Math 582G - Convex Algebraic Geometry

Today: Real algebraic geometry basics

Take $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$

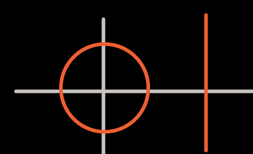
Def: A <u>variety</u> or <u>algebraic set</u> in $\mathbb{F}^n$ (or $\mathbb{A}^n(\mathbb{F})$) has the form

$$V_{\mathbb{F}}(f_1, \dots, f_r) = \{ p \in \mathbb{F}^n : f_1(p) = 0, \dots, f_r(p) = 0 \}$$

where $f_1, \dots, f_r \in \mathbb{F}[x_1, \dots, x_n]$.

A finite Boolean combination of algebraic sets is called <u>constructible</u>. construct using finitely many intersections, unions, complements

Ex: $f_1 = 1 - x^2 - y^2$, $f_2 = x - 2$



$V_{\mathbb{C}}(f_1, f_2) = \{(2, \pm i\sqrt{3})\}$ $V_{\mathbb{R}}(f_1, f_2) = \phi$

Ex: $\mathcal{M}^{d,r}_{sym} = \{ A \in \mathbb{F}^{d \times d}_{sym} : \operatorname{rank}(A) \leq r \}$ $\qquad \mathbb{F}^{d\times d}_{sym} \cong \mathbb{F}^{\binom{d+1}{2}}$

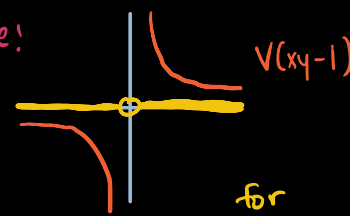
$$= V_{\mathbb{F}}(\text{all } (r+1) \times (r+1) \text{ minors of } A)$$ algebraic

$\{A = \mathbb{F}^{d \times d}_{sym} : \operatorname{rank}(A) = r\} = \mathcal{M}^{d,r}_{sym} \setminus \mathcal{M}^{d,r-1}_{sym}$ constructible

<u>Chevalley's Theorem</u>: Over $\mathbb{C}$, the image of an algebraic set under linear projection is constructible.

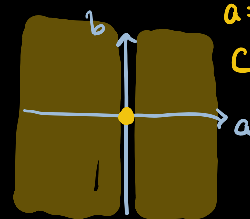
Ex: $\pi : \mathbb{C}^2 \to \mathbb{C}$, $\pi(x,y) = x$ constructible!

$\pi(V_{\mathbb{C}}(xy-1)) = \mathbb{C}\setminus\{0\} = V_{\mathbb{C}}(0)\setminus V_{\mathbb{C}}(x)$



Ex: $\pi : \mathbb{C}^{2\times 2}_{sym} \to \mathbb{C}^2$ $\pi\begin{pmatrix} a & b \\ b & c \end{pmatrix} = (a,b)$

$\pi(\mathcal{M}^{2,1}_{sym}) = \mathbb{C}^2 \setminus V_{\mathbb{C}}(a) \cup V_{\mathbb{C}}(a,b)$



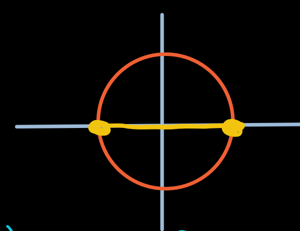
for $a \neq 0$, $c = \frac{b^2}{a}$

$a=0$, $\Rightarrow b=0$

Note: this doesn't hold over $\mathbb{R}$!

Ex: $\pi(x,y) = x$

$\pi(V_{\mathbb{R}}(1-x^2-y^2)) = [-1,1]$ ← not constructible! ← is semialg.



($S \subseteq \mathbb{R}$ constructible $\Leftrightarrow$ S or $\mathbb{R}\setminus S$ finite)

Def: A <u>basic closed semialgebraic set</u> in $\mathbb{R}^n$ has the form

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

where $f_1, \ldots, f_r \in \mathbb{R}[x_1, \ldots, x_n]$.

A finite Boolean combination of basic closed semialg. sets is called a <u>semialgebraic set</u>.

