Computer Algebra and Gröbner Bases

Frank-Olaf Schreyer

Saarland University WS 2020/21

Overview

Today's topics are

1. Projective morphisms
2. Semi continuity of the fiber dimensions
3. The blow-up
4. Resolution of singularities
5. A birartional map between $\mathbb{P}^1 \times \mathbb{P}^1$ and $\mathbb{P}^2$

Projective morphism

Last time we proved that a morphism $\varphi : A \to B$ from a projective algebraic set to a quasi-projective algebraic set B is closed, i.e., maps Zariski-closed subsets of A to Zariski-closed subsets of B. Actually, we proved a stronger result.

Definition. A morphism $\varphi : A \to B$ is called a **projective morphism** if φ is the composition of a closed embedding $\iota : A \to \mathbb{P}^n \times B$ with the projection onto B. Here a morphism $\iota : A \to C$ is called a **closed embedding** if ι induces an isomorphism $A \to \iota(A)$ and $\iota(A)$ is a Zariski-closed subset of C.

Theorem. *A projective morphism is a closed map.*

Proof. Indeed in the proof of the fundamental theorem of elimination we replaced $A \subset \mathbb{P}^n$ with the graph of φ in $A \times B \subset \mathbb{P}^n \times B$. The map $\iota : A \to \mathbb{P}^n \times B$ to the graph of φ in $\mathbb{P}^n \times B$ is a closed embedding.

Projective morphisms are closed

In the remaining part of the proof all we used was that $A \cong \iota(A) \subset \mathbb{P}^n \times B$ is closed. Thus closed subsets of $X \subset A$ are also closed subsets of $\mathbb{P}^n \times B$ and out argument showed that the image Y of X under the projection to B is closed in B. $\square$

Definition. Let $\varphi : X \to Y$ be a morphism. The **fiber** of φ over a point $q \in Y$ is $X_q := \varphi^{-1}(q) \subset X$. Since morphisms are continues in the Zariski topology, the preimage of the point p is a Zariski closed subset of X.

If φ is a projective morphism, say φ factors over a closed embedding $\iota : X \to \mathbb{P}^n \times Y$, then the situation is better: The fiber

$$X_p \subset \mathbb{P}^n \times \{p\} \cong \mathbb{P}^n$$

is a projective algebraic set.

Semi continuity of the fiber dimension

Theorem. *Let $\varphi : X \to Y$ be a projective morphism and $r \geq -1$ an integer. Then the set*

$$U_r = \{q \in Y \mid \dim X_q \leq r\}$$

is Zarsiki-open in Y.

Proof. The set

$$U_{-1} = \{q \in Y \mid \dim X_q \leq -1\} = \{q \in Y \mid X_q = \emptyset\}$$

is open in Y because it is the complement of the closed subset $\varphi(X) \subset Y$.

Suppose $\dim X_q = r \geq 0$. We assume that φ factors over $\mathbb{P}^n \times Y$. Consider a linear space $L \subset \mathbb{P}^n$ of dimension $n - r - 1$ with $X_q \cap L = \emptyset$ and

$$Z = X \cap (L \times Y) \subset \mathbb{P}^n \times Y.$$

Fibers X_q with $\dim X_q > r$ intersect Z. Thus $U = Y \setminus \varphi(Z)$ is an open neighbourhood of $p \in U_r$. $\square$

Dimension of general fibers

In case of a surjective projective morphism between varieties the result can be strengthed.

Theorem. *Let $\varphi : X \to Y$ be a surjective projective morphism between varieties. Then*

$$\dim X_q \geq \dim X - \dim Y,$$

and equality holds for $q \in U$ of a non-empty open subset U of Y.

