INTRODUCTION TO MODEL THEORY FOR REAL ANALYTIC GEOMETERS

DEIRDRE HASKELL

1. Basic Definitions

Model theory uses mathematical logic to formalise the underlying language of mathematics. The natural objects of study are the definable sets, and the key is to choose an appropriate language so that the definable sets are both tractable and the natural objects of study in another branch of mathematics. Consider the following example of a mathematical statement:

> for every x, if x is greater than 0 then there is a y such that y is the square root of x.

For this statement to mean anything, first of all we need to be working in a context in which "the square root" makes sense. Thus we need to have a multiplication, or an interpretation of multiplication by some other binary function. Once the statement has meaning, we can address the question of whether or not it is true. This depends on the set with respect to which we make the statement.

We thus see that many mathematical assertions incorporate three facets.

(1) The logical language, which is always present, consists of the *connectives:* $\vee$ (disjunction), $\wedge$ (conjunction), $\rightarrow$ (implication), $\neg$ (negation), the *quantifiers:* $\forall$ (universal), $\exists$ (existential), and *variables.*
(2) A language for a particular mathematical context includes a list of relation symbols $R_1, R_2, \ldots$ of given arity, function symbols $f_1, f_2, \ldots$ of given arity and constant symbols $c_1, c_2, \ldots$. For example, to talk about rings we need to have both an addition and a multiplication, and the identities for each operation. Thus the language of rings $\mathcal{L}_r = (+, \cdot, 0, 1)$, where $+$ and $\cdot$ are binary relation symbols, and 0 and 1 are constant symbols. The language of ordered rings $\mathcal{L}_{or} = (<, +, \cdot, 0, 1)$ includes a binary relation symbol for the ordering.
(3) A set, called the *universe,* over which the variables are allowed to range.

A *structure* $\mathcal{M}$ for a language $\mathcal{L}$ consists of a set M and an interpretation for each symbol of the language:

$$\mathcal{M} = (M, R_1^{\mathcal{M}}, \ldots, f_1^{\mathcal{M}}, \ldots, c_1^{\mathcal{M}}, \ldots) .$$

We will usually not distinguish between the formal symbol for the relations, functions and constants and their interpretation in any particular structure, except as is standard in the

Date: January 19, 2009.

I would like to express my debt to the works of David Marker [6], [7]. He has greatly influenced my understanding of model theory and how to present it. If I have copied verbatim from him anywhere, I apologize.

given mathematical context. For example, $\mathcal{M}_2 = (M_2, +, \cdot, \mathbf{0}_2, I_2)$, where M_2 is the set of 2×2 matrices over a given field, $+$ and $\cdot$ are interpreted as matrix addition and multiplication, $\mathbf{0}_2$ is the zero matrix and I_2 is the identity matrix, is a structure in the language of rings. Also $\mathcal{C} = (\mathbb{C}, +, \cdot, 0, 1)$ is a structure in the language of rings, with the obvious interpretations of the symbols.

Since a structure consists of both a set which is its universe and a set which is the interpretation of the language, we can get subsets in two different ways. If we change the language, we say that the corresponding structure is a *reduct* of the original one. Thus if we forget the multiplicative structure on the complex numbers, $\mathcal{C} = (\mathbb{C}, +, 0)$ is a reduct of $\mathcal{C} = (\mathbb{C}, +, \cdot, 0, 1)$. If we take a subset of the universe, the new structures is called a *substructure* of the old one, provided the interpretation of the symbols of the language remains the same from one set to the other. Thus $\mathcal{R} = (\mathbb{R}, +, \cdot, 0, 1)$, the real field, is a substructure of the complex field $\mathcal{C} = (\mathbb{C}, +, \cdot, 0, 1)$; however $(\mathbb{Z}_p, +, \cdot, 0, 1)$ with addition and multiplication modulo the prime p is not a substructure of $\mathcal{R} = (\mathbb{R}, +, \cdot, 0, 1)$.

Terms in the language $\mathcal{L}$ are built up by finitely many applications of function symbols to the appropriate number of variables and constant symbols. We allow ourselves to use parentheses as necessary for readability of terms. Thus $(x \cdot y + 1) \cdot z$ is a term in $\mathcal{L}_r$. An *atomic formula* is an application of a relation symbol or equality to terms: $(x \cdot y + 1) \cdot z = 0$ is an atomic formula in the language $\mathcal{L}_r$ and $(x \cdot y + 1) \cdot z < 1$ is an atomic formula in $\mathcal{L}_{or}$. *Formulae* are formed by finitely many applications of connectives and quantifiers to atomic formulae. Thus

$$\begin{aligned} \varphi(x, y) \quad &\text{is} \quad \neg(x = 0) \to x \cdot y = 1 \\ \psi \quad &\text{is} \quad \forall x \exists y (x = y \cdot y) \end{aligned}$$

are both formulae in $\mathcal{L}_r$. Informally, formulae are the things we can say in the language; terms are the objects about which we speak. In $\mathcal{L}_r$, the terms are polynomials, and the atomic assertions we can make about the polynomials are that they are, or are not equal to zero.

The above formula ψ is an example of a *sentence* as all of its variables are within the scope of a quantifier; a sentence is a formula with no free variables. As such, it makes sense to ask whether the sentence is true in a particular structure. In the structure $\mathcal{C} = (\mathbb{C}, +, \cdot, 0, 1)$, the variables are allowed to range over the universe $\mathbb{C}$, and then the sentence makes a true assertion about the complex numbers. In the structure $\mathcal{R} = (\mathbb{R}, +, \cdot, 0, 1)$, the variables are allowed to range over the universe $\mathbb{R}$, and the sentence is not true. We write

$$\begin{aligned} \mathcal{C} &\models \forall x \exists y (x = y \cdot y) \ , \\ \text{and} \quad \mathcal{R} &\not\models \forall x \exists y (x = y \cdot y) \ , \end{aligned}$$

and say that $\mathcal{C}$ is a model for the sentence ψ, or that ψ is true in $\mathcal{C}$.