Ex: $\{A \in \mathbb{R}^{d\times d}_{sym} : A \succeq 0, \operatorname{rank}(A) \leq r\}$ basic closed semialg. set.

defined by • principal minors $\det\begin{pmatrix} a_{i_1i_1} & \cdots & a_{i_1i_k} \\ \vdots & \ddots & \vdots \\ a_{i_ki_1} & \cdots & a_{i_ki_k} \end{pmatrix} \geq 0$

• all $(r+1)\times(r+1)$ minors $\det\begin{pmatrix} a_{i_1j_1} & \cdots & a_{i_1j_{r+1}} \\ \vdots & \ddots & \vdots \\ a_{i_{r+1}j_1} & \cdots & a_{i_{r+1}j_{r+1}} \end{pmatrix} = 0$

(Note "$f=0$" equiv to "$f\geq 0$ and $-f\geq 0$")

Tarski-Seidenberg Theorem:

The image of a semialgebraic set under linear projection is semialgebraic.

Computational Question:

Given polynomials $f_1,\dots,f_r$ and a projection π, how can we compute algebraic description of $\pi(S)$ where S is described by $f_1,\dots,f_r$?

Over $\mathbb{C}$ ⇝ Gröbner bases

Over $\mathbb{R}$ ⇝ cylindrical algebraic decomposition

Certification

Given $f_1,\dots,f_r \in \mathbb{C}[x_1,\dots,x_n]$, what polynomials "obviously" vanish on $V_{\mathbb{C}}(f_1,\dots,f_r)$?

Def: The ideal generated by $f_1,\dots,f_r$ in $\mathbb{F}[x_1,\dots,x_n]$ is

$$\langle f_1,\dots,f_r\rangle = \left\{ \sum_{i=1}^{r} h_i f_i \;:\; h_i \in \mathbb{F}[x_1,\dots,x_n]\right\}.$$ ← ideal of $\mathbb{F}[x_1,\dots,x_n]$

If $g = \sum_{i=1}^{r} h_i f_i$ then for any $p \in V_{\mathbb{F}}(f_1, \dots, f_r)$ ↜ $\mathbb{F}$-linear subspace

$$g(p) = \sum_{i=1}^{r} h_i(p) f_i(p) = \sum_{i=1}^{r} h_i(p) \cdot 0 = 0.$$

Ex: $f_1 = 1 - x^2 - y^2$, $f_2 = x - 2$ $\quad V_{\mathbb{C}}(f_1, f_2) = \{(2, \pm i\sqrt{3})\}$

$$\underline{-f_1 - (x+2) f_2} = x^2 + y^2 - 1 - (x^2 - 4) = \underline{y^2 + 3}$$

← certificate that y^2+3 vanishes on $V_{\mathbb{C}}(f_1, f_2)$

Hilbert's Nullstellensatz:

$V_{\mathbb{C}}(f_1, \dots, f_r)$ is empty $\iff 1 \in \langle f_1, \dots, f_r \rangle$

"$1 = \sum_{i=1}^{r} h_i f_i$" is a certificate that $V_{\mathbb{C}}(f_1, \dots, f_r) = \emptyset$

Over $\mathbb{R}$? Useful to consider polynomials that are "obviously" nonnegative on $V_{\mathbb{R}}(f_1, \dots, f_r)$.

Let SOS_n denote the set of sums of squares in $\mathbb{R}[x_1, \dots, x_n]$, i.e.

← convex

$$SOS_n = \left\{ \sum_{i=1}^{s} g_i^2 \ : \ s \in \mathbb{N},\ g_i \in \mathbb{R}[x_1, \dots, x_n] \right\}.$$

Any polynomial in $SOS_n + \langle f_1, \dots, f_r \rangle$ is nonnegative on $V_{\mathbb{R}}(f_1, \dots, f_r)$.

$$q = \sum_{i=1}^{s} g_i^2 + \sum_{j=1}^{r} h_j f_j \Rightarrow q(p) = \sum_{i=1}^{s} \underbrace{g_i(p)^2}_{\geq 0} + \sum_{j=1}^{r} h_j(p) \underbrace{f_j(p)}_{=0}$$

$p \in V_{\mathbb{R}}(f_1, \dots, f_r)$ $\qquad \Rightarrow q(p) \geq 0$

Krivine's Positivstellensatz:

$$V_{\mathbb{R}}(f_1,\dots,f_r)=\emptyset \iff -1 \in SOS_n + \langle f_1,\dots,f_r\rangle$$

Ex: $f_1 = 1-x^2-y^2 \qquad f_2 = x-2$

$$y^2+3 = -f_1 - (x+2)f_2$$

$$\Rightarrow -1 = \left(\frac{y}{\sqrt{3}}\right)^2 + \left[f_1 + (x+2)f_2\right]\frac{1}{3}$$

certificate that $V_{\mathbb{R}}(f_1,f_2)=\emptyset$