Algebraic Geometry Lecture 29 – Semi-algebraic geometry

Lee Butler

1. Semi-algebraic sets

Algebraic sets are great, but from a logician's point of view they have a few shortcomings. Specifically, if V is an algebraic set in k^n then $k^n \setminus V$ isn't an algebraic set, and if we project V down to k^{n-1} then in general the result won't be an algebraic set either. But these are the properties one wants when one is dealing with questions of decidability, completeness, and other things you've probably never heard of. And they're also the properties that semi-algebraic sets do have. The natural setting for semi-algebraic geometry is not algebraically closed fields, but real closed fields.

Definition 1.1. We call a field *formally real* if -1 is not a sum of squares in the field. A formally real field R is called *real closed* if no proper algebraic extension of R is formally real.

From now on we'll fix a real closed field R. You can always think of $R = \mathbb{R}$ if you want, or if you keep accidentally writing $\mathbb{R}$ instead of R. We'll define the semi-algebraic sets algebraically and then deal with the logic, since it's a little easier than doing it the other way around.

Definition 1.2. A subset $E \subseteq R^n$ of affine n-space over R is a *semi-algebraic set* if E is a finite union of sets of the form

$$\{x \in R^n \,:\, f(x) = 0, g_1(x) > 0, \ldots, g_k(x) > 0\}$$

with $f, g_1, \ldots, g_k \in R[X_1, \ldots, X_n]$.

Why, you may cry, do we only have one equality and many inequalities, that's inequality against equality, surely. Well if our basic sets were of the form

$$\{x \in R^n \,:\, f_1(x) = 0, \ldots, f_\ell(x) = 0, g_1(x) > 0, \ldots, g_k(x) > 0\}$$

then we could replace each of them by

$$\{x \in R^n \,:\, f_1^2(x) + \ldots + f_\ell^2(x) = 0, g_1(x) > 0, \ldots, g_k(x) > 0\}$$

and get back the same sets, since R is a formally real field. We'll call these sets *basic* since proofs can often boil down to proving things about them.

Definition 1.3. A *boolean algebra of subsets of a set* X is a nonempty collection $\mathcal{C}$ of subsets of X such that if $A, B \in \mathcal{C}$ then $A \cup B \in \mathcal{C}$ and $X \setminus A \in \mathcal{C}$.

Note in particular that if $\mathcal{C}$ is a boolean algebra of subsets of X then $\emptyset, X \in \mathcal{C}$ and for any $A, B \in \mathcal{C}$ we will have $A \cap B \in \mathcal{C}$. (Exercise!)

Lemma 1.4. *The set of semi-algebraic sets of R^n forms a boolean algebra of the subsets of R^n.*

Proof. Obviously if A and B are finite unions of basic sets then $A \cup B$ will be a finite union of basic sets, at worst the sets forming A and the sets forming B. So we just need to deal with the complement. We'll show that the intersection of two basic sets is a basic set, and that the complement of a basic set is semi-algebraic, and the rest of the proof is an exercise in set theory. First let

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

and

$$B = \{x \in R^n \,:\, p(x) = 0, q_1(x) > 0, \ldots, q_\ell(x) > 0\}.$$

Then

$$A \cap B = \{x \in R^n \,:\, f^2(x) + p^2(x) = 0, g_1(x) > 0, \ldots, g_k(x) > 0, q_1(x) > 0, \ldots, q_\ell(x) > 0\}.$$

So the intersection of basic sets is basic. Now we'll show that the complement of a basic set is semi-algebraic. Let A be the basic set as above. Then

$$\begin{aligned} R^n \setminus A &= \{x \in R^n \,:\, f(x) \neq 0 \text{ or } g_1(x) \leqslant 0 \text{ or } \ldots \text{ or } g_k(x) \leqslant 0\} \\ &= \{x \in R^n \,:\, f(x) > 0\} \cup \{x \in R^n \,:\, -f(x) > 0\} \cup \\ &\quad \cup \left(\bigcup_{i=1}^{k} \{x \in R^n \,:\, g_i(x) = 0\} \right) \cup \left(\bigcup_{i=1}^{k} \{x \in R^n \,:\, -g(x) > 0\} \right), \end{aligned}$$

and this is a finite union of basic sets, hence semi-algebraic. □

2. Topology versus logic

One can show that sets of the form $\{x \in R^n \,:\, g(x) > 0\}$ form a base for a topology on R^n, and so finite unions of sets of this form are called *open semi-algebraic sets*. However, unlike algebraic geometry where the Zariski topology is of major interest, here we don't really care about it, instead it's the boolean algebra that's important. That's because semi-algebraic sets have close ties to logic, and through logic they can solve some rather nifty problems.

