Reading course report, on the book Ideals, Varieties, and Algorithms by D. Cox, J. Little, D. O'Shea.

Vincent Neiger

Western University

December 8, 2014

Outline

Affine varieties

k is an infinite field.

An affine variety is the set of solutions of a system of polynomial equations: polynomials $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ define the variety

$$\mathbf{V}(f_1, \ldots, f_m) = \{(a_1, \ldots, a_n) \in k^n \mid f_i(a_1, \ldots, a_n) = 0 \text{ for } 1 \leqslant i \leqslant m\}$$

Examples:

- in $\mathbb{R}$, $\mathbf{V}(x^2 + 1) = \emptyset$
- in $\mathbb{R}^2$, $\mathbf{V}(x^2 - y^2) = \{(a, \pm a),\ a \in \mathbb{R}\} = (1, -1)\mathbb{R} \cup (1, 1)\mathbb{R}$
- in $\mathbb{R}^2$, $\mathbf{V}(x^2 + y^2) = \{(0, 0)\}$
- in $\mathbb{C}^2$, $\mathbf{V}(x^2 + y^2) = \{(a, \pm ia),\ a \in \mathbb{C}\} = (1, -i)\mathbb{C} \cup (1, i)\mathbb{C}$
- in $\mathbb{C}^2$, $\mathbf{V}((x^2 + y^2)^{17}) = \{(a, \pm ia),\ a \in \mathbb{C}\} = (1, -i)\mathbb{C} \cup (1, i)\mathbb{C}$
- affine subspaces of k^n

