Computer Algebra and Gröbner Bases

Frank-Olaf Schreyer

Saarland University WS 2020/21

Overview

Today's topics are

1. Linear projections
2. A dimension bound
3. The Veronese embeddings
4. The fundamental theorem of elimination

Morphism

We recall the definition of a morphism.

Definition. Let A be a quasi-projective algebraic set.

1. Let $B \subset \mathbb{A}^m$ be a quasi-affine algebraic set. A morphism $\varphi : A \to B$ is a map which is given by an m-tupel of regular functions $f_j \in \mathcal{O}(A)$:
$$\varphi(p) = (f_1(p), \ldots, f_m(p)) \; \forall p \in A.$$
2. Let $B \subset \mathbb{P}^m$ be a quasi-projective algebraic set. A map $\varphi : A \to B$ is a morphism if φ is locally given by regular functions, i.e., for each point $p \in A$ there exists an open neighbourhood $U \subset A$ and regular functions $f_0, \ldots, f_m \in \mathcal{O}(U)$ such that
$$\varphi(p) = [f_0(p) : \ldots : f_m(p)] \; \forall p \in U$$

Clearly, morphisms can be composed.

Definition. A morphism $\varphi : A \to B$ is an isomorphism if there exists a morphism $\psi : B \to A$ such that $\psi \circ \varphi = id_A$ and $\varphi \circ \psi = id_B$.

Linear projections

Let $A \subset \mathbb{P}^n$ be a projective variety. Let $\ell_0, \ldots, \ell_r \in K[x_0, \ldots, x_n]$ be $r+1$ linear independent linear forms such that $L = V(\ell_1, \ldots, \ell_r) \cong \mathbb{P}^{n-r-1}$ does not intersect A. Then

$$\pi_L : A \to \mathbb{P}^r, a \mapsto [\ell_0(a) : \ldots : \ell_r(a)]$$

is called the **linear projection from** L. The condition $A \cap L = \emptyset$ is equivalent to $\operatorname{rad}(\mathrm{I}(A) + (\ell_0, \ldots, \ell_r)) = (x_0, \ldots, x_n)$. If we choose coordinates on $\mathbb{P}^n$ such that $\ell_0 = x_{n-r}, \ldots, \ell_r = x_n$ then $A \cap L = \emptyset$ is equivalent to the condition that there are homogeneous equations $f_i \in \mathrm{I}(A)$ with

$$f_i \equiv x_i^{d_i} \mod (x_{n-r}, \ldots, x_n) \text{ for } i = 0, \ldots, n-r-1.$$

Thus in this case the map

$$\phi : K[x_{n-r}, \ldots, x_n] \to K[A] = K[x_0, \ldots, x_n]/\,\mathrm{I}(A)$$

induces an integral ring extension $K[A'] \hookrightarrow K[A]$ where $A' = V(\ker(\phi))$.

A dimension bound

Thus in this situation π_L induces a finite and surjective map $A \to A' \subset \mathbb{P}^r$. In particular, $\dim A' = \dim A \leq r$.

Corollary. *Let $A \subset \mathbb{P}^n$ be a projective algebraic set. If there exists a linear subspace $L \subset \mathbb{P}^n$ of dimension $n - r - 1$ with $A \cap L = \emptyset$, then* $\dim A \leq r$. $\square$

Definition. Let $A \subset \mathbb{P}^n$ be a projective algebraic set. We call a linear projection $\pi_L : A \to \mathbb{P}^r$ with $L \cap A = \emptyset$ with $r = \dim A$ a **linear Noether normalization**.

Corollary. *Let $A \subset \mathbb{P}^n$ be a projective algebraic set of dimension* $\dim A = r$. *Then every linear subspace L of dimension* $\dim L \geq n - r$ *intersects A.*

Proof. If $L \cap A = \emptyset$, then $\dim A < r$. $\square$

Theorem. *Let $X, Y \subset \mathbb{P}^n$ be projective algebraic sets. Then*

$$\dim X \cap Y \geq \dim X + \dim Y - n.$$

In particular the intersection of algebraic sets of complementary dimensions is always non-empty.

