Math 591 – Real Algebraic Geometry and Convex Optimization
Lecture 6: Algebraic geometry basics
Cynthia Vinzant, Spring 2019

For today, we will work over a field k, where $k = \mathbb{R}$ or $k = \mathbb{C}$. (The adventurous reader can replace these by any algebraically closed or real closed field, respectively).

Definition. A **variety** or **algebraic set** in k^n has the form

$$V_k(f_1, \ldots, f_r) \;=\; \{p \in k^n \;:\; f_1(p) = 0, \ldots, f_r(p) = 0\},$$

where $f_1, \ldots, f_r \in k[x_1, \ldots, x_n]$. A set $S \subseteq k^n$ is called **constructible** if it is a finite Boolean combination of algebraic sets (obtained via finitely many unions, intersections, and complements).

In $\mathbb{R}^n$ is a **basic closed semialgebraic set** is one of the form

$$\{p \in \mathbb{R}^n \;:\; f_1(p) \geq 0, \ldots, f_r(p) \geq 0\},$$

where $f_1, \ldots, f_r \in \mathbb{R}[x_1, \ldots, x_n]$, and a **semialgebraic set** is a finite Boolean combination of basic closed semialgebraic sets.

For this lecture, we will focus on varieties.

Example. For $f_1 = x^2 + y^2 - 1$ and $f_2 = y - 2$, $V_{\mathbb{C}}(f_1, f_2)$ consists of two points $(\pm i\sqrt{3}, 2)$ and $V_{\mathbb{R}}(f_1, f_2)$ is empty.

Example. For any positive integers d, n and $r \leq \min\{d, n\}$, the set $\mathcal{M}_r$ of $d \times n$ matrices with rank $\leq r$ is a variety defined by the vanishing of all $\binom{d}{r+1} \cdot \binom{n}{r+1}$ of the $(r+1) \times (r+1)$ minors of the matrix. The set of $d \times n$ matrices of rank equal to r is constructible, since it can be written as $\mathcal{M}_r \backslash \mathcal{M}_{r-1}$.

Definition. The **Zariski topology** on k^n is a topology whose closed sets are varieties (called **Zariski-closed**). The **Zariski-closure** of a set $S \subseteq k^n$, denoted $\overline{S}^{\text{Zar}}$ is the inclusion-minimal variety containing S. Complements of Zariski-closed sets are called **Zariski-open**, and we say that a **generic** point in k^n has a property is there exists a non-empty Zariski-open set $U \subseteq k^n$ so that every point in U has that property.

Question. Consider the subset of $\mathbb{R}^{2\times 2}_{\text{sym}}$ defined by

$$S \;=\; \left\{ \begin{pmatrix} v_1^2 & v_1 v_2 \\ v_1 v_2 & v_2^2 \end{pmatrix} \;:\; (v_1, v_2) \in \mathbb{R}^2 \right\} \;=\; \left\{ \text{rank} \leq 1 \text{ PSD matrices in } \mathbb{R}^{2\times 2}_{\text{sym}} \right\}.$$

Is S a basic closed semialgebraic set? a variety? If not, what is $\overline{S}^{\text{Zar}}$?

Answer.

We can write S as a basic closed semialgebraic set using the semialgebraic description of the 2×2 PSD cone, namely:

$$S \;=\; \left\{ \begin{pmatrix} x_{11} & x_{12} \\ x_{12} & x_{22} \end{pmatrix} \in \mathbb{R}^{2\times 2}_{\text{sym}} \;:\; x_{11} \geq 0, x_{22} \geq 0, \text{ and } x_{11}x_{22} - x_{12}^2 \geq 0 \right\}$$

However S is not a variety! To see this, we show that $\overline{S}^{\text{Zar}}$ contains more points than S. Suppose that for some polynomial $F \in \mathbb{R}[x_{11}, x_{12}, x_{22}]$, $F(x_{11}, x_{12}, x_{22}) = 0$ for whenever $X = \begin{pmatrix} x_{11} & x_{12} \\ x_{12} & x_{22} \end{pmatrix}$ belongs to S. Since S is invariant under positive scaling, for any

