Hilbert’s Nullstellensatz

Bernhard Bauer

bauerb@in.tum.de

Sarntal, September 19 – October 1, 2004

Outline

Affine Varieties

Problem: Given a set of polynomials $f_1, \ldots, f_r \in k[x_1, \ldots, x_n]$, what are the common zeroes?

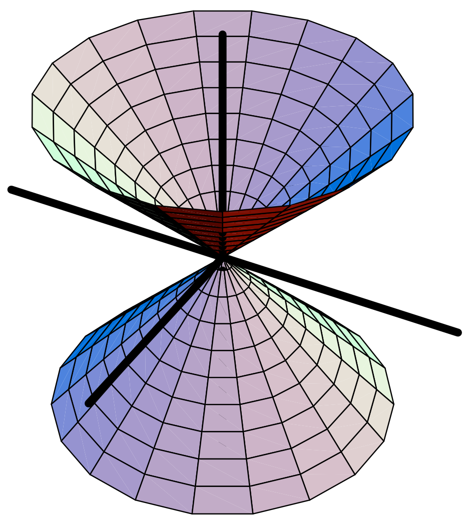
Definition 1 *Let k be a field, and let $f_1, \ldots, f_r$ be polynomials in $k[x_1, \ldots, x_n]$. Then we set*

$$\mathbf{V}(f_1, \ldots, f_r) = \{(a_1, \ldots, a_n) \in k^n : f_i(a_1, \ldots, a_n) = 0 \text{ for all } 1 \leq i \leq r\}.$$

We call $\mathbf{V}(f_1, \ldots, f_r)$ the ***affine variety*** *(or simply variety) defined by $f_1, \ldots, f_r$.*

Examples of affine varieties (in $\mathbb{R}^3$)

- $\mathbf{V}(z)$: xy-plane
- $\mathbf{V}(x, y)$: z-axis
- $\mathbf{V}(x^2 + y^2 - z^2)$: cone



Ideals

We now consider the set of all polynomials vanishing on a given variety.

Definition 2 *Let $V \subset k^n$ be an affine variety. The we set*

$$\mathbf{I}(V) = \{f \in k[x_1, \ldots, x_n] : f(a_1, \ldots, a_n) = 0 \textit{ for all } (a_1, \ldots, a_n) \in V\}.$$

$\mathbf{I}(V)$ is an *ideal* in $k[x_1, \ldots, x_n]$. This means:

Definition 3 *A subset I of a ring R is an **ideal** if:*

(i) $0 \in I$.

(ii) If $f, g \in I$, then $f + g \in I$.

(iii) If $f \in I$ and $h \in R$, then $hf \in I$.

An ideal is closed under linear combinations with R.

Ideals (2)

Every ideal $I \subset k[x_1, \ldots, x_n]$ can be generated by linear combinations of a *finite* set of polynomials called **basis** (Hilbert's Basis Theorem):

$$I = \langle f_1, \ldots, f_r \rangle = \{A_1 f_1 + \ldots + A_r f_r : f_1, \ldots, f_r \in k[x_1, \ldots, x_n]\}$$

An ideal generated by a single polynom is called a **principal ideal**.

Examples:

- $\langle x \rangle$: The set of all polynomials divisible by x
- $\langle 1 \rangle = k[x_1, \ldots, x_n]$

The Ideal-Variety Correspondence

The variety $\mathbf{V}(I)$ of a whole ideal $I = \langle f_1, \ldots, f_r \rangle$ is the same as the variety of its generators $\mathbf{V}(f_1, \ldots, f_r)$.

Therefore, we have maps

$$\mathbf{V} : \text{ideals} \mapsto \text{affine varieties}$$

and

$$\mathbf{I} : \text{affine varieties} \mapsto \text{ideals}$$

which give us a correspondence between ideals and varieties.

Is this correspondence one-to-one?