Proof of the dimension bound

Proof. Consider the projective space $\mathbb{P}^{2n+1}$ with coordinate ring $K[x_0, \ldots, x_n, y_0, \ldots, y_n]$ and the algebraic set $J(X, Y)$ defined by $\mathrm{I}(X) + \mathrm{I}(Y)$ where $\mathrm{I}(X) \subset K[x_0, \ldots, x_n]$ and $\mathrm{I}(Y) \subset K[y_0, \ldots, y_n]$ denote the homogeneous ideals in a disjoint sets of variables. The variety $J(X, Y)$ is called the **join** of X and Y because it is the union of all lines joining a point of X and with a point of Y,

$$X \subset \mathbb{P}^n \cong V(y_0, \ldots, y_n) \subset \mathbb{P}^{2n+1} \supset V(x_0, \ldots, x_n) \cong \mathbb{P}^n \supset Y.$$

Clearly,

$$\dim J(X, Y) = \dim X + \dim Y + 1$$

as one can see by combining linear Noether normalizations of X and Y. $X \cap Y = J(X, Y) \cap V(x_0 - y_0, \ldots, x_n - y_n)$ is the intersection of $J(X, Y)$ with a linear subspace of dimension n. Thus the intersection $X \cap Y \neq \emptyset$ if

$$n \geq 2n + 1 - (\dim X + \dim Y + 1) \Leftrightarrow \dim X + \dim Y - n \geq 0$$

by the second corollary.

Proof of the dimension bound continued

Suppose $\dim X \cap Y = e > 0$. Let $\ell_0, \ldots, \ell_e \subset K[x_0, \ldots, x_n]$ define a linear Noether normalization of $X \cap Y$. Then

$$J(X, Y) \cap L = \emptyset$$

where $L = V(x_0 - y_0, \ldots, x_n - y_n, \ell_0, \ldots, \ell_e)$ is a linear space of dimension $2n + 1 - (n + 1 + e + 1) = 2n + 1 - (n + 1 + e) - 1$ and

$$\dim J(X, Y) \leq n + 1 + e$$

holds by the first corollary. Thus

$$\dim X \cap Y = e \geq \dim J(X, Y) - n - 1 = \dim X + \dim Y - n.$$

$\square$

Remark. Using Krull's principal ideal theorem one can show for projective **varieties** $X, Y \subset \mathbb{P}^n$ that every component C of $X \cap Y$ has dimension $\dim C \geq \dim X + \dim Y - n$.

The Veronese embeddings

Definition. Let $n, d \geq 1$, $N = \binom{n+d}{n}$ and $m_0 = x_0^d, \dots, m_N = x_n^d$ be all degree d monomials in $K[x_0, \dots, x_n]$ in some order. The monomials define a morphism

$$\rho_{n,d} : \mathbb{P}^n \to \mathbb{P}^N$$

which turns out to be an embedding, i.e., an isomorphism to it's image $V_{n,d} \subset \mathbb{P}^N$. $\rho_{n,d}$ is called the **Veronese or d-uple embedding** of $\mathbb{P}^n$.

Example. In case of $n = 1$ the morphism $\rho_{1,d}$ embeds $\mathbb{P}^1 \hookrightarrow \mathbb{P}^d$ as the rational normal curve of degree d in $\mathbb{P}^d$ defined by the 2×2-minors of

$$\begin{pmatrix} x_0 & x_1 & \dots & x_{d-1} \\ x_1 & x_2 & \dots & x_d \end{pmatrix}.$$

Example. We discuss

$$\rho_{2,2} : \mathbb{P}^2 \to \mathbb{P}^5, [x : y : z] \mapsto [x^2 : xy : y^2 : xz : yz : z^2]$$

in some details. We use homogeneous coordinates $w_0, \dots, w_5$ on $\mathbb{P}^5$. Consider the symmetric matrix

$$\Delta = \begin{pmatrix} w_0 & w_1 & w_3 \\ w_1 & w_2 & w_4 \\ w_3 & w_4 & w_5 \end{pmatrix}$$

and let $V \subset \mathbb{P}^5$ be the algebraic set defined by the ideal I of 2×2-minors of Δ. Clearly, these minors vanish on all points of $\rho_{2,2}(\mathbb{P}^2)$. We show that $\rho_{2,2}$ induces an isomorphism of $\mathbb{P}^2$ with V by describing the inverse morphism ψ. $V \subset U_0 \cup U_2 \cup U_5$ because

$$w_1^2, w_3^2, w_4^2 \in I + (w_0, w_2, w_5).$$

On $V \cap U_0$ the inverse map is given by

$$p \mapsto [w_0(p) : w_1(p) : w_3(p)]$$

because $[x^2 : xy : xz] = [x : y : z]$ on $U_x = \{x \neq 0\} \subset \mathbb{P}^2$.