$X \in S$, $F(\lambda x_{11}, \lambda x_{12}, \lambda x_{22}) = 0$ for all $\lambda \in \mathbb{R}_+$. This implies that as a polynomial in λ, $F(\lambda x_{11}, \lambda x_{12}, \lambda x_{22}) \in \mathbb{R}[\lambda]$ is *identically* zero, and therefore $F(\lambda x_{11}, \lambda x_{12}, \lambda x_{22}) = 0$ for all $\lambda \in \mathbb{R}$.

Therefore any polynomial that vanishes on S also vanished on $-S$. For example, the matrix $\begin{pmatrix} -1 & 0 \\ 0 & 0 \end{pmatrix}$ belongs to $\overline{S}^{\text{Zar}}$, but not S. In fact, in this case, we see that $S \cup -S$ equals $V(\det(X)) = V(x_{11}x_{22} - x_{12}^2)$ is a variety, so this must be the Zariski-closure of S.

$$S \quad \to \quad \overline{S}^{\text{Zar}}$$

The complement of $V(\det(X))$ is a non-empty Zariski-open set consisting of matrices of rank two. Therefore we can say that a generic matrix in $\mathbb{R}^{2\times 2}_{\text{sym}}$ has rank two.

Projections. A fundamental question is what can happen to these sets under (linear) projections.

Question. Define the linear map $\pi : \mathbb{R}^{2\times 2}_{\text{sym}} \to \mathbb{R}^2$ by $\pi \begin{pmatrix} x_{11} & x_{12} \\ x_{12} & x_{22} \end{pmatrix} = (x_{11}, x_{12})$.
What is $\pi(S)$? What is $\pi(\overline{S}^{\text{Zar}})$?

Answer. One can check that $\pi(S) = \{(0,0)\} \cup (\mathbb{R} \times \mathbb{R}_{>0})$ and $\pi(\overline{S}^{\text{Zar}}) = \{(0,0)\} \cup (\mathbb{R} \times \mathbb{R}^*)$.

The following theorems characterize images under linear projections over $\mathbb{C}$ and $\mathbb{R}$.

Theorem (Chevalley). *Over $\mathbb{C}$, the projection of a variety is a constructible set.*

Theorem (Tarski-Seidenberg). *The projection of a semialgebraic set is semialgebraic.*

In fact, we can replace the linear projection in these theorems by an arbitrary polynomial map, as follows. Suppose that $F : k^n \to k^m$ is defined by $F(p) = (f_1(p), \ldots, f_m(p))$, where $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$. Then for any set $S \subset k^n$, we have

$$F(S) \;=\; \pi\left(\{(p,q) \in k^n \times k^m \;:\; p \in S, q_i = f_i(p), \text{ for } i = 1, \ldots, m\}\right),$$

where $\pi(p,q) = q$. Since $q_i = f_i(p)$ are algebraic equations on (p,q) this set (before projection π) is algebraic if S is algebraic and semialgebraic is S is semialgebraic. Therefore $F(S)$ is the image of an algebraic, or semialgebraic, set under linear projection π.

Computation. Let $\pi : k^n \to k^m$ be the linear projection $\pi(x_1, \ldots, x_n) = (x_1, \ldots x_m)$.

