EE464: Algebraic Geometric Dictionary

algebraic geometry

One way to view linear algebra is as the study of equations of the form

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= y_1 \\ a_{21}x_2 + a_{22}x_2 + \cdots + a_{2n}x_n &= y_2 \\ &\vdots \\ a_{m1}x_2 + a_{m2}x_2 + \cdots + a_{mn}x_n &= y_m \end{aligned}$$

one may view algebraic geometry as the study of equations of the form

$$\begin{aligned} f_1(x_1, \ldots, x_n) &= 0 \\ f_2(x_1, \ldots, x_n) &= 0 \\ &\vdots \\ f_m(x_1, \ldots, x_n) &= 0 \end{aligned}$$

where the functions f_i are *polynomials*

feasibility problems

consider the feasibility problem

$$\boxed{\begin{array}{l}\text{does there exist } x \in \mathbb{R}^n \text{ such that} \\ f_i(x) = 0 \qquad \text{for all } i = 1, \ldots, m\end{array}}$$

sample problems

- is there a solution $x \in \mathbb{R}^n$, or $x \in \mathbb{C}^n$
- find all solutions x; i.e., *parametrize* them
- among all solutions, find the one which minimizes a given cost function

algebraic geometry and linear algebra

many ideas from linear algebra can be generalized

abstractions

duality, subspaces S, $S^{\perp}$	ideals, varieties, quotient spaces

solving equations

Gaussian elimination	Groebner basis algorithms

solving inequalities

LP duality	real algebraic geometry, p-satz

multivariable polynomials

a *monomial* in $x_1, \ldots, x_n$ is a product, written

$$x^\beta = x_1^{\beta_1} x_2^{\beta_2} \ldots x_n^{\beta_n}$$

where $\beta = (\beta_1, \ldots, \beta_n)$ the *degree* of the monomial is $\beta_1 + \cdots + \beta_n$, denoted $|\beta|$

we'll also index the coefficients of polynomials by β, as in

$$f = \sum_{\beta \in C} a_\beta x^\beta$$

for example

$$f = 7x_1^4 x_3 + 2x_1^2 x_3^2 + 3x_2 x_3$$

has $C = \Big\{ (4,0,1), (2,0,2), (0,1,1) \Big\}$, and $a_{4,0,1} = 7$

multivariable polynomials

- the set of polynomials in n variables with *real coefficients* is denoted $\mathbb{R}[x_1, \ldots, x_n]$, also called the set of $n-$ary polynomials

- the *degree* of a polynomial is the maximum degree of its terms, with the convention that $\deg(0) = -\infty$, so
$$\deg(fg) = \deg(f) + \deg(g)$$

- we'll need to work over both $\mathbb{R}$ and $\mathbb{C}$; we'll use $\mathbb{K}$ to denote either

abstract spaces: groups

In a *group*, the operation ($+$ or $\times$) is *associative*, *invertible*, and has an *identity* (0 or 1) ;

examples

- The rationals $\mathbb{Q}$ under addition
- The non-zero rationals $\mathbb{Q}\backslash\{0\}$ under multiplication
- Every vector space under addition
- The invertible matrices under matrix multiplication

abstract spaces: rings and fields

In a (commutative) *ring* R we have *two* operations

- addition: *associativity*, *commutativity*, *identity*, *invertibility*
- multiplication: *associativity*, *commutativity*, *identity*
- and *distributivity* $f(g+h) = fg + fh$

If the nonzero elements of R form a group under multiplication then R is called a *field*

- The set of polynomials in n variables $\mathbb{R}[x_1, \ldots, x_n]$
- $\mathbb{Z}$ is a ring; $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields
- The set of functions $f : S \to \mathbb{R}$ is a ring

abstract spaces

- Every ring is a commutative group under addition
- The additive identity is 0, the multiplicative identity is 1

The ring of polynomials $\mathbb{R}[x_1, \dots, x_n]$ contains $\mathbb{R}$, so it is also a vector space (of infinite dimension)

e.g. we can view $\mathbb{R}[x]$ as the set of all sequences $(f_0, f_1, f_2, \dots)$ where only finitely many of the f_i are nonzero

then multiplication is convolution

$$fg = (c_0, c_1, \dots) \quad \text{with} \quad c_k = \sum_{i=0}^{k} f_i g_{k-i}$$

multivariable polynomials

- notice that $\mathbb{R}[x_1, x_2] = (\mathbb{R}[x_1])[x_2]$, e.g.