- $\mathbf{V}(\mathbf{I}(V)) = V$, i.e. $\mathbf{I}$ is one-to-one
- Different ideals can give the same variety:
  - $\langle x \rangle \neq \langle x^2 \rangle$, but $\mathbf{V}(x) = \mathbf{V}(x^2) = \{0\}$
  - If k isn't algebraically closed, e.g. $k = \mathbb{R}$:
    $I_1 = \langle 1 \rangle, I_2 = \langle 1 + x^2 \rangle, I_3 = \langle 1 + x^2 + x^4 \rangle$ are different ideals, but
    $\mathbf{V}(I_1) = \mathbf{V}(I_2) = \mathbf{V}(I_3) = \emptyset$

The Weak Nullstellensatz

Theorem 1 *Let k be an algebraically closed field and let $I \subset k[x_1, \ldots, x_n]$ be an ideal with $\mathbf{V}(I) = \emptyset$. Then $I = k[x_1, \ldots, x_n]$.*

We can check whether a set of polynomials $f_1, \ldots, f_r \in k[x_1, \ldots, x_n]$ has one or more common zeroes (**consistency problem**) if we check whether the ideal $\langle f_1, \ldots, f_r \rangle$ generated by them is not equal to $k[x_1, \ldots, x_n]$.

Gröbner Bases

A basis of an ideal $\langle f_1, \ldots, f_r \rangle$ is a **Gröbner Basis** $G(f_1, \ldots, f_r)$ for some monomial order if the ideal given by the leading terms of all elements of the ideal is itself generated by the leading terms of the basis.

A **reduced** Gröbner Basis G_{red} is a Gröbner Basis where the coefficients of the leading terms are 1 and no monomial in any element of the basis can be generated by the leading terms of the rest of the basis.

Properties of Gröbner Bases:

- The remainder obtained when applying the **multivariate division algorithm** is independent of the ordering of the polynomials.

- The reduced Gröbner Basis is unique up to the monomial ordering, and can therefore be used to check the equality of two ideals.

- When using lexicographic order with $x_1 > x_2 > \ldots > x_n$, the intersection of an ideal I with the subring $k[x_m, x_{m+1}, \cdots, x_n]$ is generated by the intersection of the Gröbner Basis $G(I)$ with $k[x_m, x_{m+1}, \cdots, x_n]$ (**elimination property**).

A Gröbner Basis can be computed using **Buchberger's Algorithm**.

The Consistency Problem

A set of polynomials $f_1, \ldots, f_r \in k[x_1, \ldots, x_n]$ has no common zeroes iff

$$\langle f_1, \ldots, f_r \rangle = k[x_1, \ldots, x_n]$$
$$\Leftrightarrow 1 \in \langle f_1, \ldots, f_r \rangle$$

This is the case if the reduced Gröbner Basis $G_{red}(f_1, \ldots, f_r) = \{1\}$.

Hilbert's Nullstellensatz

We have seen that $\langle x \rangle$ and $\langle x^2 \rangle$ lead to the same variety.

In general, a power of a polynomial vanishes on the same set as the original polynomial.

Hilbert's Nullstellensatz states that (over an algebraically closed field) this the only reason that two different ideals lead to the same variety:

Theorem 2 *Let k be an algebraically closed field. If $f, f_1, \ldots, f_r \in k[x_1, \ldots, x_n]$ are such that $f \in \mathbf{I}(\mathbf{V}(f_1, \ldots, f_r))$, then there exists an integer $m \geq 1$ such that $f^m \in \langle f_1, \ldots, f_r \rangle$.*

Proof

Given a polynomial f which vanishes at every common zero of the polynomials $f_1, \ldots, f_r$, we must show that there exists an integer $m \geq 1$ and polynomials $A_1, \ldots, A_r$ such that

$$f^m = A_1 f_1 + A_2 f_2 + \ldots + A_r f_r$$

To show this, we consider the ideal

$$\tilde{I} = \langle f_1, \ldots, f_r, 1 - yf \rangle \subset k[x_1, \ldots, x_n, y].$$

We claim that $\mathbf{V}(\tilde{I}) = \emptyset$.

