Algebraic Geometry Lecture 30 – Semi-algebraic geometry part 2

Lee Butler

4. A crash course in model theory

Now for the model theory. Model theory is essentially a branch of logic that formalises the language used in mathematics, kind of like how category theory formalises the objects in mathematics. But you can actually prove stuff with model theory.

Consider the following innocuous statement:

> for every x greater than zero there is a y such that y is the square root of x.

Normally you wouldn't bat an eyelid at this statement, but there's a lot going on here. Before the statement makes any sense we need to have a notion of "greater than" and know what "zero" is. We also need to know about multiplication, since y being the square root of x really just means $y \cdot y = x$. Finally we need to know what set we're working in. As you've probably already figured out, the statement is true in the real numbers or the real algebraic numbers, but not in the rational numbers (since 2 doesn't have a square root, say), nor in the complex numbers since there's no concept of an order on $\mathbb{C}$ by theorem 4.1.

If we strip away the flesh of many mathematical statements we're left with a very basic language to use:

1. The logical symbols, $=, \exists, \forall, \vee$ (or), $\wedge$ (and), $\neg$ (not), $\Rightarrow$, and $\Leftrightarrow$ and variables $x, y, z, \ldots$ or $v_0, v_1, v_2, \ldots$. We don't need all of these as some can be expressed in terms of the others, but they're useful abbreviations.
2. A specific *language* for a given context. This consists of a set of function symbols of given arity, a set of relation symbols of given arity, and a set of constant symbols. The language of rings, for example, is $\mathcal{L}_r = \{+, \cdot, 0, 1\}$. Here $+$ and $\cdot$ are binary functions, there are no relations, and 0 and 1 are constants. The language of ordered rings is $\mathcal{L}_{or} = \{+, \cdot, <, 0, 1\}$, which includes the binary relation $<$.

As they stand, the two languages mentioned above don't mean anything. We could just as easily write $\mathcal{L}_r = \{f_1, f_2, c_1, c_2\}$ for binary functions f_1, f_2 and constants c_1, c_2. To give a language $\mathcal{L}$ context we need an *$\mathcal{L}$-structure* $\mathcal{M}$. This is a set M and an interpretation for each symbol in $\mathcal{L}$. The interpretation of an n-ary function symbol $f \in \mathcal{L}$ is a function $f^{\mathcal{M}} : M^n \to M$, the interpretation of an n-ary relation symbol $R \in \mathcal{L}$ is a subset $R^{\mathcal{M}} \subset M^n$, and the interpretation of a constant symbol $c \in \mathcal{L}$ is an element $c^{\mathcal{M}} \in M$. We usually don't distinguish between the symbols in $\mathcal{L}$ and their interpretation in $\mathcal{M}$, though.

As an example consider the $\mathcal{L}_r$-structure $\mathcal{M} = (\mathbb{R}, +, \cdot, 0, 1)$. So this is the set of real numbers equipped with addition and multiplication and special constants zero and one.

The other basic idea in model theory is that of an *$\mathcal{L}$-theory.* This is just a well-formed set of formulae using the logical symbols and the language $\mathcal{L}$, and where every variable in each formula is bound either by $\exists$ or by $\forall$. So a typical $\mathcal{L}_{or}$-theory might be

$$T = \{\forall x\, (0 < x \rightarrow (\exists y\, y \cdot y = x))\, ,\, \forall x \exists y\, x < y\, ,\, \exists x\, (0 < x\, \wedge\, \forall y\, \neg(y \cdot y = x))\}.$$

The first formula says that every positive number has a square root. The second says that for every number, there's a bigger number. The final one says that there's a positive number with no square root. This is a valid $\mathcal{L}_r$-theory, but the first and last formulae contradict each other, so whatever context we work in, we can't satisfy all the formulae in T. Suppose we drop the last formula, though, to get a new theory T'. The two formulae are then satisfied if we work in the $\mathcal{L}_r$-structure $\mathcal{M} = (\mathbb{R}, +, \cdot, 0, 1)$, so we say that $\mathcal{M}$ is a *model* for T' and write $\mathcal{M} \models T'$.