$$x_1^2 x_2^2 + 4x_1^3 x_2 + 2x_1 x_2^2 + 3 = (x_1^2 + 2x_1)x_2^2 + (4x_1^3)x_2 + 3$$

- we'll also use $\mathbb{R}_d[x_1, \ldots, x_n]$ to denote the set of polynomials in n variables with degree $\leq d$, i.e., the $n-$ary $d-$ics

- $\mathbb{R}_d[x_1, \ldots, x_n]$ has dimension $\displaystyle\binom{n+d}{n} = \frac{(n+d)!}{n!d!}$

- $\mathbb{R}(x_1, \ldots, x_n)$ is the *quotient field* of rational functions

algebraically closed fields

A field $\mathbb{K}$ is called *algebraically closed* if every polynomial in $\mathbb{K}[x]$ with degree ≥ 1 has a root.

The Fundamental Theorem of Algebra says that $\mathbb{C}$ is algebraically closed.

$\mathbb{R}$ is not (e.g. $x^2 + 1$)

a nonzero polynomial in $\mathbb{K}[x]$ of degree m has at most m roots

varieties

consider the feasibility problem

$$\boxed{\begin{array}{l}\text{does there exist } x \in \mathbb{K}^n \text{ such that} \\ f_i(x) = 0 \qquad \text{for all } i = 1, \ldots, m\end{array}}$$

The *variety* defined by polynomials $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_m]$ is the corresponding feasible set; i.e.,

$$\boxed{\mathcal{V}\{f_1, \ldots, f_m\} = \left\{\, x \in \mathbb{K}^n \mid f_i(x) = 0 \text{ for all } i = 1, \ldots, m \,\right\}}$$

A variety is also called an *algebraic set*, or an *affine variety*.

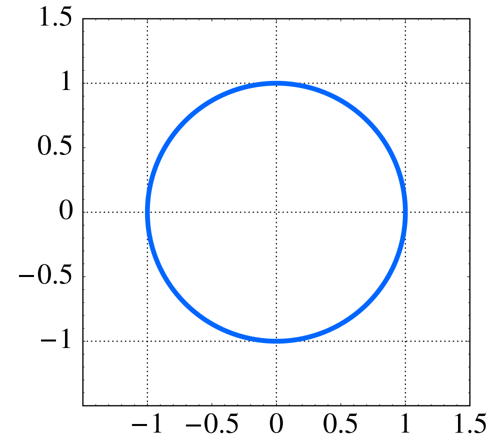
Sometimes we'll use $\mathcal{V}_{\mathbb{R}}\{f\}$ to denote the real solutions

examples of varieties

in general, a *variety* is any subset of $\mathbb{K}^n$ which can be expressed as the common roots of a set of polynomials

- If $f(x) = x_1^2 + x_2^2 - 1$ then

  $\mathcal{V}(f)$ is the unit circle in $\mathbb{R}^2$.