Given a structure $\mathcal{M}$ in a language $\mathcal{L}$, any sentence in the language will be either true or false in $\mathcal{M}$. We call the set of all sentences which are true in $\mathcal{M}$ the *theory* of $\mathcal{M}$, and write $\mathrm{Th}(\mathcal{M})$. In general, any set of sentences forms a theory; we say that the theory is *satisfiable* if there is a structure in which all the given sentences are true. We call this structure a *model* for the theory. We say that a theory T is *complete* if, for every sentence in the language, either the sentence or its negation is in T. The theory T is *axiomatized* by a smaller set of sentences Δ if, for any structure $\mathcal{M}$, $\mathcal{M} \models T$ if and only if $\mathcal{M} \models \Delta$.

Problem 1. Choose an appropriate language and write axioms for the theories of groups, rings, fields, vector spaces, algebraically closed fields. Consider how the character of the axioms changes if you choose a different language.

In the above example, we can remove one of the quantifiers, and consider the formula $\psi(x)$ which is $\exists y(x = y \cdot y)$. It no longer makes sense to ask if the formula is true in a particular structure, as the answer depends on the choice of x. Instead the formula defines a set in any structure:

$$\{x \in \mathbb{C} : \exists y(x = y \cdot y)\} = \mathbb{C} \ ,$$

$$\{x \in \mathbb{R} : \exists y(x = y \cdot y)\} = [0, \infty) \ .$$

In general, if $\mathcal{M} = (M, \mathcal{L})$ is a structure in the language $\mathcal{L}$, a subset X of M^n is *definable* if there is a formula $\psi(x_1, \ldots x_n)$ in $\mathcal{L}$ such that

$$X = \{x \in M^n : \mathcal{M} \models \psi(x)\} \ .$$

It is often convenient to have a particular set A in mind as a subset of the universe, and then allow parameters from this set when constructing terms. (Formally, this is done by increasing the set of constant symbols to include symbols for each element of A and interpreting these symbols as the indicated element.) A set which is defined by a formula with parameters in the set A is said to be A-definable. A set which can be defined without parameters is called $\emptyset$-definable (pronounced "zero-definable"). Thus $\{x \in \mathbb{R} : x < \pi\}$ is $\{\pi\}$-definable in $\mathcal{L}_{or}$; $\{x \in \mathbb{R} : x < \sqrt{2}\}$ is defined here by a formula with the parameter $\sqrt{2}$, but in fact is $\emptyset$-definable, since it is the same as $\{x \in \mathbb{R} : x < 0 \vee x = 0 \vee x \cdot x < 1 + 1\}$.

The role of the logical symbols in the language can be understood geometrically in the context of the collection of definable sets. Consider $\mathcal{M} = (M, \mathcal{L})$ an $\mathcal{L}$-structure, $\varphi(x)$, $\psi(x)$ formulae with n free variables, $X = \{x \in M^n : \mathcal{M} \models \varphi(x)\}$, $Y = \{x \in M^n : \mathcal{M} \models \psi(x)\}$. The conjunction, disjunction and negation give the intersection, union and complement respectively:

$$\{x \in M^n : \mathcal{M} \models \varphi(x) \wedge \psi(x)\} = X \cap Y \ ,$$

$$\{x \in M^n : \mathcal{M} \models \varphi(x) \vee \psi(x)\} = X \cup Y \ ,$$

$$\{x \in M^n : \mathcal{M} \models \neg\varphi(x)\} = M^n \setminus X \ .$$

(These are called the boolean operations.) Existential quantification is a projection:

$$\{(x_2, \ldots, x_n) \in M^{n-1} : \mathcal{M} \models \exists x_1 \varphi(x_1, x_2, \ldots, x_n)\}$$

is the projection of X onto the last $n-1$ coordinates. Universal quantification can be seen geometrically after observing that it can be replaced by an existential quantifier as follows: $\forall x \varphi(x)$ is equivalent to $\neg\exists x \neg\varphi(x)$. Thus

$$\{(x_2, \ldots, x_n) \in M^{n-1} : \mathcal{M} \models \forall x_1 \varphi(x_1, x_2, \ldots, x_n)\} =$$
$$\{(x_2, \ldots, x_n) \in M^{n-1} : \mathcal{M} \models \neg\exists x_1 \neg\varphi(x_1, x_2, \ldots, x_n)\}$$

is the complement of the projection of the complement of X. For example, in the language $\mathcal{L}_r$, let $\varphi(x_1, x_2)$ be the formula $x_1^2 + x_2^2 = 1$. In the structure $\mathcal{R} = (\mathbb{R}, +, \cdot, 0, 1)$, $X = \{(x_1, x_2) \in \mathbb{R}^2 : \varphi(x_1, x_2)\}$ is a circle, and $\mathbb{R}^2 \setminus X$ is the complement of the circle. The projection of X onto the second coordinate, which of course is the interval $[-1, 1]$, is given by $\{x_2 \in \mathbb{R} : \exists x_1(x_1^2 + x_2^2 = 1)\}$. In particular, the interval is a definable set in the language $\mathcal{L}_r$. Notice that this is not immediately obvious, since the natural "definition" of the interval as $\{x \in \mathbb{R} : -1 \leq x \leq 1\}$ uses a formula in the language of *ordered* rings, which is not a formula in the language without the ordering. The projection of the complement of X is the real line, and hence the set defined by $\forall x_1 \varphi(x_1, x_2)$ is the empty set.

Problem 2. Let $X \subseteq \mathbb{R}^n$ be an A-definable set in the language of ordered rings. Show that the topological closure of X is also A-definable.

The logical language described so far is called first-order logic. It has its limitations, the most fundamental one being that in it, we cannot quantify over subsets of the universe. Thus, for example, we cannot state the completeness property of the real numbers — all bounded subsets of $\mathbb{R}$ have a least upper bound — since, however, it is formulated, it requires referring to all subsets of $\mathbb{R}$. First-order logic is nevertheless still currently the logic of choice for working mathematicians, primarily because it has the twin properties of completeness and compactness. Gödel's completeness theorem ties the model theoretic notion of satisfiability to the proof-thoeretic notion of consistency. In these lectures, we are not concerned with a formal notion of proof, but whatever a "proof" is, it must be a finite object.

Theorem 1. *Let T be a theory. Then T is satisfiable (has a model) if and only if T is consistent (does not prove a contradiction).*

The completeness theorem gives a very easy proof of the compactness theorem, which is fundamental to model theory.