Twisted cubic: $\mathbf{V}(y - x^2, z - x^3)$ in $\mathbb{R}^3$

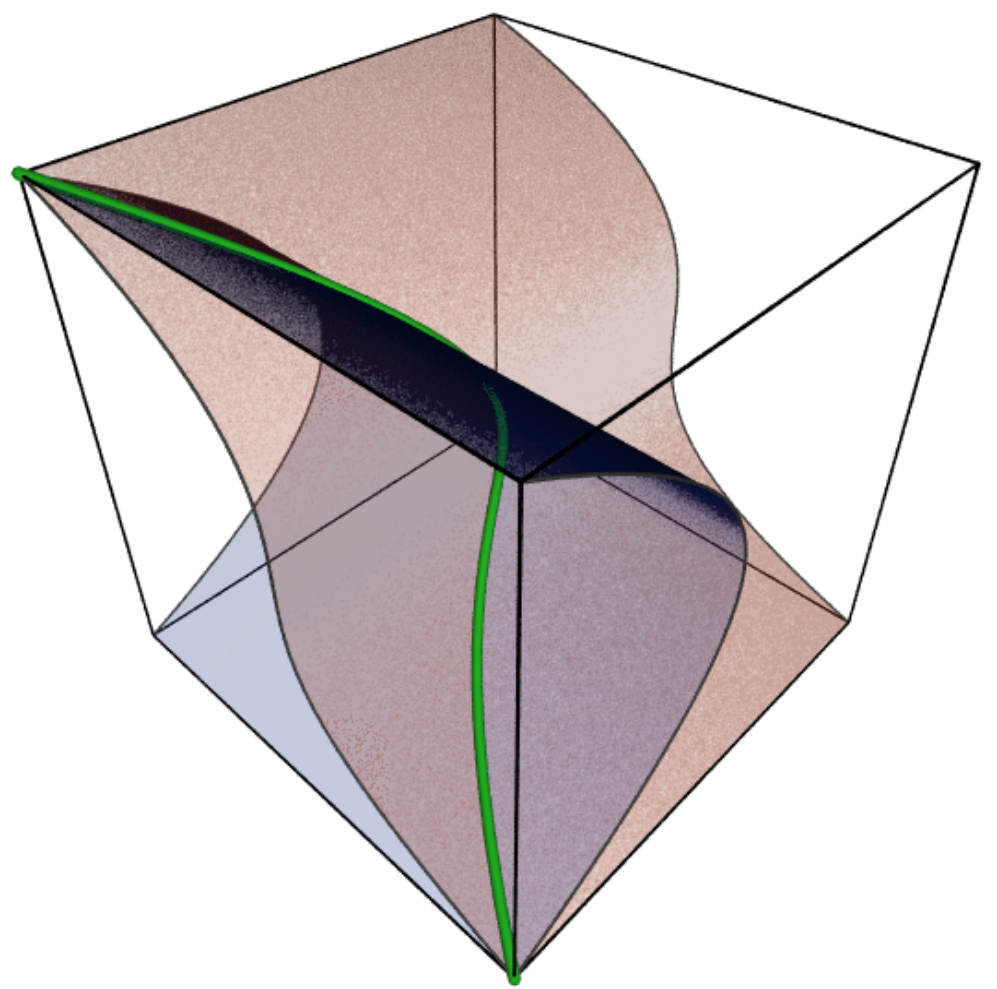


image from Wikipedia, user: Rocchini

Ideals in polynomials rings

A set of polynomials $I \subseteq k[x_1, \ldots, x_n]$ is an ideal if it is closed under addition and $f\, I \subseteq I$ for any $f \in k[x_1, \ldots, x_n]$

Examples:

- $\{0\}$ and $k[x_1, \ldots, x_n]$ in $k[x_1, \ldots, x_n]$
- $\{g(x, y, z)(x^2 + 3z),\ g \in \mathbb{R}[x, y, z]\}$ in $\mathbb{R}[x, y, z]$
- $\{g_1(x, y)\, x + g_2(x, y)\, y,\ g_i \in \mathbb{C}[x, y]\}$

Given polynomials $f_1, \ldots, f_m$, the ideal they generate is

$$\langle f_1, \ldots, f_m \rangle = \{g_1 f_1 + \cdots + g_m f_m,\ g_i \in k[x_1, \ldots, x_n]\}$$

Given a variety $V \in k^n$, we define the ideal of V as

$$\mathbf{I}(V) = \{f \in k[x_1, \ldots, x_n] \mid f(a) = 0 \text{ for every } a \in V\}$$

Ideals and varieties

If $I = \langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$,

$$\mathbf{V}(f_1, \ldots, f_s) = \mathbf{V}(g_1, \ldots, g_t) =: \mathbf{V}(I)$$

Example in $k[x, y]$:
$\langle xy + 1, y^2 - 1, x^2y + x \rangle = \langle x + y, y^2 - 1 \rangle$, so that we have
$\mathbf{V}(xy + 1, y^2 - 1, x^2y + x) = \mathbf{V}(x + y, y^2 - 1)$

Theorem (Hilbert's Basis Theorem)

Every ideal I in $k[x_1, \ldots, x_n]$ has a finite generating set:
$I = \langle f_1, \ldots, f_m \rangle$ *for some* $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$.

Conclusion: varieties are defined by ideals

Note: Hilbert's proof (end of XIXth century) is non-constructive

Special case: univariate polynomials

Here $n = 1$. What are the varieties in k? the ideals in $k[x]$?

By definition, $\mathbf{V}(f_1, \ldots, f_m) = \{\text{common roots of } f_1, \ldots, f_m\}$
$\Longrightarrow$ a variety is either k or a finite subset of k
... thanks to Euclidean division!

An ideal in $k[x]$ is either $\{0\}$ or $\langle g \rangle$ for some nonzero $g \in k[x]$
Indeed here $\langle f_1, \ldots, f_m \rangle = \langle \gcd(f_1, \ldots, f_m) \rangle$
... thanks to Euclidean division!