- The affine set

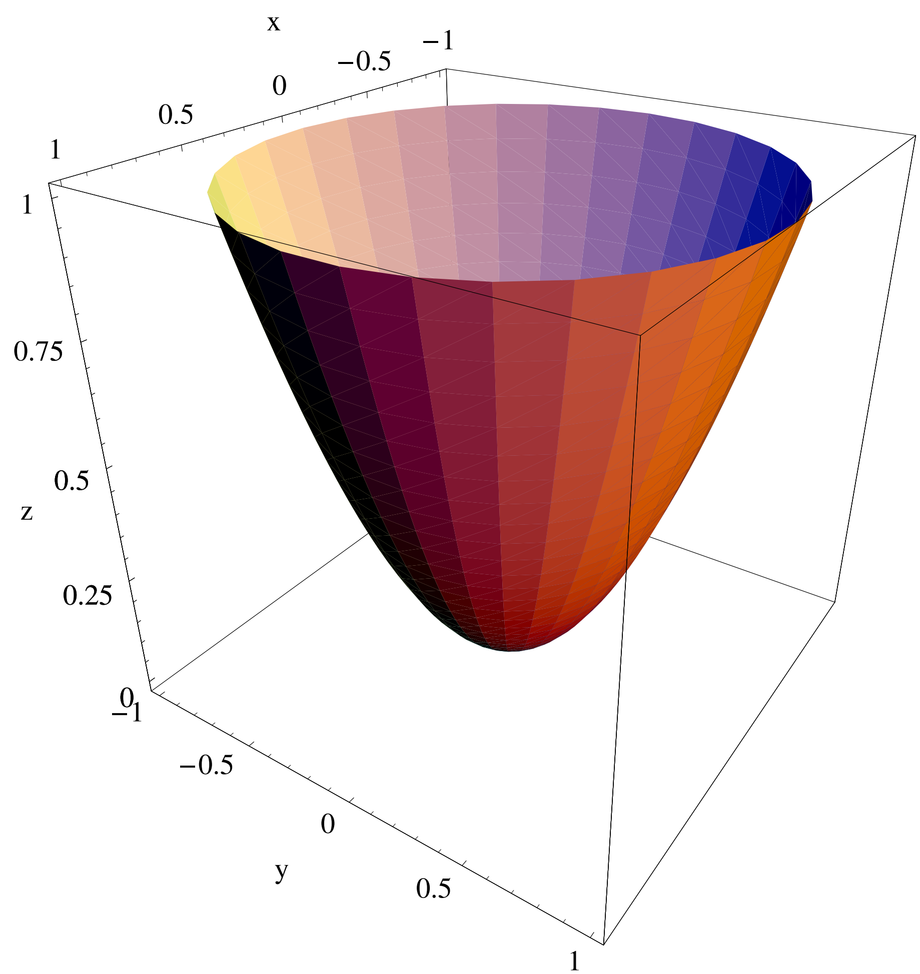
$$\{ x \in \mathbb{R}^n \mid Ax = b \}$$