$V = V_{2,2}$ continued

Similarly, the inverse map ψ is given on $V \cap U_2$ and $V \cap U_5$ by the second respectively third row of Δ. The maps coincide on $V \cap U_i \cap U_j$ for $i, j \in \{0, 2, 5\}$ since the 2×2-minors of Δ vanish on V. Thus these pieces glue to a well-defined morphism $\psi : V \to \mathbb{P}^2$ and $\mathbb{P}^2 \cong V$.

Remark. Notice that ψ is a morphism which cannot be defined globally by only one tuple of three homogeneous polynomials of the same degree.

We finish the treatment of this example by proving

Claim. *I is the homogeneous ideal of V.*

Proof. Consider the ring homomorphism

$$\varphi : K[w_0, \dots, w_5] \to K[x, y, z], w_0 \mapsto x^2, w_1 \mapsto xy, \dots, w_5 \mapsto z^2.$$

Then $I \subset \ker(\varphi)$. To prove equality we consider a reverse lexicographic order with $w_0, \dots, w_5$ are ordered such that $w_1, w_3, w_4 > w_0, w_2, w_5$. Then

$$w_1^2, w_1 w_3, w_3^2, w_1 w_4, w_3 w_4, w_4^2$$

$V = V_{2,2}$ continued

Thus a remainder of a the division by the minors is at most linear in w_1, w_3 and w_4, and there are precisely

$$\binom{d+2}{2} + 3\binom{d+1}{2} = 2d^2 + 3d + 1 = \binom{2d+2}{2}$$

different monomials of degree d occuring as remainders. Since φ is surjective the homogeneous coordinate ring S_V has precisely that many elements in degree d. Thus $I = \ker(\varphi)$ and the minors form a Gröbner basis.The ideal I is prime because

$$S_V = K[w_0, \dots, w_5]/I \cong K[x^2, xy, y^2, xz, yz, xz] \subset K[x, y, z]$$

is isomorphic to a subring of a domain.
Finally we note that the Hilbert polynomial of V is

$$p_V(t) = \binom{2t+2}{2} = 4\frac{t^2}{2!} + 3t + 1, \text{ hence } \deg V = 4.$$

$\square$

$V_{n,d}$

Theorem. *The Veronese morphism*

$$\rho_{n,d} : \mathbb{P}^n \to \mathbb{P}^N, [x_0 : \ldots : x_n] \mapsto [x_0^d : x_0^{d-1}x_1 : \ldots : x_n^d]$$

where $N = \binom{n+d}{n} - 1$ *induces an isomorphism onto its image* $V_{n,d}$*, which is a subvariety of* $\mathbb{P}^N$ *of degree* $\deg V_{n,d} = d^n$*.*

Proof. The homogeneous coordinate ring of $\mathbb{P}^N$ has a variable y_α for each $\alpha \in \mathbb{N}^n$ with $|\alpha| = d$, and $\rho_{n,d}$ corresponds to the ring homomorphism

$$\varphi : K[y_\alpha' s] \to K[x_0, \ldots, x_n], y_\alpha \mapsto x^\alpha.$$

We will show that $V_{n,d}$ coincides with the a projective variety $V(\ker(\varphi)) \subset \mathbb{P}^N$.

Some equations in $I = \ker(\varphi)$ can be obtained as follows: Consider the $\binom{n+d-1}{n} \times (n+1)$-matrix Δ with rows corresponding to monomials of x^β of degree $d-1$ and columns corresponding to the variables $x_0, \ldots, x_n$ whose entries are $\Delta_{x^\beta, x_j} = y_\alpha$ where $x^\alpha = x^\beta x_j$. The 2×2-minors of Δ are contained in I.

