defined syntactically, it has a semantic criterion, which is very useful.

Theorem

T has QE if and only if for a $\aleph_0$-saturated and $\aleph_1$-strongly homogeneous model $\mathfrak{C}$ of T, the following holds: For an isomorphism $f : A \to B$ between finitely generated substructures A and B of $\mathfrak{C}$ and $a \in \mathfrak{C}^1$, there is $b \in \mathfrak{C}^1$ such that the map $f \cup \{(a, b)\}$ is extended into an isomorphism between finitely generated substructures of $\mathfrak{C}$.

- A structure $\mathfrak{C}$ is called $\aleph_0$-saturated if the following holds: Let $\Sigma(x)$ be a countable set of $\mathcal{L}(\mathfrak{C})$-formulae in the variable x of countable length. Suppose any finite subset Σ_0 of Σ has a solution in $\mathfrak{C}$. Then, there is a solution of Σ.
- A structure $\mathfrak{C}$ is called $\aleph_1$-strongly homogeneous if for any tuples $\bar{a}$ and $\bar{b}$ of elements in $\mathfrak{C}$ of countable length,

$$\bar{a} \equiv \bar{b} \Rightarrow (\exists \sigma \in \mathrm{Aut}(\mathfrak{C}))(\sigma(\bar{a}) = \bar{b}),$$

where $\bar{a} \equiv \bar{b}$ means $\mathfrak{C} \models \varphi(\bar{a}) \Leftrightarrow \mathfrak{C} \models \varphi(\bar{b})$ for all formulas $\varphi(x)$.

- Let $\mathcal{L} = \emptyset$ and let T be the theory of infinite sets.
- Then, T has QE.
- Let $\mathfrak{C}$ be a $\aleph_0$-saturated and $\aleph_1$-strongly homogeneous infinite set.
- Note that any subset of $\mathfrak{C}$ is a substructure because thee are no function symbols.
- Let $f : A \to B$ be an isomorphism between finite subsets of $\mathfrak{C}$ with $|A| = |B| = n < \omega$.
- That is, f is just a bijection between A and B.
- Take $a \in \mathfrak{C}$ arbitrary. If $a \in A$, then $f \cup \{(a, f(a))\}$ does work.
- Suppose $a \notin A$. Since $\mathfrak{C}$ is infinite and B is finite, there is $b \in \mathfrak{C} \setminus B$. Then, the map $f \cup \{(a, b)\}$ does work.

- Let $\mathcal{L} = \{<\}$ and let T be the theory of linear orders without endpoints.
- Then, DLO has QE.
- Let $\mathfrak{C}$ be a $\aleph_0$-saturated and $\aleph_1$-strongly homogeneous DLO.
- Note that any subset of $\mathfrak{C}$ is a substructure because thee are no function symbols.
- Let $f : A \to B$ be an isomorphism between finite subsets of $\mathfrak{C}$ with $|A| = |B| = n < \omega$.
- That is, f is an increasing bijection between A and B.
- Write $A := \{a_0 < a_1 < \cdots < a_{n-1}\}$ and $B := \{b_0 < b_1 < \cdots < b_{n-1}\}$ with $b_i = f(a_i)$.

- Take $a \in \mathfrak{C} \setminus A$ arbitrary.
- Then, there are essentially $(n+1)$-many cases:
  1. $a < a_0$.
  2. For some $0 \leq i < n-1$,
  $$a_i < a < a_{i+1}.$$
  3. $a > a_{n-1}$.
- Suppose $a_0 < a < a_1$.
- Then, since $\mathfrak{C}$ is dense, there is b such that $b_0 < b < b_1$, and the map $f \cup \{(a, b)\}$ does work.
- For the first and third cases, it comes from the fact that $\mathfrak{C}$ has no endpoints.

- Let $\mathcal{L}_{ring} = \{+, \cdot, 0, 1\}$ be the ring language and ACF_p be the theory of algebraically closed fields of characteristic p.
- Then, ACF_p has QE.
- Let $\mathfrak{C}$ be a $\aleph_0$-saturated and $\aleph_1$-strongly homogeneous model of ACF_p.
- For a subset A of $\mathfrak{C}$, the substructure generated by A is the field generated by A.
- Let $f : A \to B$ be an isomorphism between finitely generated subfields of $\mathfrak{C}$.
- The isomorphism f can be extended into an isomorphism between the algebraic closure of A and B.
- WLOG, we may assume that A and B are algebraically closed.