  is the variety of the polynomials $a_i^T x - b_i$

varieties

example

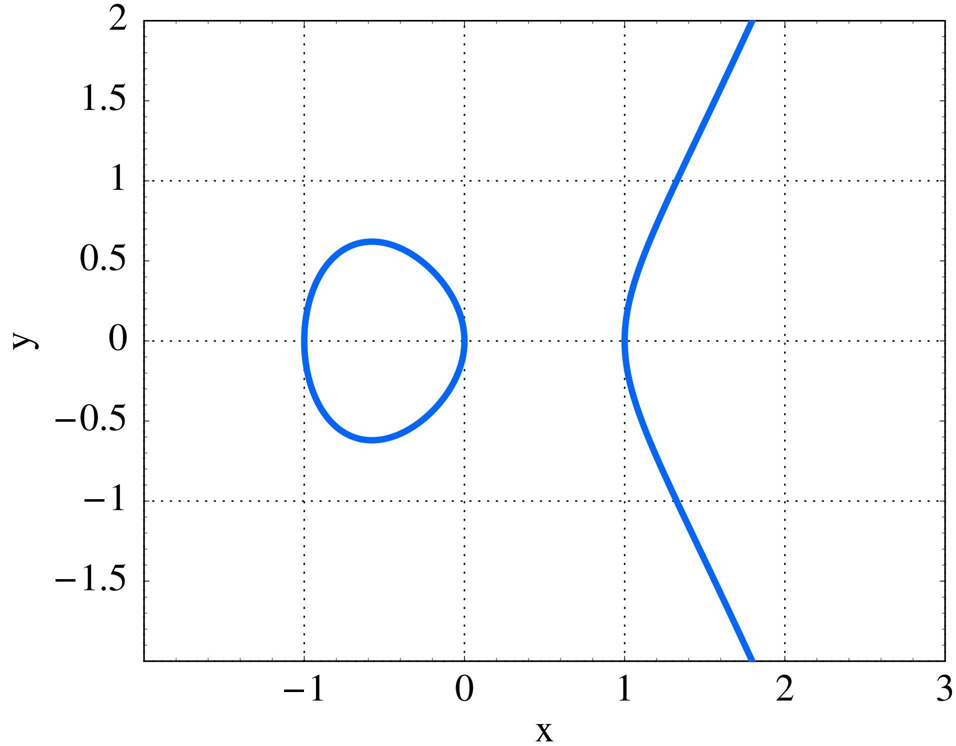
$$\mathcal{V}(z - x^2 - y^2)$$



varieties may not be connected

for example

$$\mathcal{V}(x + y^2 - x^3)$$



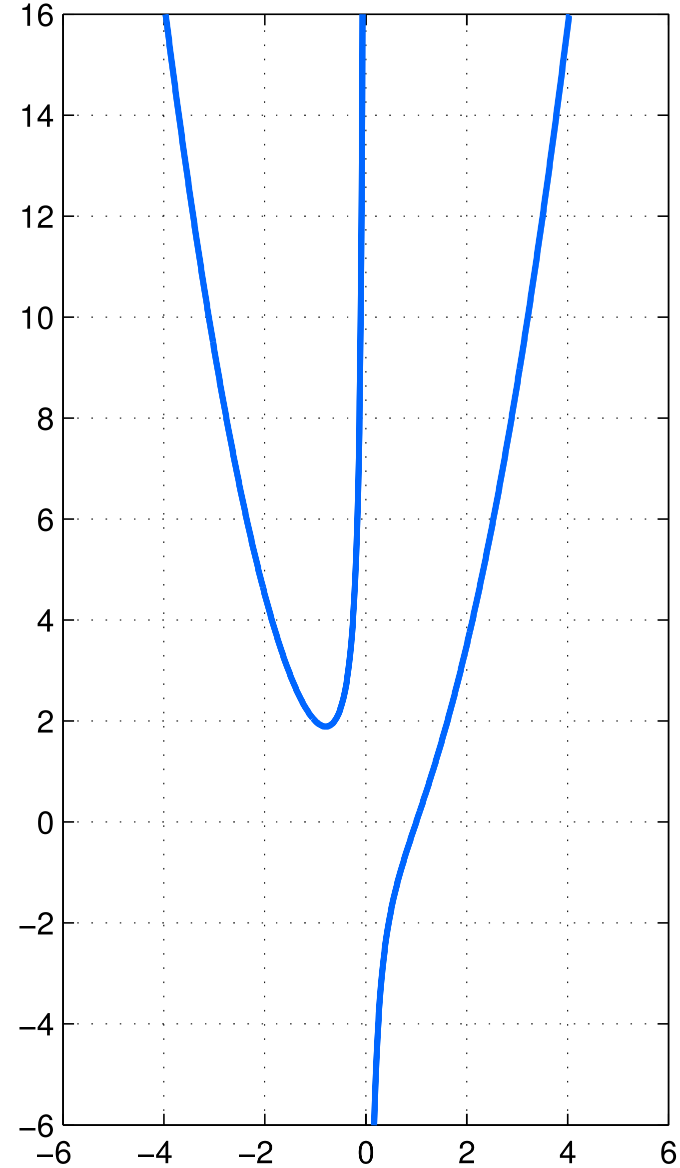
examples of varieties

the graph of the rational function

$$y = \frac{x^3 - 1}{x}$$