Theorem 2. *Let T be a theory. Then T is satisfiable if and only if every finite subset of T is satisfiable.*

Proof. One direction is immediate. To prove the other direction, suppose for contradiction that every finite subset of T is satisfiable but T is not. By the completeness theorem, T must fail to be consistent, so proves a contradiction. As any proof can only involve finitely many sentences from T, there is a finite subset of T which is inconsistent, and hence not satisfiable. This contradicts the hypothesis. □

A typical example of the use of the compactness theorem is outlined in the following problem.

Problem 3. Let T be the theory of $\mathbb{R}$ in the language of ordered rings $\mathcal{L}_{or}$. Adjoin a new constant symbol c to the language and write sentences ϕ_k which assert that c is larger than k. Deduce from the compactness theorem that there is a model of T in which there is an element larger than every real number.

2. Some examples of structures

At this point it is useful to catalogue some further examples of languages, structures and theories which are particularly relevant in the study of o-minimality. We have already seen the real numbers, which I will write $\mathcal{R} = (\mathbb{R}, +, \cdot, 0, 1)$ as a structure in the language of rings and its expansion $\mathcal{R}_< = (\mathbb{R}, +, \cdot, 0, 1, <)$ as a structure in the language of ordered rings. $\mathcal{R}_<$ is called an *expansion by definition* of $\mathcal{R}$, as the interpretation of the symbol $<$ is a definable set in $\mathcal{R}$; $\mathrm{Th}(\mathcal{R}) \models \forall x \, \forall y \, \big(x < y \leftrightarrow \exists z \, (x + z^2 = y)\big)$. $\mathrm{Th}(\mathcal{R})$ is called the theory of *real closed fields* RCF; $\mathrm{Th}(\mathcal{R}_<)$ is the theory of *real closed ordered fields* RCOF. The real numbers contain the real algebraic numbers as a substructure; $\mathcal{R}^{\mathrm{alg}} = (\mathbb{R}^{alg}, +, \cdot, 0, 1)$, and similarly ${\mathcal{R}^{\mathrm{alg}}}_<$. $\mathcal{R}^{\mathrm{alg}}$ is a model of RCF and ${\mathcal{R}^{\mathrm{alg}}}_<$ is a model of RCOF.

Problem 4. To be more precise, a field is called *formally real* if -1 cannot be written as a sum of squares of elements of the field. This is equivalent to saying there is an ordering on the field which is compatible with the field operations. State precisely what this means and prove it. (Hint: an ordering can be defined by stating the set of positive elements.)

A formally real field F is *real closed* if no algebraic extension of F is formally real. It is somewhat more work to prove that this is equivalent to saying that for every $a \in F$, either a or $-a$ is a square, and every odd degree polynomial over F has a root in F. This latter statement can be expressed by infinitely many sentences in first-order logic. It is this theory that is called RCF. The fact that $\mathrm{Th}(\mathcal{R})$ is RCF follows from Section 4.

An example of a structure with a larger universe is given by the set of rational functions over the reals, $\mathbb{R}(X)$. $\mathbb{R}(X)$ is clearly the universe of a structure in the language of rings. It can also be made into an ordered field; in fact there are infinitely many different possible orderings which respect the field structure. Here, the symbol X can be either a single indeterminate or a finite tuple of indeterminates. If $<_1$ and $<_2$ are two different orderings on $\mathbb{R}(X)$, both of which extend the ordering on $\mathbb{R}$, this gives an example of two structures $(\mathbb{R}(X), <_1)$, $(\mathbb{R}(X), <_2)$ with a common substructure $(\mathbb{R}, <)$, for which neither is a substructure of the other. $(\mathbb{R}(X), \mathcal{L}_{or})$ is not a model of RCF; indeed, it is not true in $\mathbb{R}(X)$ that $x < y \leftrightarrow \exists z(x + z^2 = y)$. For example, take an ordering on $\mathbb{R}(X)$ in which the element X is positive, so $0 < X$. But there is no element z with $z^2 = X$. In fact, $\mathbb{R}(X)$ can be extended to a real closed field by formally adjoining square roots for positive elements, and roots of odd-degree equations.

Problem 5. Give an explicit description of the real closure of $\mathbb{R}(X)$, given a choice of ordering.

We move into the realm of analysis when we increase the language by adding symbols for new functions which are not definable in $\mathcal{L}_{or}$. For example, we can add a symbol for a function exp which is intended to be interpreted by the exponential function on $\mathbb{R}$. Thus $\mathcal{R}_{\exp} = (\mathbb{R}, +, \cdot, 0, 1, \exp)$ and $\mathcal{R}_{\exp,<} = (\mathbb{R}, +, \cdot, 0, 1, <, \exp)$ are expansions of $\mathcal{R}$ and $\mathcal{R}_<$ respectively. The theory of $\mathcal{R}_{\exp,<}$ will include sentences stating algebraic properties of the exponential function; for example, $\forall x, y \; \exp(x + y) = \exp(x) \cdot \exp(y)$. It will not include analytic properties; for example $\exp(1) = \lim_{x \to 0}(1 + x)^{\frac{1}{x}}$, as this is not a formula in the language $\mathcal{L}_r$.

We can even add infinitely many function symbols, as in the structure called "R-an", defined as follows. Write $\mathcal{F}_n$ for the set of elements of the ring of formal power series in n variables over $\mathbb{R}$, $\mathbb{R}[[X_1, \ldots, X_n]]$, which converge in a neighbourhood of $[-1, 1]^n$. The language $\mathcal{L}_{\mathrm{an}}$ consists of $\mathcal{L}_{\mathrm{or}}$ together with a constant symbol for every real number and, for every natural number n, a function symbol f for every element of $\mathcal{F}_n$. The structure $\mathcal{R}_{\mathrm{an}}$

interprets the symbols of $\mathcal{L}_{or}$ in the usual way, and interprets each function symbol by the corresponding restricted analytic function

$$f(x) = \begin{cases} \sum f_\nu x^\nu, & \text{if } |x_i| < 1 \text{ for all } i; \\ 0, & \text{otherwise.} \end{cases}$$

Notice that in this case we have defined a language with uncountable cardinality, which is much bigger than any other example we have looked at until now. The language $\mathcal{L}_{\mathrm{an}}^{\mathrm{D}}$ contains in addition a binary function symbol D which, in the structure $\mathcal{R}_{\mathrm{an}}^{\mathrm{D}}$ is interpreted as the restricted division function:

$$D(x,y) = \begin{cases} x/y, & \text{if } |x| \le |y| \le 1, y \neq 0; \\ 0, & \text{otherwise.} \end{cases}$$

Problem 6. Give an explicit construction which replaces occurrences of the symbol D in a formula by an $\mathcal{L}_{an}$-formula with extra variables. Thus an $\mathcal{L}_{an}^{\mathrm{D}}$-formula is equivalent to an $\mathcal{L}_{an}$-formula, but with more existential quantifiers. We will use this construction in Section 5.