Consider two $\mathcal{L}$-structures $\mathcal{M} = (M, \mathcal{L})$ and $\mathcal{N} = (N, \mathcal{L})$, and suppose that $M \subseteq N$ and that the inclusion map i respects the interpretation of the symbols in $\mathcal{L}$, so $i(f^{\mathcal{M}}(a)) = f^{\mathcal{N}}(i(a))$ for every $a \in M$, and so on. Suppose moreover that given any formula ϕ in the language $\mathcal{L}$ we have $\mathcal{M} \models \phi$ if and only if $\mathcal{N} \models \phi$. Then we say $\mathcal{M}$ is an *elementary substructure* of $\mathcal{N}$ and write $\mathcal{M} \prec \mathcal{N}$.

Given an $\mathcal{L}$-theory T we say T is *model-complete* if, for any models $\mathcal{M}$ and $\mathcal{N}$ of T, if $M \subseteq N$ then $\mathcal{M} \prec \mathcal{N}$.

5. Definable sets and quantifier elimination

We said that every formula in a theory had to have all its variables bound by quantifiers, such as in $\forall x \exists y\, x < y$. That's so the formula is either true or false in any given model. If we don't bind all the variables it's not so cut-and-dry. Consider the formula $\phi(x, y)$ given by

$$\exists z(z \neq 0 \wedge y = x + z \cdot z).$$

This formula doesn't bind x or y, so there's no sense asking if it's true in a given structure since it depends on your choice of x and y. Instead this formula defines a set in a given structure:

$$\{(x,y) \in \mathbb{R}^2 \,:\, \exists z(z \neq 0 \wedge y = x + z \cdot z)\} = \{(x,y) \in \mathbb{R}^2 \,:\, x < y\}$$

$$\{(x,y) \in \mathbb{N}_0^2 \,:\, \exists z(z \neq 0 \wedge y = x + z \cdot z)\} = \{(x,y) \in \mathbb{N}_0^2 \,:\, y - x \text{ is a nonzero square}\}.$$

In general we say a set $X \subset M^n$ is *definable* if there is a formula $\psi(\underline{x}, \underline{y})$ in $\mathcal{L}$ such that

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

for some $\underline{b} \in M^m$.

Some examples using the language $\mathcal{L}_r$ of rings include:

- In the structure $(\mathbb{Z}, +, \cdot, 0, 1)$ the set $\{(m,n) \in \mathbb{Z}^2 \,:\, m < n\}$ is definable using Lagrange's four squares theorem.
- If F is a field and we consider the structure $(F[X], +, \cdot, 0, 1)$ then F is definable in this structure – it's the set of units.
- More surprisingly, we can define $\mathbb{C}$ in the structure $(\mathbb{C}(X), +, \cdot, 0, 1)$ using arguments involving elliptic curves.
- $\mathbb{Z}_p$ is definable in $(\mathbb{Q}_p, +, \cdot, 0, 1)$ using Hensel's lemma.
- One of the great results in model theory in the twentieth century was a result by Julia Robinson who showed that the integers are definable in $(\mathbb{Q}, +, \cdot, 0, 1)$. To define them let $\phi(x, y, z)$ be the formula

  $$\exists a \exists b \exists c\, xyz^2 + 2 + yc^2 = a^2 + xy^2$$

  and let $\psi(x)$ be the formula

  $$\forall y \forall z\, ([\phi(y,z,0) \wedge (\forall w\, (\phi(y,z,w) \rightarrow \phi(y,z,w+1)))] \rightarrow \phi(y,z,x)).$$

  Then $\psi(x)$ define $\mathbb{Z}$.

In general the definable sets are the smallest collection of sets $\mathcal{D} = \{D_n\}_{n \geqslant 1}$ such that each D_n boolean algebra of subsets of M^n and the sets are closed under projection, i.e. if $A \in D_{n+1}$ and $\pi : M^{n+1} \to M^n$ is a projection map then $\pi(A) \in D_n$, and such that a few simple sets are included just to get things started. This sounds an awful lot like semi-algebraic sets, except we don't know they're closed under projection. Yet.