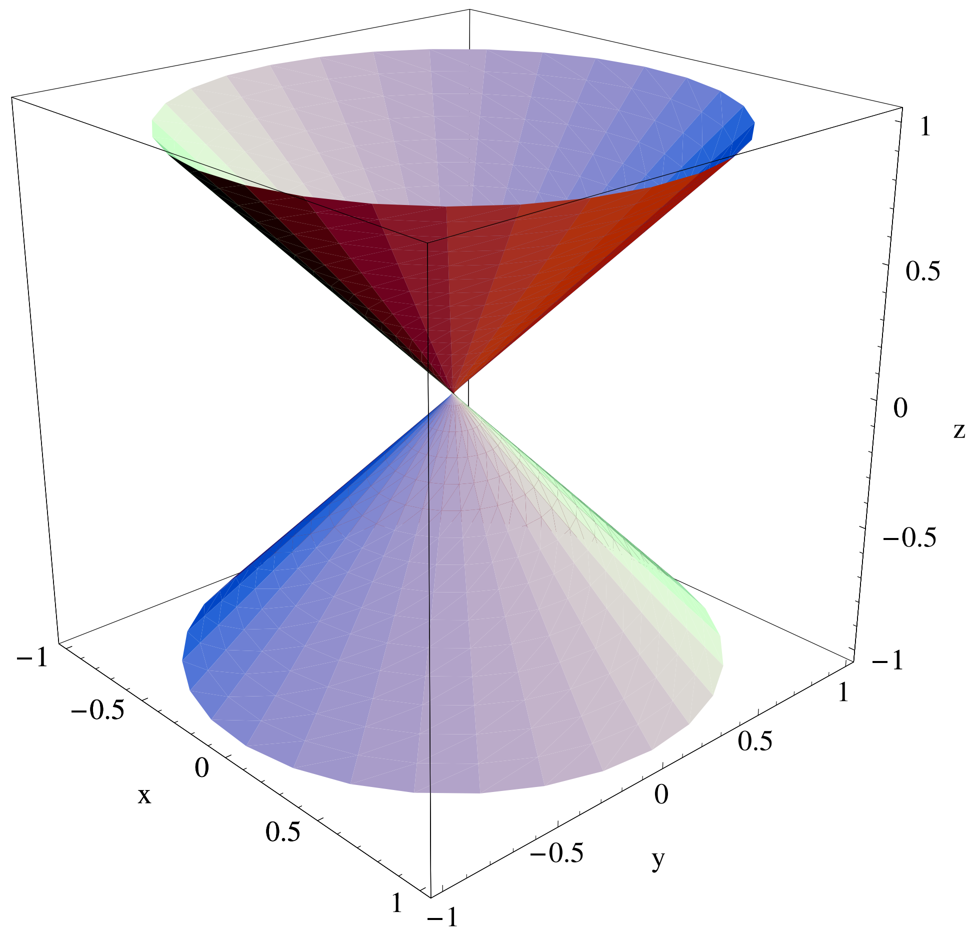
is the variety

$$\mathcal{V}(xy - x^3 + 1)$$



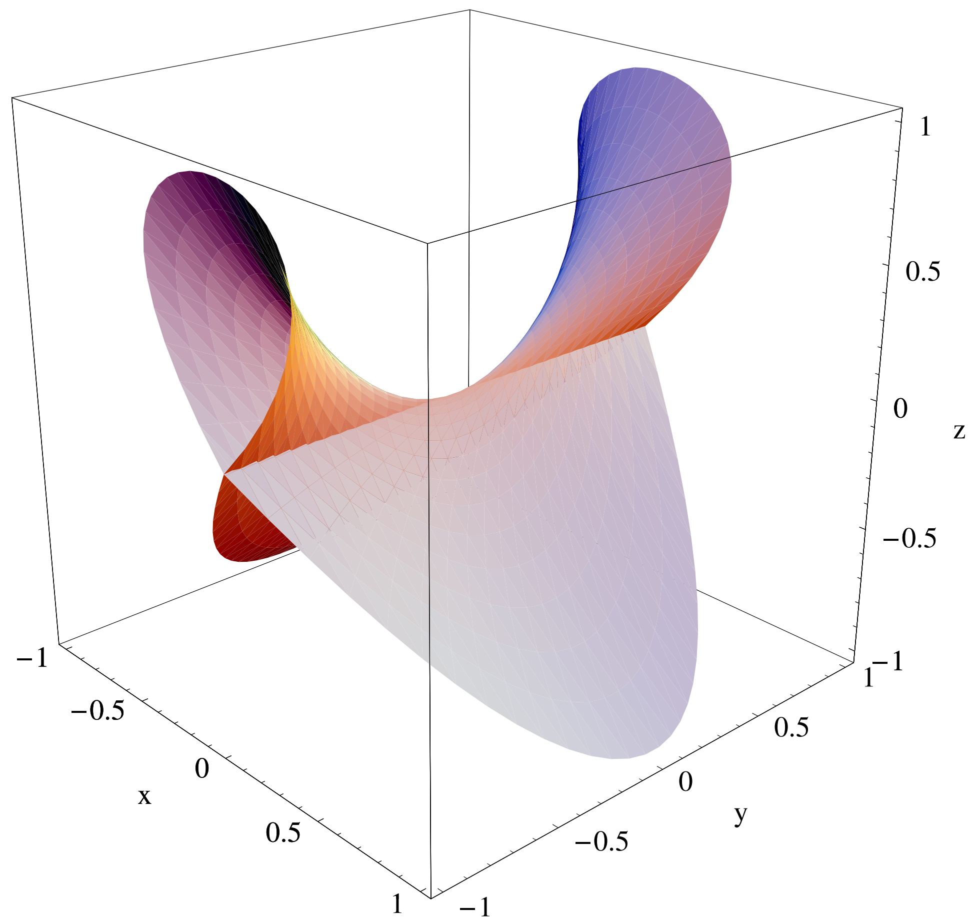
examples of varieties

example: $\mathcal{V}(z^2 - x^2 - y^2)$



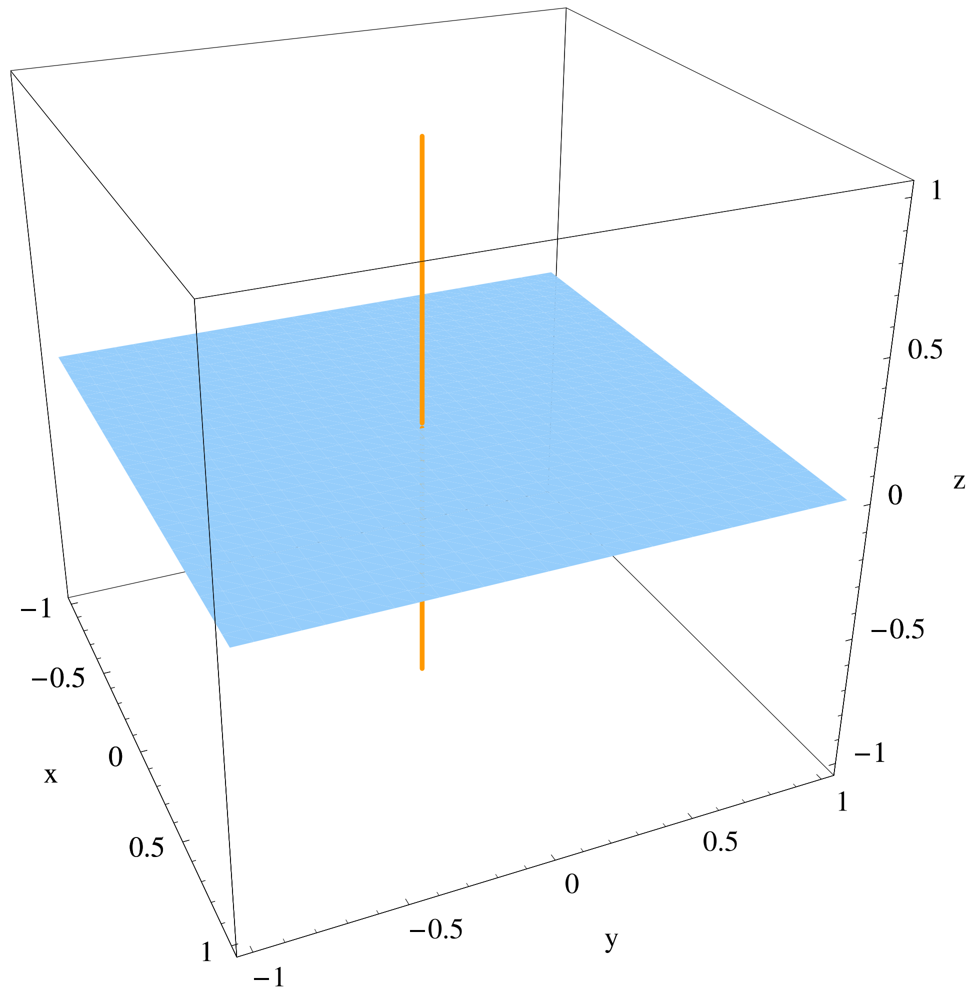
examples of varieties

example: $\mathcal{V}(x^2 - y^2z^2 + z^3)$



examples of varieties

the variety $\mathcal{V}(xz, yz)$ has two pieces of different dimension



examples of varieties

the set of matrices of rank $\leq k$ is a variety

$$\left\{ A \in \mathbb{C}^{n \times n} \mid \mathbf{rank}\, A \leq k \right\}$$

because $\mathbf{rank}(A) \leq k$ if and only if the determinant of all $(k+1) \times (k+1)$ submatrices vanishes