Correspondence between varieties and ideals
... up to zeroes' multiplicities and irreducible polynomials of degree > 1:

$$\begin{aligned} \mathbf{V}(f_1, \ldots, f_m) &= \mathbf{V}(\gcd(f_1, \ldots, f_m)) \\ \mathbf{I}(\{a_1, \ldots, a_s\}) &= \langle (x - a_1) \cdots (x - a_s) \rangle \end{aligned}$$

Univariate case put into perspective

Thanks to Euclidean division of univariate polynomials,

- Ideal description
  every ideal generated by one polynomial, which division can compute
- Does $f \in k[x]$ belongs to I? (Ideal membership)
  $\Leftrightarrow$ remainder zero in division by the generator
- Link between ideals and varieties
  the ideal of $\mathbf{V}(I) = \mathbf{V}(\langle g \rangle)$ is $\sqrt{I} = \langle \sqrt{g} \rangle$
  (where $\sqrt{\cdot}$ = discard multiplicities and irreducible factors of deg > 1)
- Does $f \in k[x]$ vanish on $\mathbf{V}(I)$? (Ideal of variety membership)
  $\Leftrightarrow$ remainder zero in division by $\sqrt{g}$

Euclidean division: given f and $g \neq 0$ in $k[x]$, compute the unique q, r such that $f = qg + r$ and $\deg r < \deg g$
What about division in $k[x_1, \ldots, x_n]$?

Outline

Division algorithm

Theorem (Division algorithm)

Fix a monomial order $\succ$. $F = (f_1, \ldots, f_m)$ an ordered list of polynomials. Every $f \in k[x_1, \ldots, x_n]$ can be written

$$f = a_1 f_1 + \cdots + a_m f_m + r$$

where the monomials appearing in r are not in $\langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_m) \rangle$. Furthermore $\mathrm{multideg}(f) \succeq \mathrm{multideg}(a_i f_i)$ for each i.

Example: in $k[x, y]$ using lexicographic order with $x > y$
Consider $f_1 = y^2 - 1, f_2 = xy - 1, f = x^2y + xy^2 + y^2$

- Dividing f by (f_1, f_2): $f = (x + 1) \cdot f_1 + x \cdot f_2 + 2x + 1$
- Dividing f by (f_2, f_1): $f = (x + y) \cdot f_2 + 1 \cdot f_1 + x + y + 1$

Special case: linear polynomials

Example: in $\mathbb{C}[x_1, x_2, x_3, x_4, x_5]$ using lex order

$$\begin{aligned} f_1 &= 13x_1 - 65x_2 - 14x_3 + 44x_4 - 85x_5 \\ f_2 &= -3x_1 + 15x_2 + 7x_3 - 17x_4 + 34x_5 \\ f_3 &= 4x_1 - 20x_2 - 4x_3 + 13x_4 - 25x_5 \\ f_4 &= -x_1 + 5x_2 - 3x_3 - 5x_5 \end{aligned}$$

Divide $f = 5x_1 + 3x_2 - 15x_3 + x_5$ by (f_1, f_2, f_3, f_4)

$$f = \frac{5}{13} \cdot f_1 + 28x_2 + \frac{70}{13}x_3 - \frac{415}{13}x_4 + \frac{438}{13}x_5$$

Now divide f_2 by (f_1, f_2, f_3, f_4):

$$f_2 = -\frac{3}{13} \cdot f_1 + \frac{49}{13}x_3 - \frac{89}{13}x_4 + \frac{187}{13}x_5$$

Frustrating results...

Focus on remainder

Two unwanted properties:

- Remainder depends on an ordering of the divisors
- Ideal membership does not imply zero remainder

Interested in remainder, not quotients

Division:

$$f = a_1 f_1 + \cdots + a_m f_m + r$$

where the monomials appearing in r are not in $\langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_m) \rangle$.

$\Rightarrow$ dividing by another basis of $\langle f_1, \ldots, f_m \rangle$ is ok!

Important role of the ideal of leading terms

Previous example: $\langle \mathrm{LT}(f_1), \mathrm{LT}(f_2), \mathrm{LT}(f_3), \mathrm{LT}(f_4) \rangle = \langle x_1 \rangle$

Division of $f \in \langle x_2, x_3, x_4, x_5 \rangle$ by $\{f_1, \ldots, f_4\}$ is f itself...

