Computer Algebra and Gröbner Bases

Frank-Olaf Schreyer

Saarland University WS 2020/21

Overview

Today we will prove Hilbert's Nullstellensatz.

1. Vanishing loci of ideals
2. The projection theorem
3. Change of coordinates
4. Proof of the Nullstellensatz
5. Tower of projections

Hilbert's Nullstellensatz

Theorem. *Let K be an algebraically closed field, and $f_1, \dots, f_r \in K[x_1, \dots, x_n]$.*

$$V(f_1, \dots, f_r) = \emptyset \iff 1 \in (f_1, \dots, f_r).$$

Remember: $\mathbb{A}^n = K^n$ always denotes the affine space over an algebraically closed field.

$$V(f_1, \dots, f_r) = \{a \in \mathbb{A}^n \mid f_j(a) = 0 \text{ for } j = 1 \dots, r\}.$$

The right hand condition can be decided by computing a Gröbner basis for $f_1, \dots, f_r$.
$\Leftarrow$ is by an elementary argument true.

Vanishing loci of ideals.

Definition. Let $I \subset K[x_1, \dots, x_n]$ be an ideal. We define

$$V(I) = \{a \in \mathbb{A}^n \mid f(a) = 0 \, \forall f \in I\}$$

Since I is finitely generated, say $I = (f_1, \dots, f_r)$, we have

$$V(I) = V(f_1, \dots, f_r).$$

The basic approach of the proof of the Nullstellensatz is an induction of the number of variables.

If $n = 1$, the theorem holds, because $K[x]$ is a principal ideal domain. So every ideal

$$(0) \subsetneq I \subsetneq K[x]$$

is generated by a monic polynomial of positive degree, $I = (f)$, and f has a zero because K is algebraically closed.

Basic approach of the induction step

Let $I \subset K[x_1, \ldots, x_n]$. Consider the projection

$$\mathbb{A}^n \to \mathbb{A}^{n-1}, (a_1, \ldots, a_n) \mapsto (a_2, \ldots, a_n)$$

and the ideal

$$I_1 = I \cap K[x_2, \ldots, x_n]$$

obtained by eliminating x_1. If $I \neq (1)$, then $I_1 \neq (1)$, so by the induction hypothesis $V(I_1) \subset \mathbb{A}^{n-1}$ is non empty.
Let

$$a' = (a_2, \ldots, a_n) \in V(I_1) \subset \mathbb{A}^{n-1}$$

be a point and consider the ideal

$$(\{f(x_1, a') \mid f \in I\}) \subset K[x_1].$$

This is a principal ideal and a root a_1 of its generator would give a solution

$$a = (a_1, a') \in V(I) \subset \mathbb{A}^n.$$

A counter example

So we have a diagram

$$
\begin{array}{ccc}
V(I) & \subset & \mathbb{A}^n \\
\downarrow & & \downarrow \pi \\
V(I_1) & \subset & \mathbb{A}^{n-1}
\end{array}
.
$$

Since $I_1 \subset I$ we have $\pi(V(I)) \subset V(I_1)$. However the map is not necessarily surjective.

Example. For $I = (xy - 1)$ we have $I_1 = (0) \subset k[y]$ but the origin $a' = 0 \in V(I_1) = \mathbb{A}^1$ has no preimage:
$(\{f(x, a') \mid f \in I\}) = (x0 - 1) = (-1)$ has no zero.
In a certain sense the solution $(1/t, t)$ approaches $(\infty, 0)$ for $t \to 0$.

part 1

The projection theorem

Theorem. *Let* $I \subset K[x_1, \ldots, x_n]$ *be an ideal, and* $I_1 = I \cap K[x_2, \ldots, x_n]$. *Suppose* I *contains an element* f *which is monic in* x_1*:*

$$f = x_1^d + c_1(x_2, \ldots, x_n)x_1^{d-1} + \ldots + c_d(x_2, \ldots, x_n).$$

Then the projection

$$\pi \colon \mathbb{A}^n \to \mathbb{A}^{n-1}, (a_1, \ldots, a_n) \mapsto (a_2, \ldots, a_n)$$

onto the last $n-1$ *components satisfies*

$$\pi(V(I)) = V(I_1).$$

Remark. Since $f \in I$ we can have at most d points $a \in V(I)$ over any given point $a' \in V(I_1)$.

Proof of the projection theorem

We already know that $\pi(V(I)) \subset V(I_1)$ because $I_1 \subset I$.

To prove the converse inclusion we have to find for any $a' \in \mathbb{A}^{n-1} \setminus \pi(V(I))$ a polynomial $h \in I_1$ with $h(a') \neq 0$.