- Take $a \in \mathfrak{C} \setminus A$ arbitrary. Then a is transcendental over A.
- We can take $b \in \mathfrak{C}$ which is transcendental over B because $\mathfrak{C}$ is $\aleph_0$-saturated and B is countably generated.
- Then, there is an isomorphism

$$f' : A(a) \cong_A A(X) \cong B(X) \cong_B B(b), a \mapsto a$$

extending f.
- The similar process works for the theory DCF_0 of differentially closed fields of characteristic 0 in the differential ring language.
- In this case, we work with
  - Differential polynomials analogous to polynomials,
  - Differential ideals analogous to ideals,
  - The Kolchin topology, which is Noetherian, analogous to the Zariski topology.

- QE is very much dependent on the choice of a language.
- Consider the field $\mathbb{R}$ of reals.
- Let T_1 be the theory of $\mathbb{R}$ in the ring language $\mathcal{L}_1 := \mathcal{L}_{ring}$ and let T_2 be the theory of $\mathbb{R}$ in the ordered ring language $\mathcal{L}_2 := \mathcal{L}_{ring} \cup \{<\}$.
- In $\mathbb{R}$, $<$ is definable in the ring language, that is,

$$\mathbb{R} \models \forall x, y \left(x < y \leftrightarrow \exists z (y = z^2 + x) \right).$$

- So, $\mathbb{R}$ has the exactly same definable sets or the same 'expressing' power in both languages of $\mathcal{L}_1$ and $\mathcal{L}_2$. More generally, the same thing holds for all real closed fields.
- A field F is called **real closed** if
  - it is formally real, that is, -1 is not a sum of squares,
  - any polynomial over F of odd degree has a zero in F.

- We will show that T_1 has no QE in $\mathcal{L}_1$ but T_2 has QE in $\mathcal{L}_2$.
- Let $\mathfrak{C}$ be a real closed fields which is $\aleph_0$-saturated and $\aleph_1$-strongly homogeneous so that it is as a model of T_1 and of T_2.
- T_1 has no QE in $\mathcal{L}_1 = \mathcal{L}_{ring}$:
- Consider an ring isomorphism

$$f : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(-\sqrt{2}), \sqrt{2} \mapsto -\sqrt{2}.$$

- Take $a = \sqrt[4]{2} \in \mathfrak{C}$. Then, we can not find $b \in \mathfrak{C}$ such that there is an ring isomorphism between finitely generated subfields of $\mathfrak{C}$, extending $f \cup \{(a, b)\}$.
- Why? Suppose there is such a 'b'.

$$a^2 = \sqrt{2} \Rightarrow b^2 = -\sqrt{2}.$$

- In the real closed field $\mathfrak{C}$,

$$0 < b^2 = -\sqrt{2} < 0,$$

a contradiction.

- QE of *ACF* implies Chevalley's theorem on constructible sets.

Theorem

The set of constructible sets on $\mathbb{C}$ is closed under taking projection.

- An algebraic subset of $\mathbb{C}^n$ is a zero of polynomial equations over $\mathbb{C}$.
- A subset of $\mathbb{C}^n$ is called constructible if it is a boolean combination of algebraic subsets.
- Chevalley's theorem says that given a constructible subset A of $\mathbb{C}^{n+1}$, the projection $\pi[A]$ is also constructible, where $\pi : (x_0, \dots, x_n) \mapsto (x_1, \dots, x_n)$.

- By definition, a subset of $\mathbb{C}^n$ is constructible if and only if it is definable by a quantifier-free formula over $\mathbb{C}$.
- Let $A \subseteq \mathbb{C}^{n+1}$ be constructible.
- So, there is a quantifier-free formula $\varphi(x_0, \ldots, x_n)$ such that

$$A = \{\bar{a} \in \mathbb{C}^{n+1} : \mathbb{C} \models \varphi(\bar{a})\}.$$

- Then,

$$\pi[A] := \{(b_1, \ldots, b_n) \in \mathbb{C}^n : \exists x_0 \in \mathbb{C}\,((x_0, b_1, \ldots, b_n) \in A)\}.$$

- That is, for $\psi(x_1, \ldots, x_n) \equiv \exists x_0 \varphi(x_0, x_1, \ldots, x_n)$,

$$\pi[A] := \{\bar{b} \in \mathbb{C}^n : \mathbb{C} \models \psi(\bar{b})\}.$$

- By QE, ψ is equivalent to a quantifier-free formula, and so $\pi[A]$ is again constructible.