Note: $f_5 = \frac{3}{13} f_1 + f_2 = \frac{49}{13} x_3 - \frac{89}{13} x_4 + \frac{187}{13} x_5 \in \langle f_1, f_2, f_3, f_4 \rangle$

Special case: linear polynomials (continued)

We consider the matrix

$$\begin{bmatrix} 13 & -65 & -14 & 44 & -85 \\ -3 & 15 & 7 & -17 & 34 \\ 4 & -20 & -4 & 13 & -25 \\ -1 & 5 & -3 & 0 & -5 \end{bmatrix}$$

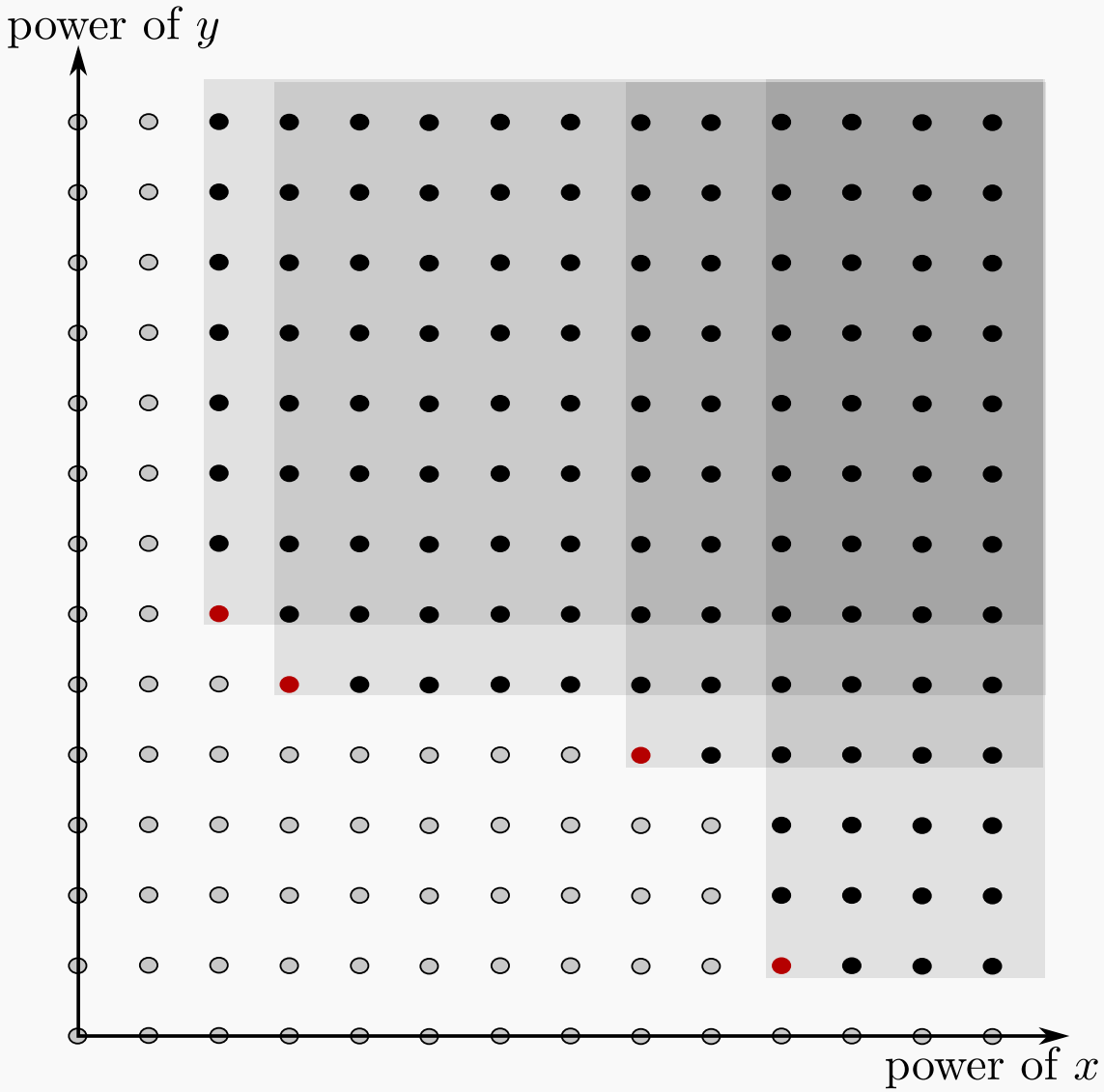
Reduced row echelon form (via Gaussian elimination)