The symbols $\exists$ and $\forall$ are called *quantifiers*, and in general they complicate things. But sometimes one can replace a formula involving quantifiers by a quantifier-free formula. For example, consider the set in $\mathbb{R}^3$ defined by the formula $\phi(a, b, c)$

$$\exists x \, ax^2 + bx + c = 0.$$

A little thought shows this gives the same numbers a, b, c as the following formula:

$$(a \neq 0 \wedge b^2 - 4ac \geqslant 0) \vee (a = 0 \wedge (b \neq 0 \vee c = 0)).$$

Here we've taken some liberties with the notation, such as writing $\neg \, a = 0$ as $a \neq 0$, and $b \cdot b - 4ac = 0 \vee b \cdot b - 4ac > 0$ as $b^2 - 4ac \geqslant 0$. Technically we shouldn't even use 4 or $>$, we should write $1 + 1 + 1 + 1$ and flip the inequalities the other way around, but we're here for semi-algebraic geometry not semi-obfuscating pedantry, so we'll let it go.

As an exercise you might want to work out a quantifier-free formula equivalent to the following:

$$\exists x \exists y \exists u \exists v \, (xa + yc = 1 \wedge xb + yd = 0 \wedge ua + vc = 0 \wedge ub + vd = 1).$$

If any formula involving quantifiers can be rewritten without them then we say the set of formulae under consideration has *quantifier elimination.* There's a result in model theory that says if a theory has quantifier elimination then it is model-complete. What does this mean in our case?

Consider the set X in R^n defined by the formula $\phi(x)$ given by

$$\exists y \, (f(x, y) = 0 \wedge g_1(x, y) > 0 \wedge \ldots \wedge g_k(x, y) > 0)$$

where y is in R, say. So then x_0 is in X if and only if there is a point y_0 in R such that

$$(x_0, y_0) \in \{(x, y) \in R^n \times R : f(x, y) = 0, g_1(x, y) > 0, \ldots, g_k(x, y) > 0\} = A.$$

Let $\pi : R^{n+1} \to R^n$ be the projection map on the first n coordinates. The above says that $x_0 \in X$ precisely if $x_0 \in \pi(A)$. This means that we can get rid of the quantifier and define X just using polynomial identities and inequalities if and only if the projection of a semi-algebraic set is still semi-algebraic.

It is not at all obvious that this is true. The corresponding statement for algebraic sets is very false, just consider the circle in $\mathbb{C}^2$, say, and project it down to $\mathbb{C}$ and you get a disc, which isn't an algebraic set. The result does hold for semi-algebraic sets, though, a result known as the Tarski–Seidenberg theorem.

Theorem 5.1 (Tarski–Seidenberg)**.** *Let $E \subset R^{n+1}$ be a semi-algebraic set and π be the projection map on the first n coordinates. Then $\pi(E)$ is a semi-algebraic set in R^n. Equivalently the theory of semi-algebraic sets has quantifier elimination.*

The Tarski–Seidenberg theorem is fairly amazing, and the proof isn't terribly difficult. We're solving Hilbert's seventeenth problem, though, so we'll just need a consequence of this theorem.

Corollary 5.2. *The definable sets in the theory of real closed fields are precisely the semi-algebraic sets.*

Corollary 5.3. *The theory of real closed fields is model-complete.*

6. Hilbert's seventeenth problem

Definition 6.1. Let F be a real closed field and $f(\underline{X}) \in F(X_1, \ldots, X_n)$ be a rational function. We say that f is *positive semidefinite* if $f(\underline{a}) \geqslant 0$ for all $\underline{a} \in F^n$.

Hilbert asked if real positive semidefinite polynomials could always be written as sums of squares of rational functions, similarly to how positive integers can be written as sums of squares. The answer is: yes, yes they can.

Theorem 6.2 (Hilbert's seventeenth problem)**.** *If f is a positive semidefinite rational function over a real closed field F, then f is a sum of squares of rational functions.*

Proof. Let $f(X_1, \ldots, X_n)$ be a positive semidefinite rational function over F that isn't a sum of squares. So by theorem 3.1 there's an ordering of $F(\underline{X})$ such that $f(\underline{X})$ is negative. Let R be the real closure of $F(\underline{X})$ extending this order, which we have by corollary 3.4. Then

$$R \models \exists \underline{v}\, f(\underline{v}) < 0$$

since the variable now ranges over R and $\underline{X} \in R$, and we have $f(\underline{X}) < 0$ in R. But RCF is model-complete so anything true in an extension structure is true in a substructure, so

$$F \models \exists \underline{v}\, f(\underline{v}) < 0,$$

where now the variable ranges over F^n. This contradicts f being positive semidefinite. Thus no such f can exist. □