- Hilbert's 17th problem (theorem) says that given a polynomial $p(T) \in \mathbb{R}[T]$ with $|T| \geq 1$, if $p(a) \geq 0$ for all $a \in \mathbb{R}$, then p is a sum of squares of rational polynomials in $\mathbb{R}(T)$.
- It was first proved by Artin in 1927.

Example

Motzkin provided an example of polynomial having non-negative values for reals but not sum of squares of polynomials over $\mathbb{R}$:

$$x^4y^2+x^2y^4+1-3x^2y^2 = \frac{x^2y^2(x^2+y^2+1)(x^2+y^2-2)^2+(x^2-y^2)^2}{(x^2+y^2)^2}.$$

- Using QE of RCF, we will give a model theoretic proof of Hilbert's 17th problem (by Robinson in 1955).
- QE of RCF implies that RCF is model-complete:
- For $M, N \models RCF$ with $M \subseteq N$, then M is an elementary substructure of N, denoted by $M \prec N$, that is, for any for any formula $\varphi(x)$ and $a \in M^{|x|}$,

$$M \models \varphi(a) \Leftrightarrow N \models \varphi(a).$$

- Suppose there is a polynomial $p(T) \in \mathbb{R}[T]$ with $T = (T_0, \ldots, T_{n-1})$ such that
  - $p(a) \geq 0$ for all $a \in \mathbb{R}^n$,
  - $p \neq q_0^2 + \cdots + q_m^2$ for all $q_0, \ldots, q_m \in \mathbb{R}(T)$.

Fact

For a field F and $a \in F$, suppose -1 is not a sum of squares in F and a is not a sum of squares in F. Then, there is a linear order $<$ on F such that $(F, <)$ is an ordered field with $a < 0$.

- By the above fact, there is a linear order $<'$ on $\mathbb{R}(T)$ such that $(\mathbb{R}(T), <')$ is an ordered field with $p(T) <' 0$.
- Note that $<'$ is extending the linear order $<$ on $\mathbb{R}$ because for any real number a, either a or $-a$ is a square of real number.

Fact

*Any formally real field F has a real closure (**unique** up to isomorphism over F), which is a real closed algebraic extension of F.*

- Let $(F, <')$ be the real closure of $(\mathbb{R}(T), <')$, extending $(\mathbb{R}, <)$
- By model-completeness, $(F, <')$ is an elementary extension of $(\mathbb{R}, <)$.
- By the choice of $p \in \mathbb{R}[T]$, we have that

$$(\mathbb{R}, <) \models \forall x \, (p(x) \geq 0) \, .$$

- Since $\mathbb{R} \prec F$, we have that

$$(F, <') \models \forall x \, (p(x) \geq 0) \, ,$$

- Since $T_0, \ldots, T_{n-1} \in \mathbb{R}(T) \subseteq F$, for $T := (t_0, \ldots, t_{n-1})$

$$(F, <') \models 0 \leq' p(T),$$

which contradicts with $p(T) <' 0$.

[1] E. Artin,
Über die Zerlegung definiter Funktionen in Quadrate, Abh. Math. Sem. Univ. Hamburg, **5** (1927), 100-115.

[2] D. Marker,
Model Theory: An Introduction, Graduate Texts in Mathematics 217, Springer, 2002.

[3] A. Robinson,
On ordered fields and definite functions, Math. Ann. **130** (1955), 257-271.

[4] A. Tarski,
A decision method for elementary algebra and geometry, 2nd ed. University of California Press, 1951.

[5] K. Tent and M. Ziegler,
A course in model theory, Lecture Notes in Logic, **40**, Cambridge University Press, 2012, 248 pp.

Thank you for your listening
Happy Logic Day