$$\begin{bmatrix} 1 & -5 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & 2 \\ 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Gives $g_1 = x_1 - 5x_2 - x_5, \quad g_2 = x_3 + 2x_5, \quad g_3 = x_4 - x_5$

$$f = 5x_1 + 3x_2 - 15x_3 + x_5 \;=\; 5 \cdot g_1 - 15 \cdot g_2 \;+\; 28x_2 + 36x_5$$

Exponents of leading terms



Gröbner bases: introduction

Properties:

- $\langle f_1, f_2, f_3, f_4 \rangle = \langle g_1, g_2, g_3 \rangle$
- $\langle \mathrm{LT}(g_1), \mathrm{LT}(g_2), \mathrm{LT}(g_3) \rangle = \langle \mathrm{LT}(\langle f_1, f_2, f_3, f_4 \rangle) \rangle$

Definition (Gröbner basis (1960s, Buchberger / Hironaka))

Fix a monomial ordering $\succ$. Let $I \neq 0$ be an ideal of $k[x_1, \ldots, x_n]$.
$G = \{g_1, \ldots, g_s\}$ is a Gröbner basis for I if

$$\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle = \langle \mathrm{LT}(I) \rangle$$

- Buchberger's algorithm computes a Gröbner basis for $\langle f_1, \ldots, f_m \rangle \neq 0$
- Remainder independent of the order of the divisors $\{g_1, \ldots, g_s\}$

Gröbner bases: first results

- Compute the unique remainder of f on division by I
  $\longrightarrow$ Standard representation of elements in $k[x_1, \ldots, x_n]/I$
- Do $\{f_1, \ldots, f_s\}$ and $\{h_1, \ldots, h_t\}$ generate the same ideal?
  $\Leftrightarrow$ $\langle f_1, \ldots, f_s \rangle$ and $\langle h_1, \ldots, h_t \rangle$ have same reduced Gröbner basis
- Ideal membership: does f belong to I?
  $\Leftrightarrow$ remainder zero in division by a Gröbner basis for I
- Efficient implementations in many computer algebra systems

```
sage: R.<x,y> = PolynomialRing( CC, order="lex" )
sage: f1 = y^2-1 ; f2 = x*y - 1 ; f = x^2*y + x*y^2 + y^2
sage: I = Ideal( f1, f2 ) ; I.groebner_basis()
[x - y, y^2 - 1.00000000000000]
sage: I.reduce(f) ; (f1 + x*y*f2) in I
2.00000000000000*y + 1.00000000000000
True
```

Recall the univariate case...

Thanks to Euclidean division of univariate polynomials,

- Ideal description
  every ideal generated by one polynomial, which division can compute
- Does $f \in k[x]$ belongs to I? (Ideal membership)
  $\Leftrightarrow$ remainder zero in division by the generator
- Link between ideals and varieties
  the ideal of $\mathbf{V}(I) = \mathbf{V}(\langle g \rangle)$ is $\sqrt{I} = \langle \sqrt{g} \rangle$
  (where $\sqrt{\cdot}$ = discard multiplicities of zeroes and irreducible factors)
- Does $f \in k[x]$ vanish on $\mathbf{V}(I)$? (Ideal of variety membership)
  $\Leftrightarrow$ remainder zero in division by $\sqrt{g}$

Points 1 and 2 now generalized to the multivariate case!