Finally, we will look at a rather different example, which also arises in the study of o-minimal structures. To the language of ordered rings $\mathcal{L}_{or}$ add a new unary predicate symbol S, a unary function symbol λ and a family of unary predicate symbols P_n for n any natural number greater than 1. As well as the axioms for real closed ordered fields, the theory includes axioms to say that $2 \in S$, S is a multiplicative subgroup of the set of positive elements of the ring, and the following:

T1 $\forall x \, (1 < x < 2 \rightarrow x \notin S)$;
T2 $\forall x \, \big(x > 0 \rightarrow \exists y \, (y \in S \wedge y \le x < 2y)\big)$;
T3 $\forall x \, \big(P_n(x) \rightarrow \exists y \, (y \in S \wedge y^n = x)\big)$;
T4 $\forall x \forall y \big(\lambda(x) = y \leftrightarrow (x < 0 \wedge y = 0) \vee (x \ge 0 \wedge y \in S \wedge y \le x < 2y)\big)$.

The intended model is the real numbers with the predicate S interpreted as the integer powers of 2, $2^{\mathbb{Z}}$. The function λ then assigns to each positive real number x the highest power of 2 less than or equal to x, and the set P_n is interpreted by the set $2^{n\mathbb{Z}}$. I will call this language $\mathcal{L}_{two}$, and the theory outlined here T_{two}.

3. Model completeness and quantifier elimination

We now turn to look at structural properties that structures may have. Let $\mathcal{M} = (M, \mathcal{L})$, $\mathcal{N} = (N, \mathcal{L})$ be two structures in the same language. As observed before, we say that $\mathcal{M}$ is a substructure of $\mathcal{N}$, and write $\mathcal{M} \subseteq \mathcal{N}$, if $M \subseteq N$ and all the symbols in $\mathcal{L}$ are interpreted in the same way in $\mathcal{M}$ as in $\mathcal{N}$. More generally, a map $\sigma : \mathcal{M} \rightarrow \mathcal{N}$ is an *embedding* if σ is an injective function from M to N which preserves the interpretation of all of the symbols of the language. That is, for every relation symbol R, every function symbol f, every constant symbol c and every tuple $a \in M^n$ of the appropriate arity,

$$\mathcal{M} \models R^{\mathcal{M}}(a) \Longrightarrow \mathcal{N} \models R^{\mathcal{N}}(\sigma(a)),$$
$$\sigma(f^{\mathcal{M}}(a)) = f^{\mathcal{N}}(\sigma(a)),$$
$$\sigma(c^{\mathcal{M}}) = c^{\mathcal{N}}.$$

Thus M is a substructure of $\mathcal{N}$ if the inclusion map is an embedding. We say that σ is an isomorphism between $\mathcal{M}$ and $\mathcal{N}$ if it is a bijection. It is fairly easy to show that an isomorphism perserves the truth value of all formulae. Consequently, if $\sigma : \mathcal{M} \to \mathcal{M}$ is an isomorphism fixing each element of a subset A of M, and X is an A-definable set, then $\sigma(X) = X$; that is, X is fixed setwise by the isomorphism.

Two structures are isomorphic if there is an isomorphism between them. A weaker relation between structures is that of *elementary equivalence*. $\mathcal{M}$ and $\mathcal{N}$ are elementarily equivalent, written $\mathcal{M} \equiv \mathcal{N}$ if, for every sentence φ in the language, $\mathcal{M} \models \varphi$ if and only if $\mathcal{N} \models \varphi$. That is, $\mathrm{Th}(\mathcal{M}) = \mathrm{Th}(\mathcal{N})$. Certainly if $\mathcal{M}$ and $\mathcal{N}$ are isomorphic then they are elementarily equivalent. The converse is not true; for example, $\mathcal{R}^{alg} \equiv \mathcal{R}$, but they cannot be isomorphic just for cardinality reasons.

An embedding $\sigma : \mathcal{M} \to \mathcal{N}$ is an *elementary embedding* if σ is an embedding with respect to the language $\mathcal{L}_M$ with constants for all elements of M, and $\mathcal{M}$ and $\mathcal{N}$ are elementarily equivalent in $\mathcal{L}_M$. If $\mathcal{M}$ is a substructure of $\mathcal{N}$, we say that $\mathcal{M}$ is an *elementary substructure* of $\mathcal{N}$, and write $\mathcal{M} \preccurlyeq \mathcal{N}$, if the inclusion map is an elementary embedding. That is, $\mathcal{M}$ and $\mathcal{N}$ are elementarily equivalent as structures in the language with constants added for every element of M.

Definition 3. We say that a theory is *model complete* if, for every $\mathcal{M}$ and $\mathcal{N}$ models of the theory, if $\mathcal{M} \subseteq \mathcal{N}$ then $\mathcal{M} \preccurlyeq \mathcal{N}$.

A beautiful example of the power of model completeness is given by the following proof of the solution to Hilbert's seventeenth problem.

Theorem 4. *Let $f(X) \in \mathbb{R}[X]$ be a polynomial in n variables, and suppose that for all $x \in \mathbb{R}^n$, $f(x) \geq 0$. Then there exist rational functions $g_1, \ldots, g_k \in \mathbb{R}(X)$ such that*

$$f(X) = \sum_{i=1}^{k} g_i(X)^2 \ .$$

Proof. The proof uses that fact that the theory of real closed fields, which is $\mathrm{Th}(\mathcal{R})$, is model complete, as well as algebraic facts about the set of all orderings on a field.