$V_{n,d}$ continued

$V_{n,d}$ is contained in the union of $n+1$ standard charts of $\mathbb{P}^N$:
$V_{n,d} \cap V(y_{(d,0,\dots,0)}, \dots, y_{(0,\dots,0,d)}) = \emptyset$ because

$$y_\alpha^d - y_{(d,0,\dots,0)}^{\alpha_0} \cdot \dots \cdot y_{(0,\dots,0,d)}^{\alpha_n} \in I.$$

Thus

$$V_{n,d} \subset \widetilde{U}_0 \cup \dots \cup \widetilde{U}_n$$

for $\widetilde{U}_j = \{y_{(0,\dots,d,\dots 0)} \neq 0\}$ corresponding to the monomial x_j^d.
$\rho_{n,d}$ induces an isomorphism of U_0 with $V_{n,d} \cap \widetilde{U}_0$: The map

$$p \mapsto [y_{(d,0,\dots,0)}(p) : y_{(d-1,1,\dots,0)}(p) : \dots : y_{(d-1,0,\dots,1)}(p)]$$

corresponding to the row of $\Delta_{x_0^d}$ defines the inverse. Similarly

$$V_{n,d} \cap \widetilde{U}_j \cong U_j$$

by the map defined by the row $\Delta_{x_j^d}$.

$V_{n,d}$ continued

These maps glue to a well-defined inverse morphism

$$\psi : V_{n,d} \to \mathbb{P}^n$$

since the 2×2-minors of Δ vanish on $V_{n,d}$. To compute the degree we compute the Hilbert polynomial. Since $K[y_\alpha\,'s]/I \cong K[x^\alpha\,'s] \subset K[x_0, \ldots, x_n]$ we obtain

$$p_{V_{n,d}}(t) = \binom{dt+n}{n} = d^n \frac{t^n}{n!} + \text{ lower terms } .$$

$\square$

Corollary. *Every quasi-projective algebraic set has a finite open covering by affine algebraic sets.*

Proof of the corollary

Let

$$f = \sum_{\alpha} f_\alpha x^\alpha \in K[x_0, \ldots, x_n]$$

be a homogeneous polynomial of degree d. Consider the open set $U_f = \mathbb{P}^n \setminus V(f)$ and the corresponding hyperplane $H_f = V(\sum_\alpha f_\alpha y_\alpha) \subset \mathbb{P}^N$. Under the Veronese embedding U_f is isomorphic to the Zariski-closed subset of $\mathbb{A}^N$, since

$$U_f \cong V_{n,d} \cap (\mathbb{P}^N \setminus H_f) \subset \mathbb{P}^N \setminus H_f \cong \mathbb{A}^N.$$

Hence U_f is isomorphic to an affine variety.
Let $A = A_1 \setminus A_2$ be a quasi-projective set where $A_2 \subset A_1 \subset \mathbb{P}^n$ are projective algebraic subsets. If $A_2 = V(f_1, \ldots, f_r)$ then

$$A = \bigcup_{j=1}^{r} (A_1 \cap U_{f_j})$$

is an open covering. Since $A_1 \cap U_{f_j}$ is a closed subset of the affine variety U_f it is isomorphic to an affine algebraic set. $\square$

Morphism from projective algebraic sets

Theorem. *Let A be a projective algebraic set and $\varphi : A \to B$ a morphism to a quasi-projective algebraic set. Then $\varphi(A) \subset B$ is a Zariski-closed subset.*

Corollary. *Let A be a projective variety. Every regular function $f : A \to K$ is constant.*

Proof of the Corollary. f defines a morphism $f : A \to \mathbb{A}^1 \subset \mathbb{P}^1$. The image is closed in $\mathbb{P}^1$ hence different from $\mathbb{A}^1$. Since it is also closed in $\mathbb{A}^1$ it is a finite union of points. Since A is irreducible, it is a single point. $\square$

Remark. In case $K = \mathbb{C}$, this corollary is similar to the maximum principle: If f is a holomorphic function on a compact complex connected manifold A then $|f|$ attains its maximum, and hence f is constant.