What about points 3 and 4?

Outline

Maps $\mathbf{I}(\cdot)$ and $\mathbf{V}(\cdot)$

The two maps $\mathbf{I}(\cdot)$ and $\mathbf{V}(\cdot)$

$$\begin{array}{ccc} \text{Ideals of } k[x_1, \ldots, x_n] & \longleftrightarrow & \text{Varieties of } k^n \\ I & \xrightarrow{\mathbf{V}} & \mathbf{V}(I) \\ \mathbf{I}(V) & \xleftarrow{\mathbf{I}} & V \end{array}$$

are inclusion-reversing; furthermore

$$\begin{aligned} \mathbf{I}(\mathbf{V}(I)) &\supseteq I \\ \mathbf{V}(\mathbf{I}(V)) &= V \end{aligned}$$

so that $\mathbf{I}(\cdot)$ is one-to-one: $V_1 \neq V_2 \Rightarrow \mathbf{I}(V_1) \neq \mathbf{I}(V_2)$.

Different ideals yielding same variety:

- $\mathbf{V}(x^2 + y^2 + 1) = \mathbf{V}(x^{36} + \pi) = \mathbf{V}(1)$ in $\mathbb{R}^2$, distinct varieties in $\mathbb{C}^2$
- $\mathbf{V}((x-y)^2) = \mathbf{V}((x-y)^{17}) = \mathbf{V}(x-y)$ in k^2, for any k

Multiplicities and radical ideals

Example: $\mathbf{V}((x-y)^2) = \mathbf{V}((x-y)^{17}) = \mathbf{V}(x-y)$ in k^2

Property: if $f^r \in \mathbf{I}(V)$ for some r, then $f \in \mathbf{I}(V)$.

$$\mathbf{I}(V) \text{ is a radical ideal}$$

Given an ideal I, define $\sqrt{I} = \{f \in k[x_1, \ldots, x_n] \mid f^r \in I \text{ for some } r\}$

Example: in $\mathbb{C}[x]$, $\sqrt{\langle x^3(x-i)^2(x+5)^6 \rangle} = \langle x(x-i)(x+5) \rangle$

For any ideal I in $k[x_1, \ldots, x_n]$,

$$\begin{aligned} \mathbf{V}(I) &= \mathbf{V}(\sqrt{I}) \\ \mathbf{I}(\mathbf{V}(I)) &\supseteq \sqrt{I} \end{aligned}$$

Algorithm for Radical membership

$$\mathbf{I}(\mathbf{V}(I)) \supseteq \sqrt{I} \supseteq I$$

Problem (Radical membership)

Let $I = \langle f_1, \ldots, f_m \rangle$ and $f \in k[x_1, \ldots, x_n]$.
Does f belong to $\sqrt{I}$?

Rabinowitsch trick (1929):

$$f \in \sqrt{I} \iff \langle f_1, \ldots, f_m, 1 - yf \rangle = \langle 1 \rangle \text{ in } k[x_1, \ldots, x_n, y]$$

For any monomial order, the reduced Gröbner basis for $\langle 1 \rangle$ is $\{1\}$

$\Rightarrow$ algorithm for Radical membership
$\Rightarrow$ partial answer to Ideal of variety membership

Algorithm for the Consistency problem

Example: $\mathbf{V}(x^2 + y^2 + 1) = \mathbf{V}(x^{36} + \pi) = \mathbf{V}(1)$ in $\mathbb{R}^2$, distinct in $\mathbb{C}^2$

Assume now that k is algebraically closed

In $k[x]$: f, g have no common root iff $\gcd(f, g) = 1$

Theorem (Weak Nullstellensatz)

Polynomials which generate a proper ideal always have a common zero:

$$\mathbf{V}(I) = \emptyset \Leftrightarrow I = \langle 1 \rangle = k[x_1, \ldots, x_n]$$

$\Rightarrow$ algorithm for the Consistency problem:
does the polynomial system $(f_1 = 0, \ldots, f_m = 0)$ have a solution?