Suppose for contradiction that f cannot be written as a sum of squares of rational functions. Then there is an ordering $<^*$ on $\mathbb{R}(X)$ which extends the ordering on $\mathbb{R}$ and with the property that $f <^* 0$. The ordered field $(\mathbb{R}(X), <^*)$ is not real closed, as it is not the case that every odd degree polynomial has a root in $\mathbb{R}(X)$. But it can be extended to a real closed field L. In L, the sentence φ: $\exists x(f(x) < 0)$ is true, since it is realised by the rational function X in $\mathbb{R}(X)$. Notice that φ is a sentence with parameters from $\mathbb{R}$ (the coefficients of the polynomial f). Now $\mathcal{R}$ is a substructure of L, so by model completeness is an elementary substructure. Hence the sentence φ is true also in $\mathcal{R}$. Thus there is a tuple $x \in \mathbb{R}^n$ with $f(x) < 0$. This contradicts the assumption on f. $\square$

Now I want to consider equivalent ways to state the definition of model completeness and the related, but stronger, property of quantifier elimination. This will give us different ways to prove that a theory has one or the other of these properties.

Definition 5. Let T be a theory in a language $\mathcal{L}$.

(1) T is *model complete* if, for all models $\mathcal{M}$, $\mathcal{N}$ of T and all $\mathcal{L}$-formulae $\varphi(x)$, if $\mathcal{M} \subseteq \mathcal{N}$ then for all $m \in M^n$, $\mathcal{N} \models \varphi(m)$ if and only if $\mathcal{M} \models \varphi(m)$.
(2) T has *quantifier elimination* if, for all models $\mathcal{M}$, $\mathcal{N}$ of T and all $\mathcal{L}$-formulae $\varphi(x)$, if $\mathcal{A}$ is a common substructure of $\mathcal{M}$ and $\mathcal{N}$ then for all $a \in A^n$, $\mathcal{N} \models \varphi(a)$ if and only if $M \models \varphi(a)$.

Note that this is not the standard definition of qunatifier elimination; I just state it this way to emphasise the comparison with model completeness. Quantifier elimination clearly implies model completeness. We shall see later that the theory of $\mathcal{R}$ is model complete but does not have quantifier elimination, whereas the theory of $\mathcal{R}_<$ does eliminate quantifiers. An example illustrates how we can see the difference in the above definitions. Consider the field $F = \mathbb{R}(X)$. In F, X is not a sum of squares, so one can formally adjoin a square root for either X or $-X$. Let $F_1 = F(\sqrt{X})$, $F_2 = F(\sqrt{-X})$. F_1 and F_2 are both formally real, so can be ordered. Let $\widetilde{F_1}$, $\widetilde{F_2}$ be real closed fields containing F_1, F_2 respectively, with the respective orderings. Then $\mathbb{R}(X)$ is a common substructure of both $\widetilde{F_1}$ and $\widetilde{F_2}$. The formula $\varphi : \exists y(y^2 = X)$ has parameters in $\mathbb{R}(X)$. But $\widetilde{F_1} \models \varphi$, whereas $\widetilde{F_2} \not\models \varphi$. Thus the theory does not satisfy the criterion for quantifier elimination. This example says nothing about the criterion for model completeness, as $\mathbb{R}(X)$ is not a submodel of either $\widetilde{F_1}$ or $\widetilde{F_2}$. The example does not arise in the language with a symbol for the ordering, as in $(\mathbb{R}(X), <)$, X is definitely either positive or negative, so only one of F_1 or F_2 is a formally real field.

The following model-theoretic criteria for model-completeness and quantifier elimination are often useful for proving that a theory has these properties.

Theorem 6. *Let T be a complete theory in a language $\mathcal{L}$.*

(1) *T is model-complete if and only if the following property holds. Let $\mathcal{M}, \mathcal{N} \models T$, $\mathcal{M} \subset \mathcal{N}$, $\varphi(x, y)$ a quantifier-free $\mathcal{L}$-formula and m a tuple from M. If $\mathcal{N} \models \exists y \varphi(m, y)$ then $\mathcal{M} \models \exists y \varphi(m, y)$.*
(2) *T has quantifier elimination if and only if the following property holds. Let $\mathcal{M}, \mathcal{N} \models T$, $\mathcal{A}$ a common substructure of $\mathcal{M}$ and $\mathcal{N}$, $\varphi(x, y)$ a quantifier-free $\mathcal{L}$-formula and a a tuple from A. Then $\mathcal{N} \models \exists y \varphi(a, y)$ if and only if $\mathcal{M} \models \exists y \varphi(a, y)$.*

This theorem says that, in order to verify that a theory is model-complete or has quantifier elimination, we only need to check the condition on formulae with one (block of) existential quantifier.

Model-completeness and quantifier elimination can be restated in a more syntactic form, which explains the terminology for quantifier elimination, and also can be used to interpret the properties as statements about the definable sets in a model of the theory.

Theorem 7. *Let T be a complete theory in a language $\mathcal{L}$.*

(1) *T is model complete if and only if for any $\mathcal{L}$-formula $\varphi(x)$ there is a quantifier-free $\mathcal{L}$-formula $\psi(x, y)$ such that $T \models \forall x\, (\varphi(x) \leftrightarrow \exists y\, \psi(x, y))$.*
(2) *T has quantifier elimination if and only if for any $\mathcal{L}$-formula $\varphi(x)$ there is a quantifier-free $\mathcal{L}$-formula $\theta(x)$ such that $T \models \forall x\, (\varphi(x) \leftrightarrow \theta(x))$.*

Consider $X = \{x \in M : \mathcal{M} \models \varphi(x)\}$. If $\mathcal{M}$ is a model of the model-complete theory T, then $X = \{x \in M : \exists y\, \psi(x, y)\}$; that is, X is the projection of a quantifier-free definable set. For example, in $\mathcal{R}_{\text{an}}$, the quantifier-free definable sets are the analytic sets; their projections are called subanalytic sets. Thus the model-completeness of $\text{Th}(\mathcal{R}_{\text{an}})$ implies that the complement of a subanalytic set is also a subanalytic set. This is a result which is called Gabrielov's "theorem of the complement".

If the theory T has quantifier elimination then X would be quantifier-free definable, as is any projection of X. In $\mathcal{R}$, the quantifier-free definable sets are the semialgebraic sets. Thus quantifier elimination for $\text{Th}(\mathcal{R})$ implies that projections of semialgebraic sets are semialgebraic.

Finally, observe that we began this section by saying that a theory is model-complete if every substructure is an elementary substructure; more generally, if every embedding is elementary. To formulate a parallel statement for quantifier elimination we need the notion of a saturated structure. A structure $\mathcal{M}$ in a language $\mathcal{L}$ is *κ-saturated* if for every consistent set of formulae with parameters in a subset A of M with cardinality at most κ, there is an element in M which realizes all of the formulae simultaneously.