We will do this in two steps.

Step 1. *For every polynomial $g \in K[x_1, \ldots, x_n]$ there exists a polynomial $\tilde{g} \in K[x_1, \ldots, x_n]$ of degree $< d$ in x_1 such that*

$$\tilde{g}(x_1, a') = 0 \text{ and } g \equiv \tilde{g} \mod I.$$

Consider the ring homomorphism

$$\varphi : K[x_1, \ldots, x_n] \to K[x_1], g \mapsto g(x_1, a').$$

Since $a' \notin \pi(V(I))$ the Nullstellensatz in one variable implies

$$\varphi(I) = K[x_1].$$

Proof of step 1

Thus for every $g \in K[x_1, \ldots, x_n]$ there exists a $g_1 \in I$ with $\varphi(g) = \varphi(g_1)$. Consider $g_2 = g - g_1$. Since f is monic in x_1, division of g_2 by f gives an expression

$$g_2 = qf + \tilde{g}.$$

The remainder $\tilde{g}$ has degree $< d$ in x_1. Applying φ to this equation yields

$$0 = q(x_1, a')f(x_1, a') + \tilde{g}(x_1, a').$$

Thus $\tilde{g}(x_1, a')$ is the unique remainder of 0 under the division by $f(x_1, a')$. Hence $\tilde{g}(x_1, a') = 0 \in K[x_1]$ and

$$\begin{aligned} \tilde{g} - g = g_2 - qf - g &= g - g_1 - qf - g \\ &= -g_1 - qf \in I. \end{aligned}$$

Thus $g \equiv \tilde{g} \mod I$. $\square$

Step 2

Applying step 1 to the polynomials $1, x_1, x_1^2, \ldots, x_1^{d-1}$ we find expressions

$$\begin{array}{rcll} 1 & \equiv & g_{00} + g_{01}x_1 + \ldots + g_{0,d-1}x^{d-1} & \mod I \\ x_1 & \equiv & g_{10} + g_{11}x_1 + \ldots + g_{1,d-1}x^{d-1} & \mod I \\ & \vdots & & \\ x_1^{d-1} & \equiv & g_{d-1,0} + g_{d-1,1}x_1 + \ldots + g_{d-1,d-1}x^{d-1} & \mod I \end{array}$$

with $g_{ij} \in K[x_2, \ldots, x_n]$ and $g_{ij}(a') = 0$. In matrix form we have

$$(E_d - B) \begin{pmatrix} 1 \\ x_1 \\ \vdots \\ x_1^{d-1} \end{pmatrix} \equiv 0 \mod I$$

where $B = (g_{ij})$ and E_d is the $d \times d$ identity matrix.

Step 2 continued

Multiplying the last equation with the cofactor matrix of $(E_d - B)$ we arrive at

$$\det(E_d - B)\begin{pmatrix} 1 \\ x_1 \\ \vdots \\ x_1^{d-1} \end{pmatrix} \equiv 0 \mod I.$$

In particular $h = \det(E_d - B) \in I \cap K[x_2, \ldots, x_n] = I_1$. Since $h(a') = \det E_d = 1 \neq 0$ we have found our desired polynomial which does not vanish at a'.

This completes the proof of the projection theorem. $\square$

part 2

A change of coordinates

Lemma. *Let $f \in K[x_1, \ldots, x_n]$ be a non-constant polynomial.*

1. *If K be an infinite field and $a_2, \ldots, a_n \in K$ are sufficiently general elements, then substituting*
$$x_j = \tilde{x}_j + a_j x_1 \text{ for } j = 2, \ldots, n$$
into f gives a polynomial
$$\tilde{f} = a x_1^d + c_1(\tilde{x}_2, \ldots, \tilde{x}_n) x_1^{d-1} + \ldots + c_d(\tilde{x}_2, \ldots, \tilde{x}_n)$$
with $d \geq 1$, $a \in K \setminus \{0\}$ and $c_j \in K[\tilde{x}_2, \ldots, \tilde{x}_n]$.
2. *If K is an arbitrary field, then a substitution of the form*
$$x_j = \tilde{x}_j + x_1^{(r^{j-1})} \text{ for } j = 2, \ldots, n$$
for $r \in \mathbb{N}$ sufficiently large yields a polynomial $\tilde{f}$ of the same shape.