Ideals and varieties: the Strong Nullstellensatz

Let $I = \langle f_1, \ldots, f_m \rangle$ and $f \in k[x_1, \ldots, x_n]$.
Introduce $I_f = \langle f_1, \ldots, f_m, 1 - yf \rangle$ in $k[x_1, \ldots, x_n, y]$.

Rabinowitsch trick (1929), using the Weak Nullstellensatz:

$$f \text{ vanishes on } \mathbf{V}(I) \iff \mathbf{V}(I_f) = \emptyset \text{ in } k^{n+1} \iff f \in \sqrt{I}$$

Theorem (Strong Nullstellensatz)

$$\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$$

$\Rightarrow$ Ideal of variety membership directly reduces to Radical membership
... if k is algebraically closed! (e.g. $k = \mathbb{C}$)

Outline

Variety defined by a monomial ideal

Variety of a monomial ideal = finite union of coordinate subspaces of k^n

Example: $I = \langle x^2y, xz^3 \rangle$ in $k[x, y, z]$. In k^3,
$\mathbf{V}(I) = \mathbf{V}(x^2y) \cap \mathbf{V}(xz^3) = (\mathbf{V}(x) \cup \mathbf{V}(y)) \cap (\mathbf{V}(x) \cup \mathbf{V}(z)) = \mathbf{V}(x) \cup \mathbf{V}(y, z)$.

Definition (Dimension of a variety defined by a monomial ideal)

The dimension of a finite union of coordinate subspaces is the largest of the dimensions of these subspaces.

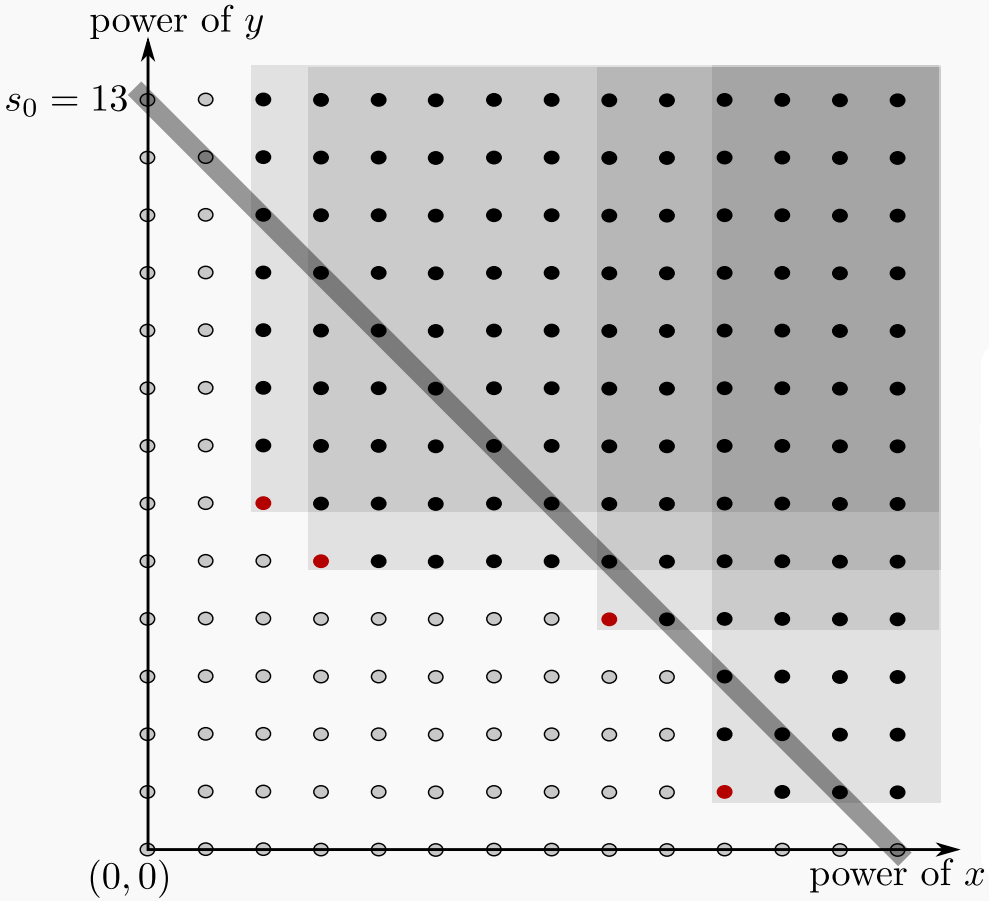
Algorithm to compute $\dim \mathbf{V}(I)$, $I = \langle x^{\alpha_1}, \ldots, x^{\alpha_m} \rangle$