Theorem 8. *The theory T has quantifier elimination if and only if the following property holds. Let $\mathcal{M}$ be a model of T, $\mathcal{A} \subset \mathcal{M}$, $\mathcal{N}$ a $|M|$-saturated model of T, $\sigma : \mathcal{A} \to \mathcal{N}$ an elementary mapping. For any $a \in M \setminus A$, σ can be extended to an elementary embedding from $A(a)$, the structure generated by a over A, into N.*

Problem 7. Prove the equivalence of the different statements for model completeness and quantifier elimination. Theorem 6 uses induction on the construction of formulas; Theorem 7 requires the compactness theorem.

4. The theory of real closed fields

We now look at examples of theories which we can prove to be model complete, or to have quantifier elimination. The first is the theory of real closed ordered fields, in the language of ordered rings. A field is said to be *real closed* if it has an ordering (is real) and no proper algebraic extension of it can be ordered. Both $\mathbb{R}$ and $\mathbb{R}^{alg}$ are examples of real closed fields. Any ordered field has an algebraic extension which is real closed.

Theorem 9. *The theory of real closed ordered fields,* $\text{Th}(\mathcal{R}_<)$*, has quantifier elimination.*

Proof. The proof uses Theorem 6. So let $\mathcal{M}$, $\mathcal{N}$ be two real closed ordered fields, $\mathcal{A}$ a common substructure of $\mathcal{M}$ and $\mathcal{N}$. Observe that, to say $\mathcal{A}$ is a substructure implies that it is closed under the operations of addition and multiplication, contains a 0 and a 1 and that there is an ordering on the universe. Furthermore, all universally axiomatised properties of these operations which hold in $\mathcal{M}$ are also true in $\mathcal{A}$. Thus $\mathcal{A}$ is an ordered integral domain. Now we use the following theorem about ordered fields.

Theorem 10. *An ordered integral domain $(A, <)$ has a unique real closure in the following sense: if $(R_1, <)$, $(R_2, <)$ are real closed ordered fields which are algebraic over A and contain A as an ordered substructure, then $(R_1, <)$ is isomorphic to $(R_2, <)$ over A.*

The algebraic closures of A in M and N respectively will each be real closed fields, and by the theorem, there is an isomorphism between them. Thus if a formula over A is realised by an element in M which is algebraic over A, there will be an element in N, also algebraic over A, which realises the same formula. So we can assume that A is in fact a real closed field.

Now let $\varphi(a, y)$ be a quantifier-free formula with parameters a from A, and assume that $\mathcal{M} \models \exists y \varphi(a, y)$. We need to examine carefully the possible form of the formula φ. As the language has only addition and multiplication as function symbols, the terms are polynomials in y, $p(y)$, with coefficients amongst the parameters a. The atomic formulae are of the form $p(y) = 0$ or $p(y) < 0$, and the negated atomic formulae can be rewritten positively as

$$\neg(p(y) = 0) \Leftrightarrow p(y) < 0 \vee -p(y) < 0;$$
$$\neg(p(y) < 0) \Leftrightarrow p(y) = 0 \vee -p(y) < 0.$$

By regrouping, the formula φ can be rewritten in *disjunctive normal form* as

$$\bigvee \left(p_1(y) = 0 \wedge \cdots \wedge p_k(y) = 0 \wedge q_1(y) < 0 \wedge \cdots \wedge q_\ell(y) < 0\right).$$

To satisfy a disjunction, just one of the disjuncts needs to be satisfied. Furthermore, in an ordered domain,

$$p_1(y) = 0 \wedge \cdots \wedge p_k(y) = 0 \Leftrightarrow p_1^2(y) + \cdots + p_k^2(y) = 0.$$

Thus we may assume that $\varphi(a, y)$ is the formula

$$p(y) = 0 \wedge \bigwedge_{i=1}^{\ell} q_i(y) < 0.$$

We assumed $\mathcal{M} \models \exists y \varphi(a, y)$, so let $b \in M$ be the element such that $\varphi(a, b)$.

First suppose that p is a non-trivial polynomial. Since $p(b) = 0$, this means that b is algebraic over A. By our assumption, then $b \in A$, so we are done.

Now suppose p is trivial, so we can assume that b is not algebraic over A. Each polynomial q_i can be factored over M as a product of linear and quadratic factors. Thus q_i can only change sign at finitely many points, and these points are algebraic over A, hence in A. Thus for each i, there are c_i, d_i in A with $c_i < b < d_i$ and $q_i(x) < 0$ for all $x \in (c_i, d_i)$. Let $c = \max\{c_i\}$, $d = \min\{d_i\}$. Then $c < b < d$ and for all $x \in (c, d)$, $q_i(x) < 0$ for all i. Thus the interval (c, d) is nonempty, so in fact there is an element $b' \in A$ with $c < b' < d$ and $\varphi(a, b')$ holds, as required. $\square$

We observed in Section 2 that the ordering $<$ is a definable predicate in RCF. Theorem 9 proves that every formula φ in $\mathcal{L}_{\mathrm{or}}$ is equivalent in the theory RCOF to a quantifier-free formula ψ in $\mathcal{L}_{\mathrm{or}}$. If every occurrence of the formula $x < y$ in ψ is replaced by the formula $\exists z\,(x + z^2 = y)$, then the theorem tells us that every formula in $\mathcal{L}_r$ is equivalent in the theory RCF to a formula with just existential quantifiers. Thus RCF is model-complete in the language $\mathcal{L}_r$.

Problem 8. One consequence of Theorem 9 is that any infinite definable subset of the real line contains an interval, and hence the property for a set of being finite is first-order. This together with compactness can be used to prove the following result on uniform bounds.