intersections and unions of varieties

- If V, W are varieties, then so is $V \cap W$

  because if $V = \mathcal{V}\{f_1, \ldots, f_m\}$ and $W = \mathcal{V}\{g_1, \ldots, g_n\}$ then

$$V \cap W = \mathcal{V}\{f_1, \ldots, f_m, g_1, \ldots, g_n\}$$

- so is $V \cup W$, because

$$V \cup W = \mathcal{V}\left\{ f_i g_j \mid i = 1, \ldots, m, j = 1, \ldots, n \right\}$$

proof: clearly $V \cup W \subset \mathcal{V}(f_i g_j)$

to show $V \cup W \supset \mathcal{V}(f_i g_j)$, suppose $x \in \mathcal{V}(f_i g_j)$, and $x \notin V$ then, for some k, $f_k(x) \neq 0$, so $f_k(x) g_j(x) = 0$ for all j

hence either $x \in V$ or $x \in W$, as desired

properties of varieties

Every variety in $\mathbb{C}^n$ is closed.

because polynomials are continuous, the inverse image of a closed set is closed

not properties

- If V is a variety, the *projection* of V onto a subspace may not be a variety. e.g., the projection onto $y = 0$ of $\mathcal{V}(x - y^2)$

- The set-theoretic difference of two varieties may not be a variety.

equality constraints

consider the feasibility problem

$$\boxed{\begin{array}{l} \text{does there exist } x \in \mathbb{R}^n \text{ such that} \\ f_i(x) = 0 \qquad \text{for all } i = 1, \dots, m \end{array}}$$

the function $f : \mathbb{R}^n \to \mathbb{R}$ is called a *valid equality constraint* if

$$f(x) = 0 \qquad \text{for all feasible } x$$

given a set of equality constraints, we can generate others as follows

(i) if f_1 and f_2 are valid equalities, then so is $f_1 + f_2$

(ii) for any $h \in \mathbb{R}[x_1, \dots, x_n]$, if f is a valid equality, then so is hf

using these will make the dual bound *tighter*

ideals and valid equality constraints

a set of polynomials $I \subset \mathbb{R}[x_1, \ldots, x_n]$ is called an *ideal* if

(i) $f_1 + f_2 \in I$ for all $f_1, f_2 \in I$

(ii) $fh \in I$ for all $f \in I$ and $h \in \mathbb{R}[x_1, \ldots, x_n]$

- given $f_1, \ldots, f_m$, we can generate an *ideal of valid equalities* by repeatedly applying these rules
- this gives the *ideal generated by* $f_1, \ldots, f_m$,

$$\boxed{\mathbf{ideal}\{f_1, \ldots, f_m\} = \left\{ \sum_{i=1}^{m} h_i f_i \mid h_i \in \mathbb{R}[x_1, \ldots, x_n] \right\}}$$

written $\mathbf{ideal}\{f_1, \ldots, f_m\}$, or sometimes $\langle f_1, \ldots, f_m \rangle$.

generators of an ideal

- every polynomial in $\mathbf{ideal}\{f_1, \ldots, f_m\}$ is a valid equality.
- $\mathbf{ideal}\{f_1, \ldots, f_m\}$ is the smallest ideal containing $f_1, \ldots, f_m$.
- the polynomials $f_1, \ldots, f_m$ are called the *generators*, or a *basis*, of the ideal.