- compute the smallest subset of variables $x_{i_1}, \ldots, x_{i_t}$ such that for every i, x^{α_i} is divisible by x_{i_j} for some j
- return $n - t$ if it is $\geqslant 0$, else report $\mathbf{V}(I) = \emptyset$

Hilbert function and polynomial of a monomial ideal

Hilbert function:

$\mathrm{HF}_I(s) =$ number of monomials of total degree $\leqslant s$ not in the ideal I



Example:

$I = \langle x^2y^6, x^3y^5, x^8y^4, x^{10}y \rangle$

When $s > s_0$,

$\mathrm{HF}_I(s) = \mathrm{HF}_I(s-1) + 3$

Theorem (Hilbert polynomial)

There is a polynomial $\mathrm{HP}_I(s)$ *s.t.*

$$\mathrm{HF}_I(s) = \mathrm{HP}_I(s)$$

for all s sufficiently large.

The degree of $\mathrm{HP}_I(s)$ *is* $\dim \mathbf{V}(I)$.

Dimension of a variety

Hilbert function of an ideal $I \subseteq k[x_1, \ldots, x_n]$:
$\mathrm{HF}_I(s) = \dim_k k[x_1, \ldots, x_n]_{\leqslant s}/I_{\leqslant s} = \dim_k k[x_1, \ldots, x_n]_{\leqslant s} - \dim_k I_{\leqslant s}$

Central property: Fix a graded monomial order, $\mathrm{HF}_I(s) = \mathrm{HF}_{\langle \mathrm{LT}(I) \rangle}(s)$

Definition (Dimension of a variety)

$V \in k^n$ a variety. The dimension of V is

$$\dim V = \deg \mathrm{HP}_{\mathbf{I}(V)}(s)$$

Note: $\deg \mathrm{HP}_I(s) = \deg \mathrm{HP}_{\sqrt{I}}(s)$
$\rightarrow$ consistent with the definition for monomial ideals
$\rightarrow$ if k algebraically closed, $\dim \mathbf{V}(I) = \deg \mathrm{HP}_I(s)$

Properties of dimension

Algorithm for computing the dimension of $V = \mathbf{V}(f_1, \ldots, f_m)$
(k is algebraically closed; using a graded monomial order)

- Step 1: compute a Gröbner basis $\{g_1, \ldots, g_s\}$ for $\langle f_1, \ldots, f_m \rangle$
- Step 2: compute $\dim V = \dim \mathbf{V}(\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle)$

k algebraically closed

- if $V_1 \subseteq V_2$ then $\dim V_1 \leqslant \dim V_2$
- $\dim \mathbf{V}(f) = n - 1$ (f nonconstant)
  $\dim \mathbf{V}(I) \geqslant \dim \mathbf{V}(I + \langle f \rangle) \geqslant \dim \mathbf{V}(I) - 1$
- V is finite $\iff \dim V = 0$
- $\dim V \cup W = \max(\dim V, \dim W)$
- $\dim V =$ largest of the dimensions of the irreducible components of V

Conclusion

1. Ideals and varieties
2. Division algorithm and Gröbner bases
3. Correspondence *Ideals* $\longleftrightarrow$ *Varieties*
4. Dimension of a variety