> *Let $\mathcal{M} \models$ RCOF. Let $\varphi(x, y)$ be an $\mathcal{L}_{or}$-formula, where $x = (x_1, \ldots, x_n)$. Suppose that, for every $a \in M^n$, $\{y \in M : \varphi(a, y)\}$ is finite. Then there is a bound N such that for every $a \in M^n$, $|\{y \in M : \varphi(a, y)\}| \leq N$.*

5. The theory of the reals with restricted analytic functions

Theorem 11. [2] $\mathrm{Th}(\mathcal{R}_{\mathrm{an}}^{\mathrm{D}})$ *has quantifier elimination.*

Proof. (This presentation is adapted from the argument outlined in [4].) I will outline the main steps in the argument. We use Theorem 7. Thus we need to consider a quantifier-free $\mathcal{L}_{an}^{\mathrm{D}}$-formula $\psi(x, y)$ and show that there is a quantifier-free $\mathcal{L}_{\mathrm{an}}^{\mathrm{D}}$-formula $\theta(x)$ such that

$$\mathcal{R}_{\mathrm{an}}^{\mathrm{D}} \models \forall x \left(\exists y\, \psi(x, y) \leftrightarrow \theta(x)\right).$$

Step 1. Terms in the $\mathcal{L}_{an}^{\mathrm{D}}$ language are finite compositions of function symbols with the function symbol D. We remove occurrences of D, at the expense of introducing new existentially quantified variables. See Problem 6. Repeating this process as many times as there are occurrences of D in the formula ψ produces an $\mathcal{L}_{an}$-formula $\psi^*(x, y, z)$ with

$$\mathcal{R}_{\mathrm{an}}^{\mathrm{D}} \models \forall x\,(\exists y\, \psi(x, y) \leftrightarrow \exists y\, \exists z\, \psi^*(x, y, z).$$

From now on, we will assume that $\psi(x, y)$ is an $\mathcal{L}_{an}$-formula in $m + n$ variables.

We will now see how to reduce the number of y-variables by one, at the expense of re-introducing symbols D, but only involving the x variables. Repeating the argument finitely many times will give the required quantifier-free $\mathcal{L}_{\mathrm{an}}^{\mathrm{D}}$-formula θ.

Step 2. Using arguments as for real closed ordered fields, we can reduce to the case that ψ is a formula of the form

$$f_1(x, y) > 0 \wedge \cdots \wedge f_k(x, y) > 0,$$

where $f_1, \ldots, f_k$ are elements of $\mathcal{F}_{m+n}$. We focus on just one of these functions, say $f(x, y)$. Write

$$f(X, Y) = \sum_{i \in \mathbb{N}^n} a_i(X) Y^i,$$

where $a_i(X) \in \mathcal{F}_m$. As a ring, $\mathcal{F}_m$ is noetherian, hence there is $d \in \mathbb{N}$ such that, for every i with $|i| > d$,

$$a_i(X) = \sum_{|j|<d} c_{ij}(X) a_j(X)$$

with $c_{ij}(X) \in \mathcal{F}_m$.

Step 3. Observe that $f(X, Y)$ can be written as

$$f(X, Y) = \sum_{|i|<d} a_i(X) Y^i u_i(X, Y),$$

where each $u_i(X, Y)$ is a unit and there is an $\varepsilon > 0$ such that for all i, $u_i(\varepsilon X, \varepsilon Y) \in \mathcal{F}_{m+n}$.

Step 4. Let

$$S_j = \{x \in \mathbb{R}^m : |a_j(x)| = \max_{|i|<d}\{|a_i(x)|\}\}$$

and observe that S_j is a quantifer-free $\mathcal{L}_{an}$-definable set. Write

$$\widetilde{f}(X, V, Y) = Y^j u_j(X, Y) + \sum_{|i|<d, i \neq j} V_i Y^i u_i(X, Y)\ .$$

Then for $x \in S_j$ and $v_i(X) = D(a_i(X), a_j(X))$,

$$f(x,y) = \widetilde{f}(x, v(x), y)\ .$$

Notice that we have reintroduced terms involving D, but only in the X-variables and not in the Y-variables. Using a standard invertible transformation of the Y-variables, we can assume that the power series $\widetilde{f}(X,V,Y)$ is regular in Y_n.

Step 5. Apply the Weierstrass Preparation Theorem to get

$$\widetilde{f}(X,V,Y) = U(X,V,Y)G(X,V,Y)$$

where $U(X,V,Y)$ is a unit and $G(X,V,Y)$ is polynomial in the last variable Y_n. This step needs some care, as U and G do not, in general, converge on a neighbourhood of $[-1,1]^n$, hence are not elements of $\mathcal{F}_{m+d+n}$. Instead, one has to apply Weierstrass preparation locally, and use compactness of the interval $[-1,1]^n$ to find finitely many $\mathcal{L}_{\mathrm{an}}^{\mathrm{D}}$-formulae of the form below. With this caveat, we have that

$$\mathcal{R}_{\mathrm{an}} \models \forall x \big(\exists y_1 \dots y_n f(x,y) > 0 \leftrightarrow \bigvee_{|j|<d} x \in S_j \wedge \exists y_1 \dots y_n a_j(x) G(x, v, y_1, \dots, y_{n-1}, y_n) > 0\big).$$

Step 6 Since y_n occurs polynomially in the above formula, by quantifier elimination for RCOF, there is a quantifier-free $\mathcal{L}_{\mathrm{an}}^{\mathrm{D}}$-formula $\theta(x, y_1, \dots, y_{n-1})$ in which D is only applied to the variables involving x such that

$$\mathcal{R}_{\mathrm{an}} \models \forall x \left(\exists y_1 \dots y_n \psi(x,y) \leftrightarrow \exists y_1 \dots y_{n-1} \theta(x, y_1, \dots, y_{n-1}\right)$$

which completes the required reduction. □

Problem 9. Write $s(x)$ for the restriction of the sine function to the unit interval. Let $\mathcal{L}_s$ be the language of rings with a function symbol added for $s(x)$. Observe that Theorem 11 implies that the theory of $\mathbb{R}$ in the language $\mathcal{L}_s$ is o-minimal, though it does not imply model completeness. Trace through the proof of Theorem 11 in this context, and try to determine what further functions need to be added in order to get model completeness in the smaller language.