Graph of a morphism

Lemma. *Let $\varphi : A \to B$ a morphism between quasi-projective algebraic sets. Then the graph of φ is a closed subset of $A \times B$.*

Proof. To be a closed subset is a local property. Hence we may replace B by an open affine subset U and A by an open affine subset of $\varphi^{-1}(U)$ since every quasi projective algebraic set has an open affine covering by the corollary to the Theorem on the Veronese embeddings. Thus we may assume the A and B are subsets of $\mathbb{A}^n$ and $\mathbb{A}^m$ respectively and that φ is given by a tuple of polynomial functions $(f_1, \dots, f_m)$. Then the graph of φ is defined by the ideal

$$(y_1 - f_1(x_1, \dots, x_n), \dots, y_m - f_m(x_1, \dots, x_n))$$

on $A \times B$. $\square$

The fundamental theorem of elimination

Passing to the graph reduces the proof of the theorem above to the following:

Theorem. *Let A be a projective algebraic set and B a quasi-projective algebraic set. Then the projection onto the second factor $A \times B \to B$ is a closed map, i.e., maps closed subsets of $A \times B$ to closed subsets of B.*

Proof. We may replace B by an open affine subset. Hence we may assume that $A \subset \mathbb{P}^n$ and $B \subset \mathbb{A}^m$ are closed subsets, and it suffices to prove that the projection $\mathbb{P}^n \times \mathbb{A}^m \to \mathbb{A}^m$ is closed. Any algebraic subset $X \subset \mathbb{P}^n \times \mathbb{A}^m$ is defined by finitely many polynomials $f_1, \dots, f_r \in K[x_0, \dots, x_n, y_1, \dots, y_m]$ where each f_i is homogeneous of some degree d_i in $x_0, \dots, x_n$. By the projective Nullstellenatz, a point $q \in \mathbb{A}^m$ lies in the image of X iff the ideal

$$I(q) := (f_1(\mathbf{x}, q), \dots, (f_r(\mathbf{x}, q)) \subset K[\mathbf{x}]$$

does not contain any of the ideals $(x_0, \dots, x_n)^d$ for $d \geq 1$.

Proof of the fundamental theorem of elimination

Define

$$Y_d = \{q \in \mathbb{A}^m \mid I(q) \not\supset (x_0, \ldots, x_n)^d\}.$$

Then the image of X is

$$Y = \bigcap_{d=1}^{\infty} Y_d$$

and it suffices to prove that each Y_d is an algebraic subset of $\mathbb{A}^m$. To obtain equations for Y_d we multiply each f_i with all monomials of degree $d - d_i$ in $\mathbf{x}$. Let T_d denote the resulting set of polynomials. Then $q \notin Y_d$ iff each monomial in $K[x_0, \ldots, x_n]_d$ of degree is a linear combination of the polynomials $f(\mathbf{x}, q)$ with $f \in T_d$. Comparing coefficients we obtain a $\binom{d+n}{n} \times \sum_{i=1}^{r} \binom{d-d_i+n}{n}$-matrix M_d with entries in $K[y_1, \ldots, y_m]$ such that $q \in Y_d$ iff $\operatorname{rank} M_d(q) < \binom{d+n}{n}$. Thus the $\binom{d+n}{n} \times \binom{d+n}{n}$-minors of M_d define Y_d. $\square$

Computing the elimination ideal in concrete examples

The proof of the theorem does not yield a practical algorithm to compute the image. Here is an approach which works frequently in practise.

Definition. Let I, J be ideals in a ring. Then the **saturation of I with respect to J** is

$$I : J^\infty = \bigcup_{N=1}^{\infty} (I : J^N).$$

To compute the saturation in noetherian rings one can iterate

$$I_{k+1} = I_k : J$$

starting with $I_0 = I$ until $I_{N+1} = I_N$. Then $I_N = I : J^\infty$.

In the situation of $X \subset \mathbb{P}^n \times \mathbb{A}^m$ defined by $f_1, \ldots, f_r$ as above, we obtain equations of the image $Y \subset \mathbb{A}^m$ by taking the elements of degree 0 in $\mathbf{x}$ of

$$(f_1, \ldots, f_r) : (x_0, \ldots, x_n)^\infty.$$