To see this, let $(a_1, \ldots, a_n, a_{n+1}) \in k^{n+1}$. Either

- $(a_1, \ldots, a_n)$ is a common zero of $f_1, \ldots, f_r$, or
- $(a_1, \ldots, a_n)$ is not a common zero of $f_1, \ldots, f_r$.

In the first case $f(a_1, \ldots, a_n)$ since f vanishes at every common zero of $f_1, \ldots, f_r$. Thus, $1 - yf = 1 - a_{n+1} f(a_1, \ldots, a_n) = 1 \neq 0$ at the point $(a_1, \ldots, a_n, a_{n+1})$.

Proof(2)

In the second case, for some f_i, $f_i(a_1, \ldots, a_n) \neq 0$. If we think of f_i as a polynomial with $n+1$ variables which doesn't depend on the last variable, we have $f_i(a_1, \ldots, a_n, a_{n+1}) \neq 0$.

Because one of the two cases applies for any $(a_1, \ldots, a_n, a_{n+1})$, $\mathbf{V}(\tilde{I})$ must be empty. We now apply the Weak Nullstellensatz to conclude that $1 \in \tilde{I}$. That is,

$$1 = \sum_{i=1}^{s} p_i(x_1, \ldots, x_n, y) f_i + q(x_1, \ldots, x_n, y)(1 - yf)$$

for some polynomials $p_i, q \in k[x_1, \ldots, x_n, y]$. Now set $y = 1/f(x_1, \ldots, x_n)$. Then we get

$$1 = \sum_{i=1}^{s} p_i(x_1, \ldots, x_n, 1/f) f_i.$$

If we multiply both sides by f^m, where m is chosen high enough to clear all the denominators, we have for some $A_i \in k[x_1, \ldots, x_n]$:

$$f^m = \sum_{i=1}^{s} A_i f_i.$$

Radical Ideals

Definition 4 *An ideal I is **radical** if $f^m \in I$ for any integer $m \geq 1$ implies that $f \in I$.*

We also define the operation of taking the radical of an ideal:

Definition 5 *Let $I \subset k[x_1, \ldots, x_n]$ be an ideal. The **radical** of I, denoted $\sqrt{I}$, is the set*

$$\{f : f^m \in I \text{ for some integer } m \geq 1\}.$$

For an arbitrary ideal, the computation of a basis for a radical is quite complicated. Fortunately, it is simpler for principal ideals:

$$\sqrt{\langle f \rangle} = \sqrt{\langle f_1^{a_1} f_2^{a_2} \cdots f_r^{a_r} \rangle} = \langle f_1 f_2 \cdots f_r \rangle$$

Hilbert's Nullstellensatz (in terms of ideals) states that

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

Sums of Ideals

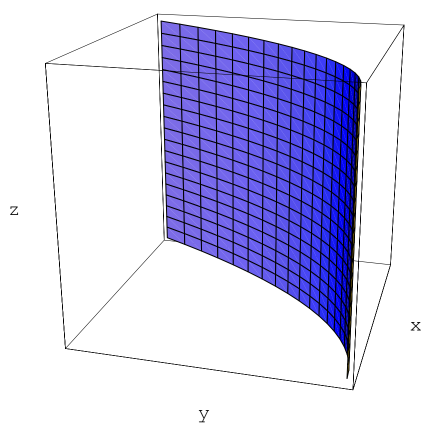
Definition 6 *If I and J are ideals in $k[x_1, \ldots, x_n]$, then the* ***sum*** *of I and J, denoted $I + J$, is the set*

$$I + J = \{f + g : f \in I \text{ and } g \in J\}.$$

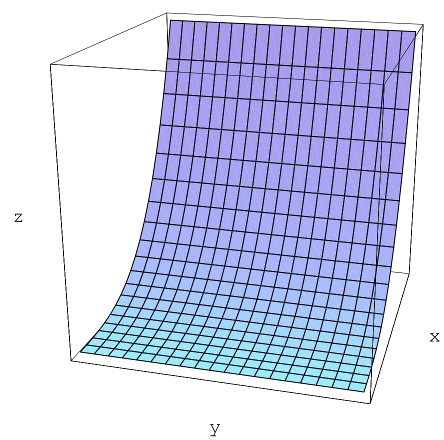
If $I = \langle f_1, \ldots, f_r \rangle$ and $J = \langle g_1, \ldots, g_s \rangle$, then $I + J = \langle f_1, \ldots, f_r, g_1, \ldots, g_s \rangle$.