properties of ideals

- if I_1 and I_2 are ideals, then so is $I_1 \cap I_2$
- an ideal generated by one polynomial is called a *principal ideal*

example

$$f_1 = x_1 - x_3 - 1 \qquad f_2 = x_2 - x_3^2 - 1$$

look at the polynomial

$$q = x_1^2 - 2x_1 - x_2 + 2$$

$q \in \mathbf{ideal}\{f_1, f_2\}$ because

$$\begin{aligned} q &= h_1 f_1 + h_2 f_2 \\ &= (x_1 + x_3 - 1) f_1 + (-1) f_2 \end{aligned}$$

so every point x in the feasible set satisfies $q(x) = 0$

this is an example of using ideals for *elimination of variables*

ideals

ideals will be a fundamental algebraic object in this course

- we can use polynomials in the ideal to strengthen the dual bound obtained via Lagrange duality

we'll see that the ideal is the appropriate *dual* object to the feasible set

the ideal-variety correspondence

we'll see that ideals and varieties are in correspondence;

another way to say this is; the ideal captures all the information about the feasible set in the polynomials

$$\boxed{\mathcal{V}(\mathbf{ideal}\{f_1, \ldots, f_m\}) = \mathcal{V}\{f_1, \ldots, f_m\}}$$

example

apart from duality, ideals give us a very important tool for *simplification* of varieties; e.g., it's easy to see

$$\mathbf{ideal}\{2x^2+3y^2-11, x^2-y^2-3\} = \mathbf{ideal}\{x^2-4, y^2-1\}$$

because if I is an ideal, then if $f_1, f_2 \in I$ then $\mathbf{ideal}\{f_1, f_2\} \subset I$

so the variety is the four points

$$\mathcal{V}\{2x^2+3y^2-11, x^2-y^2-3\} = \{(\pm 2, \pm 1)\}$$

in fact, one can do this *automatically*

the ideal-variety correspondence

given a set $S \subset \mathbb{R}^n$, the set of polynomials which vanish on S is an ideal

$$\boxed{\mathcal{I}(S) = \left\{ f \in \mathbb{R}[x_1, \ldots, x_n] \mid f(x) = 0 \text{ for all } x \in S \right\}}$$

Also given an ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ we can construct the variety

$$\mathcal{V}(I) = \left\{ x \in \mathbb{K}^n \mid f(x) = 0 \text{ for all } f \in I \right\}$$

Key question: are these maps one-to-one?

the ideal-variety correspondence

If S is a variety, then

$$\boxed{\mathcal{V}\big(\mathcal{I}(S)\big) = S}$$

This implies $\mathcal{I}$ is one-to-one (since $\mathcal{V}$ is a left-inverse); i.e., no two distinct varieties give the same ideal.

to see this,

- first we'll show $S \subset \mathcal{V}\big(\mathcal{I}(S)\big)$

  suppose $x \in S$; then $f(x) = 0$ for all $f \in \mathcal{I}(S)$, so $x \in \mathcal{V}\big(\mathcal{I}(S)\big)$

- now we'll show $\mathcal{V}\big(\mathcal{I}(S)\big) \subset S$

  suppose $S = \mathcal{V}\{f_1, \ldots, f_m\}$, and $x \in \mathcal{V}\big(\mathcal{I}(S)\big)$. Then $f(x) = 0$ for all $f \in \mathcal{I}(S)$. Also we have $f_i \in \mathcal{I}(S)$, so $f_i(x) = 0$, and so $x \in S$

the ideal-variety correspondence

We'd like to consider the converse; do every two distinct ideals map to distinct varieties? i.e. is $\mathcal{V}$ one-to-one on the set of ideals?

The answer is no; for example

$$I_1 = \textbf{ideal}\{(x-1)(x-3)\} \qquad I_2 = \textbf{ideal}\{(x-1)^2(x-3)\}$$

Both give variety $\mathcal{V}(I_i) = \{1, 3\} \subset \mathbb{C}$.

But $(x-1)(x-3) \notin I_2$, so $I_1 \neq I_2$

the ideal-variety correspondence

It turns out that that, except for multiplicities, ideals are uniquely defined by varieties.To make this precise, define the *radical* of an ideal

$$\sqrt{I} = \left\{ f \mid f^r \in I \text{ for some integer } r \geq 1 \right\}$$

An ideal is called radical if $I = \sqrt{I}$.

One can show, using the Nullstellensatz (later), that for any ideal $I \subset \mathbb{C}[x_1, \ldots, x_n]$

$$\sqrt{I} = \mathcal{I}\big(\mathcal{V}(I)\big)$$

This implies

$$\boxed{\text{There is a one-to-one correspondence between radical ideals and varieties}}$$