Here we'll settle for solving a fairly nondescript problem using this approach, we're just going to solve Hilbert's 17th problem![1] In fact we'll solve a more general version of his question, which originally was:

> Given a multivariate polynomial that takes only non-negative values over the reals, can it be represented as a sum of squares of rational functions?

First we need some field theory and then we'll get stuck into the logic.

3. Orderable fields and the real closure

Recall that a (strict) linear order on a set X is a binary relation $<$ such that for every $x, y, z \in X$,

(1) $\neg(x < x)$;
(2) $x < y$ and $y < z$ implies $x < z$;
(3) either $x < y$, $x = y$, or $y < x$.

An ordered field is then a field with a linear order that also satisfies

(1) if $x < y$ then $x + z < y + z$;
(2) if $x < y$ and $z > 0$ then $xz < yz$.

[1] !!

A field F is called *orderable* if there is a linear order $<$ on F that makes $(F, <)$ an ordered field. Fields like $\mathbb{Q}$ and $\mathbb{R}$ are orderable with the usual order, and this is in fact the only order possible on them. On the other hand the field $\mathbb{Q}(X)$ has $2^{\aleph_0}$ possible different orderings on it.[2] Orderable fields are in fact an old friend in disguise.

Theorem 3.1. *A field F is orderable if and only if it is formally real.*

In fact if F is formally real, $a \in F$, and $-a$ isn't a sum of squares then we can find an ordering on F such that $0 < a$.

So whenever we refer to a formally real field we may implicitly assume an order $<$ on it. If F is not only formally real but also real closed then there is a unique order on it. For if $a \in F^\times$ then exactly one of a and $-a$ is a square, so we may order F by

$$x < y \text{ if and only if } y - x \text{ is a nonzero square.}$$

This ordering if often called the canonical ordering on F.

Definition 3.2. If F is a formally real field then a *real closure* of F is a real closed algebraic extension of F.

For example, the real closure of $\mathbb{Q}$ is the field of real algebraic numbers. Zorn's lemma[3] tells us that every formally real field has a real closure, although it may not be unique. However, one can always find a real closure whose canonical ordering extends the ordering on our original field. To prove this we need the following lemma.

Lemma 3.3. *If $(F, <)$ is an ordered field, $0 < x \in F$, and x is not a square in F, then we can extend the ordering of F to $F(\sqrt{x})$.*

Proof. Elements of $F(\sqrt{x})$ are of the form $a + b\sqrt{x}$ for $a, b \in F$. We can extend the ordering on F to $F(\sqrt{x})$ by setting $0 < a + b\sqrt{x}$ if and only if

(1) $b = 0$ and $a > 0$, or
(2) $b > 0$ and ($a > 0$ or $x > (a/b)^2$), or
(3) $b < 0$ and ($a < 0$ and $x < (a/b)^2$).

The first condition ensures negative elements of F remain negative. Exercise: check this defines an order on $F(\sqrt{x})$. □

Corollary 3.4. *If $(F, <)$ is an ordered field then there is a real closure R of F such that the canonical ordering of R extends the ordering on F.*

Proof. Starting with F, we can apply lemma 3.3 repeatedly to arrive at an ordered field $(L, <)$ extending $(F, <)$ such that every positive element of F has a square root in L, i.e.

$$L = F(\sqrt{x} : x \in F).$$

Now, Zorn's lemma tells us that there's a maximal formally real algebraic extension R of L. Now every positive element of F is a square in L and hence in R, and so the canonical ordering on R extends the ordering on F. □

[2] Recall that $2^{\aleph_0}$ is the cardinality of $\mathbb{R}$, or the cardinality of the power set of $\mathbb{N}$. The continuum hypothesis posits that this is in fact $\aleph_1$, the next smallest size of infinity after $\aleph_0$.

[3] Zorn's lemma is equivalent to the axiom of choice and says that if $(X, <)$ is a partial order (i.e. a linear order without the law of trichotomy) such that for every chain $C \subseteq X$ (i.e. every subset linearly ordered by $<$) there is an $x \in X$ such that $c \leqslant x$ for every $c \in C$, then there is $y \in X$ such that there is no $z \in X$ such that $z > y$. In other words, if every chain has an upper bound then X has a maximal element.