6. The theory of the reals with a predicate for the powers of 2

Theorem 12. [3] *The theory T_{two} has quantifier elimination in the language $\mathcal{L}_{two}$.*

Proof. I will use Theorem 8. Thus we consider models $\mathcal{M}$ and $\mathcal{N}$ of the theory with $\mathcal{N}$ a saturated model, and let $\mathcal{A}$ be a substructure of $\mathcal{M}$. Assume that $\sigma : \mathcal{A} \to \mathcal{N}$ is an elementary embedding. We must show that for any $c \in M \setminus A$, σ can be extended to an elementary embedding from $A\langle c\rangle$, the substructure generated by c over A, into $\mathcal{N}$. Without loss of generality, we may assume that $\mathcal{A} \subset \mathcal{N}$ and that $\sigma|_A$ is the identity. To begin with, it is helpful to describe explicitly the consequences for $\mathcal{A}$ of being a substructure of $\mathcal{M}$ in the language $\mathcal{L}_{two}$. A must be closed under the function symbols $+, -, \cdot$ and λ. (For convenience, I added the symbol for the additive inverse.) As we saw in the proof of Theorem 9, this means that A is an ordered integral domain. It also means that axiom T2 must hold for $S^{\mathcal{A}}$, as for every x, $\lambda(x)$ is the required element. Note that without the function λ in the language, this axiom would not hold for an arbitrary substructure. We know that $S^{\mathcal{A}}$ is closed under multiplication, but not that it is a group, as A itself is only a ring. In a model, we know from the definition that

$$P_n^{\mathcal{M}} = \{x \in M : \exists y \in S^{\mathcal{M}}(y^n = x)\}\ .$$

In a substructure, we can only say that

$$P_n^{\mathcal{A}} = \{x \in A : \exists y \in S^{\mathcal{M}}(y^n = x)\}\ .$$

Finally note that axioms T1 and T4 together imply that $S^{\mathcal{A}} = \{\lambda(x) : x \in A\}$.

In the proof of Theorem 9, we saw that the ordered ring structure extends uniquely to the real closed field containing A, and hence we can assume that A is a real closed field. We must do the same thing for the additional symbols in the language $\mathcal{L}_{two}$. By the two comments above, we only need to show that there is only one way to extend the function λ on A to the real closed field containing A. First look at $\mathrm{qf}(A)$, the field of fractions of A. For any nonzero $a, b \in A$,

$$0 < \lambda(a) \leq a < 2\lambda(a),$$
$$0 < \lambda(b) \leq b < 2\lambda(b), \text{ and hence}$$

$$\frac{1}{2} \cdot \frac{\lambda(a)}{\lambda(b)} < \frac{a}{b} < 2 \cdot \frac{\lambda(a)}{\lambda(b)}.$$

Closure under multiplication and the fact that $S^{\mathrm{qf}(A)} \supset S^A$ means that both ends of the inequality are in $S^{\mathrm{qf}(A)}$. If $a/b < \lambda(a)/\lambda(b)$ then $\lambda(a/b) = \lambda(a)/2\lambda(b)$. If $a/b \geq \lambda(a)/\lambda(b)$ then $\lambda(a/b) = \lambda(a)/\lambda(b)$. In either case, λ is determined on $\mathrm{qf}(A)$. Thus we may assume that A is already a field.

Now let $\widetilde{A}$ be the real closure of A. Let c be a positive element of $\widetilde{A} \setminus A$. Since $\widetilde{A}$ is algebraic over A, there is a natural number n and an element $d \in A$ such that c^n/d is finite; that is, bounded by integers. We may assume that $d = \lambda(d)$. Furthermore, in the real closed field M, exactly one of d, $2d, \ldots, 2^{n-1}d$ is in P_n^M, so we may assume that $d \in P_n^M$. Thus $d^{1/n} \in S^M \cap \widetilde{A}$. Since $c/d^{1/n}$ is finite, there is an integer k such that

$$2^k \leq \frac{c}{d^{1/n}} < 2 \cdot 2^k\ .$$

Thus $\lambda(c) = 2^k d^{1/n} \in \widetilde{A}$. Hence $\widetilde{A}$ is closed under λ, which thus extends uniquely to $\widetilde{A}$.

From now on, we assume that A is a real closed field. Let $c \in M \setminus A$, so c is transcendental over A, and write A' for the substructure of $\mathcal{M}$ generated by c over A. If we can find $d \in N$ which satisfies the same type over A as c does, then the embedding of A' into N generated by sending c to d will be elementary. Since $\mathcal{N}$ is a saturated model, it will have an element which realizes this type provided the type is consistent. If the interpretation of the symbols of $\mathcal{L}_{two}$ on A' is determined by that on A, and elementary properties of c, then $\mathrm{tp}(c/A)$ will be consistent also in $\mathcal{N}$.

Case 1 $S \cap A' = S \cap A$. Then for any $e \in A'$ there is $a \in S^A$ with $a \leq e < 2a$, and hence $\lambda(e)$ must take the value a. Also, $P_n^{A'} = P_n^A$, as adding terms in c cannot add any new nth roots.

Case 2 $S \cap A' \neq S \cap A$. We may assume that $\lambda(c) \notin S^A$, and also that $c = \lambda(c)$. Let $i(n) \in \{0, 1, \ldots, n-1\}$ be such that $c/2^{i(n)} \in P_n^{\mathcal{M}}$ (from comments above, $i(n)$ is well-defined for each n). Since A' has transcendence degree one over A, it is not hard to see that $S^{A'}$ must be generated by a single element over S^A, and hence equals $\{ac^\ell : a \in S^A, \ell \in \mathbb{Z}\}$. λ is then determined on A'. Similarly, $P_n^{A'}$ is determined by the sequence of conditions $c/2^{i(n)} \in P_n^{A'}$. □

References

[1] C.C. Chang and J. Keisler, *Model Theory*, Studies in Logic, vol. 73, North Holland, 3rd ed, 1990.

[2] J. Denef and L. van den Dries, *p-adic and real subanalytic sets*, Annals of Mathematics **128** (1988), pp. 79–138.

[3] L. van den Dries, *The field of reals with a predicate for the powers of two*, Manuscripta math **54** (1985), pp 187–195.

[4] L. van den Dries, *Classical model theory of fields*, Model theory, algebra and geometry (eds D. Haskell, A. Pillay, C. Steinhorn), MSRI publications 39, Cambridge University Press (2000), pp 37–52.

[5] W. Hodges, *Model Theory*, Encyclopedia of Mathematics and its Applications vol. 42, Cambridge University Press (1993).

[6] D. Marker, *Introduction to Model Theory*, Model theory, algebra and geometry (eds D. Haskell, A. Pillay, C. Steinhorn), MSRI publications 39, Cambridge University Press (2000), pp 15–36.

[7] D. Marker, *Model theory: an introduction*, Graduate Texts in Mathematics vol. 217, Springer (2000).

Department of Mathematics and Statistics, 1280 Main St W., Hamilton ON L8S 4K1, Canada

E-mail address: haskell@math.mcmaster.ca