The corresponding operation on varieties is intersection:

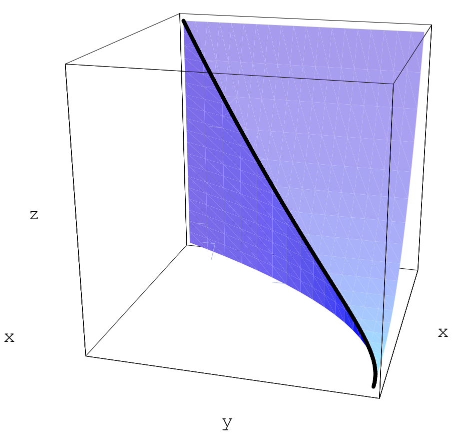
$$\mathbf{V}(I + J) = \mathbf{V}(I) \cap \mathbf{V}(J)$$



V(y-x²)



V(z-x³)



V(y-x², z-x³)

Products of Ideals

Definition 7 *If I and J are ideals in $k[x_1, \ldots, x_n]$, then the **product** of I and J, denoted $I \cdot J$ or short IJ, is the set*

$$I \cdot J = \{fg : f \in I \text{ and } g \in J\}.$$

If $I = \langle f_1, \ldots, f_r \rangle$ and $J = \langle g_1, \ldots, g_s \rangle$, then
$IJ = \langle f_i g_j : 1 \leq i \leq n, 1 \leq j \leq m \rangle$.

The corresponding operation on varieties is union:

$$\mathbf{V}(IJ) = \mathbf{V}(I) \cup \mathbf{V}(J)$$

Example: $\langle x, y \rangle \cdot \langle z \rangle = \langle xz, yz \rangle$.
$\mathbf{V}(xz, yz)$ is the union of the z-axis $\mathbf{V}(x, y)$ and the xy-plane $\mathbf{V}(z)$.

Intersections of Ideals

Definition 8 *The **intersection** $I \cap J$ of two ideals I and $J \in k[x_1, \ldots, x_n]$ is the set of all polynomials which belong to both I and J.*

The corresponding operation on varieties is again union:

$$\mathbf{V}(I \cap J) = \mathbf{V}(I) \cup \mathbf{V}(J)$$

Calculating a basis is a bit more difficult than in the former two cases:

$$\langle f_1, \ldots, f_r \rangle \cap \langle g_1, \ldots, g_s \rangle =$$
$$\langle tf_1, \ldots, tf_r, (1-t)g_1, \ldots, (1-t)g_s \rangle \cap k[x_1, \ldots, x_n]$$

The elimination of t can be done via the elimination property of Gröbner Bases: Calculate a Gröbner basis with lexicographic order where $t > x_1 > \ldots > x_n$ and drop all polynomials which depend on t.

The GCD of two polynomials

The intersection of two principal ideals gives the ideal generated by the lowest common multiple of the polynomials.

$$\langle f \rangle \cap \langle g \rangle = \langle \mathrm{LCM}(f, g) \rangle$$

Compare with product:

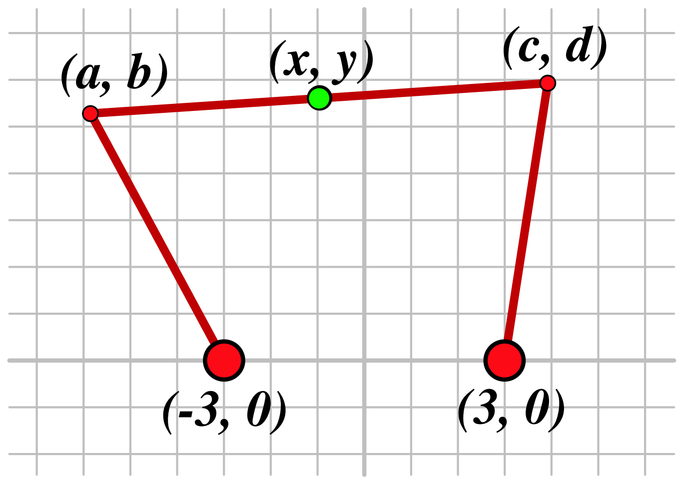
$$\langle f \rangle \cdot \langle g \rangle = \langle f \cdot g \rangle \subset \langle f \rangle \cap \langle g \rangle$$

Therefore, we can calculate the greatest common divisor of two polynomials (without having to factorise them):

$$\mathrm{GCD}(f, g) = \frac{f \cdot g}{\mathrm{LCM}(f, g)}$$

An Application from Mechanics

We have the following leverage mechanism:



What are the possible locations of the green point (x, y)?

The restrictions can be described by polynomial equations:

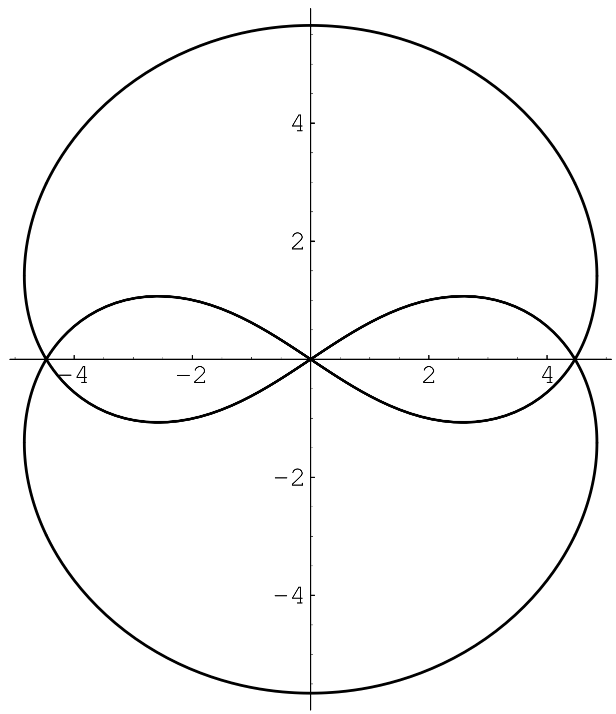
$$
\begin{aligned}
&(a+3)^2+b^2=6^2 && \Rightarrow f_1=a^2+6a+c^2-27\\
&(c-3)^2+d^2=6^2 && \Rightarrow f_2=-6b+b^2+d^2-27\\
&(c-a)^2+(d-b)^2=10^2 && \Rightarrow f_3=a^2-2ab+b^2+c^2-2cd+d^2-100\\
&x=\tfrac{1}{2}(a+c) && \Rightarrow f_4=a+b-2x\\
&y=\tfrac{1}{2}(b+d) && \Rightarrow f_5=c+d-2y
\end{aligned}
$$

The variety $\mathbf{V}(f_1,\ldots,f_5)\subset\mathbb{R}^6$ generated by these polynomials describes all possible 6-tuples (a,b,c,d,x,y).

We calculate a Gröbner basis using lexicographic order with $a>b>c>d>x>y$. By to the elimination property, the last element of the basis depends only on x and y:

$$f_6=x^6+3x^4y^2-40x^4+3x^2y^4-44x^2y^2+400x^2+y^6-4y^4-896y^2$$

Plotting $\mathbf{V}(f_6)$ gives the following picture:



Different values for the distance between the fixed points give completely different pictures (distance is, from left to right, 2, 10, 10.2, 16):