Over $\mathbb{C}$, given a variety $V = V_{\mathbb{C}}(f_1, \ldots f_r)$, there are algorithms to compute polynomials $g_1, \ldots, g_s \in \mathbb{C}[x_1, \ldots, x_m]$ defining the image of V, i.e. for which

$$V(g_1, \ldots, g_s) \;=\; \overline{\pi(V_{\mathbb{C}}(f_1, \ldots, f_r))}.$$

See: *elimination algorithms, Gröbner bases.*

Over $\mathbb{R}$, given a semialgebraic set $S \subset \mathbb{R}^n$, one can compute a semialgebraic description of $\pi(S)$. See: *cylindrical algebraic decomposition, quantifier elimination.*

Polynomials defining sets and sets defining polynomials. A variety $V \subseteq k^n$ is uniquely defined by the set of polynomials vanishing on it, i.e.

$$\mathcal{I}(V) \;=\; \{f \in k[x_1, \ldots, x_n] \;:\; f(p) = 0 \text{ for all } p \in V\}.$$

Some useful observations:

- $\mathcal{I}(V)$ is a k-linear subspace of $k[x_1, \ldots, x_n]$
- $\mathcal{I}(V)$ is an *ideal* in the ring $k[x_1, \ldots, x_n]$
  (For any $f_1, f_2 \in \mathcal{I}(V)$ and $h_1, h_2 \in k[x_1, \ldots, x_n]$, $h_1 f_1 + h_2 f_2 \in \mathcal{I}(V)$.)
- If $V = V_k(f_1, \ldots, f_r)$, then $f_1, \ldots, f_r \in \mathcal{I}(V)$.
- V is empty $\Leftrightarrow 1 \in \mathcal{I}(V)$.

Theorem. *(Hilbert's Nullstellensatz) Let $f_1, \ldots, f_r \in \mathbb{C}[x_1, \ldots, x_n]$ and $V = V_{\mathbb{C}}(f_1, \ldots, f_r)$. Then*

(1) $V = \emptyset \Leftrightarrow 1 = h_1 f_1 + \ldots + h_r f_r$ *for some* $h_1, \ldots, h_r \in \mathbb{C}[x_1, \ldots, x_n]$.
(2) $g \in \mathcal{I}(V) \Leftrightarrow g^N = h_1 f_1 + \ldots + h_r f_r$ *for some* $N \in \mathbb{Z}_+$, $h_1, \ldots, h_r \in \mathbb{C}[x_1, \ldots, x_n]$.

There are algorithms (based on *Gröbner bases*) to compute the polynomials $h_1, \ldots, h_r$. We could also search for multipliers $h_1, \ldots, h_r \in \mathbb{R}[x_1, \ldots, x_n]$ of bounded degree via linear algebra. Matching up coefficients in $1 = h_1 f_1 + \ldots + h_r f_r$ imposes affine linear conditions on the $(h_1, \ldots, h_r) \in (\mathbb{R}[x_1, \ldots, x_n]_{\leq D})^r$.

Example. For $f_1 = x^2 - x$ and $f_2 = x - 2 \in \mathbb{C}[x]$, we have $V_{\mathbb{C}}(f_1, f_2) = \emptyset$. Using the Euclidean algorithm, we can compute that

$$1 \;=\; (1/2) \cdot f_1 - 1/2(x+1) f_2,$$

which certifies that $V_{\mathbb{C}}(f_1, f_2)$ is empty. (Plugging in a common root of f_1, f_2 would result in $1 = 0$.)

What is the correct analogue for semialgebraic sets?

A basic closed semialgebraic set $S \subset \mathbb{R}^n$ is uniquely determined by the the set of polynomials that are nonnegative on it:

$$\mathcal{P}(S) \;=\; \{f \in \mathbb{R}[x_1, \ldots, x_n] \;:\; f(p) \geq 0 \text{ for all } p \in S\}.$$

Some useful observations:

- $\mathcal{P}(S)$ is a convex cone in $\mathbb{R}[x_1, \ldots, x_n]$.
- If $S = \{p \in \mathbb{R}^n : g_1(p) \geq 0, \ldots, g_r(p) \geq 0\}$, then $g_1, \ldots, g_r \in \mathcal{P}(S)$.
- $S = \emptyset \Leftrightarrow -1 \in \mathcal{P}(S)$.
- ???

Next time we expand this list and talk about an analogue of Hilbert's Nullstellensatz.