Proof of the Lemma, case 1

Let $d = \deg f$ denote the degree of f and let

$$f = f_d + \ldots + f_1 + f_0 \text{ with } f_k = \sum_{|\alpha|=k} f_\alpha x^\alpha$$

be the decomposition of $f = \sum f_\alpha x^\alpha$ into homogeneous parts. Then $f_d(1, x_2, \ldots, x_n)$ is not the zero polynomial. Hence by Exercise 1 on sheet 1 there exists $(a_2, \ldots, a_n) \in \mathbb{A}^{n-1}(K)$ with $a = f_d(1, a_2, \ldots a_n) \neq 0$. The substitution $x_j = \tilde{x}_j + a_j x_1$ gives

$f_d(x_1, \tilde{x}_2 + a_2 x_1, \ldots, \tilde{x}_n + a_n x_1) = a x_1^d +$ terms of lower degree in x_1.

Thus $f(x_1, \tilde{x}_2 + a_2 x_1, \ldots, \tilde{x}_n + a_n x_1)$ has the desired shape.

Proof of the Lemma, case 2

Take

$$r > \max\{e \mid \exists\alpha\,\exists j \text{ with } f_\alpha \neq 0 \text{ and } \alpha_j = e\}$$

larger than any exponent occuring in a term of f. Then the monomials

$$x_1^{\sum_{j=1}^{n} \alpha_j r^{j-1}} \text{ for } \alpha \text{ with } \alpha \neq 0$$

are all distinct, and the largest one will give the desired leading term after the substitution. □

Example. For $f = xy - 1$ every substitution $y = \tilde{y} + a_2 x$ for $a_2 \neq 0$ has the desired effect:

$$\tilde{f} = a_2 x^2 + x\tilde{y} - 1.$$

Proof of the Nullstellensatz

Let $I \subsetneq K[x_1, \ldots, x_n]$ be a proper ideal. We have to prove that $V(I) \neq \emptyset$. If $I = (0)$, then $V(I) = \mathbb{A}^n$. Otherwise there exists a non-constant polynomial $f \in I$. After a change of coordinates as in the Lemma we may assume that f is monic in x_1. Thus the projection $V(I) \to V(I_1)$ is surjective. Since $1 \notin I_1 \subset I$ we obtain $V(I_1) \neq \emptyset$ from the induction hypothesis. Hence $V(I) \neq \emptyset$ as well. □

Remark. Notice that we can perform the change of coordinates over the field of definition of I. Thus for example if $I \subset \mathbb{C}[x_1, \ldots, x_n]$ is generated by polynomials in $\mathbb{Q}[x_1, \ldots, x_n]$ we can take a linear change of coordinates defined over $\mathbb{Q}$.

part 3

A tower of projections

Theorem. *Suppose that* $I \subsetneq K[x_1, \ldots, x_n]$ *is a proper ideal. Let* $I_j = I \cap K[x_{j+1}, \ldots, x_n]$ *be the* j*-th elimination ideal. Set*

$$c = \min\{j \mid I_j = (0)\}$$

and suppose that for each j *with* $0 \leq j \leq c-1$ *the ideal* I_j *contains an* x_{j+1}*-monic polynomial of degree* d_j*. Then the projections* $\pi_c \colon V(I) \to \mathbb{A}^{n-c}$ *onto the last* $n-c$ *components is surjective and each fiber*

$$\pi_c^{-1}(a_{c+1}, \ldots, a_n)$$

is finite of cardinality $\leq \prod_{j=0}^{c-1} d_j$*.*

$$\begin{array}{c}
V(I) \subsetneq \mathbb{A}^n \\
\downarrow \\
V(I_1) \subsetneq \mathbb{A}^{n-1} \\
\downarrow \\
\vdots \\
V(I_{c-1}) \subsetneq \mathbb{A}^{n-c+1} \\
\downarrow \\
V(I_c) = \mathbb{A}^{n-c}
\end{array}$$

Remarks

1. If I has an infinite field of definition $L \subset K$, we can reach the assumption of the tower theorem by a triangular change of coordinates defined over L, i.e., with $a_{ij} \in L$:

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 1 & & & & \\ a_{21} & 1 & & 0 & \\ a_{31} & a_{32} & 1 & & \\ \vdots & & & \ddots & \\ a_{n1} & a_{n2} & \dots & & 1 \end{pmatrix} \begin{pmatrix} \tilde{x}_1 \\ \tilde{x}_2 \\ \tilde{x}_3 \\ \vdots \\ \tilde{x}_n \end{pmatrix}.$$

2. In the situation of the tower theorem it is tempting to define

$$\dim V(I) = n - c \text{ and } \operatorname{codim} V(I) = c$$

because the projetion $\pi_c \colon V(I) \to \mathbb{A}^{n-c}$ is surjective with finite fibers. A problem with this definition is that it is not clear that this is independent from the choice of coordinates.