Proof. We may assume that Y is affine and that $X \subset \mathbb{P}^n \times Y$ is a closed subset. Consider the function fields

$$K(Y) \subset K(X)$$

We have

$$\operatorname{trdeg}_K K(X) = \operatorname{trdeg}_{K(Y)} K(X) + \operatorname{trdeg}_K K(Y).$$

Let $I \subset K[Y][x_0, \ldots, x_n]$ be the ideal of $X \subset \mathbb{P}^n \times Y$. Consider the ideal $J \subset K(Y)[x_0, \ldots, x_n]$ generated by I. J corresponds to a variety $V(J)$ defined over the function $K(Y)$ of dimension

$$\dim V(J) = \operatorname{trdeg}_{K(Y)} K(X) = \dim X - \dim Y.$$

The proof continued

We compute a normalized Gröbner basis of J, i.e., one where the leading coefficients of all Gröbner basis elements are 1. In doing so we have to divide by finitely many polynomial functions of $K[Y]$. Let $f \in K[Y]$ be the product of these polynomials and $U_f = Y \setminus V(f)$ the corresponding non-empty open subset. We claim that for a point $q \in U_f$ the ideal

$$I_q = (\{f(x,q) | f \in I\}) \subset K[x_0, \ldots, x_n]$$

Indeed the computation of the Gröbner basis of I_q follows the same steps as the computation for $J = (I)$. We simply have to substitute q in to the rational functions in $K(Y)$ which are the coefficients. Since each coefficient has a representation as a fraction with power of f in the denominator the coefficients can be evaluated in q. Thus J and I_q have the same lead ideal.

The proof continued

Hence $K(Y)[x_0, \dots, x_n]/J$ and $K[x_0, \dots, x_n]/I_q$ have the the same Hilbert polynomial. In particular

$$\dim X_q = \dim V(J) = \operatorname{trdeg}_{K(Y)} K(X) = \dim X - \dim Y$$

holds for all $q \in Y$. Since Y is irreducible hence U_f dense Y we obtain

$$\dim X_q \geq \dim X - \dim Y$$

from the semi continuity of the fiber dimension. □

As a corollary of the proof we note

Corollary. *Let Y be an affine variety and $I \subset K[Y][x_0, \dots, x_n]$ be an ideal which is homogeneous in $x_0, \dots, x_n$. Then there exist a non-empty open subset $U \subset Y$ such that the ideals*

$$I_q = (\{f(x,q) \mid f \in I\}) \subset K[x_0, \dots, x_n]$$

have the same Hilbert function for all $q \in U$. □

Gröbner basis over prime fields

Theorem. *Let* $f_1, \dots, f_r \in \mathbb{Z}[x_0, \dots, x_n]$ *be homogeneous polynomials and let* $I_{\mathbb{Q}} \subset \mathbb{Q}[x_0, \dots, x_n]$ *and* $I_p \subset \mathbb{F}_p[x_0, \dots, x_n]$ *for* p *a prime number denote the ideals generated by* $f_1, \dots, f_r$*. Then for all but finitely many primes the lead ideal*

$$\mathrm{Lt}(I_p) \text{ and } \mathrm{Lt}(I_{\mathbb{Q}})$$

are generated by the same monomials. In particular their Hilbert polynomials coincide.

Proof. We computed a normalized Gröbner basis of $I_{\mathbb{Q}}$. In this process we have to devide by finitely many leading coefficients, and the Gröbener basis of the ideal I_p where p does not divide any of the leading coefficients, is obtained by mapping the coefficients $\frac{a}{b} \in \mathbb{Q}$ to $ab^{-1} \in \mathbb{F}_p$. □

Gröbner basis over prime fields

Remark. Notice that a Gröbner basis over $\mathbb{Q}$ can have very large coefficients: In adding or multiplying two rational numbers

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \text{ or } \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

one often obtains numbers with twice the number of digits in the numerator and denominator.

By passing to a finite prime field this effect is avoided. If we are only interested say in the degree and the dimension of the $V(I_{\mathbb{Q}})$, then the result does not change for almost all primes. This is frequently used in experiments in algebraic geometry.

The blow-up

Definition. Let $X \subset \mathbb{P}^1 \times \mathbb{A}^2$ be defined by

$$\det \begin{pmatrix} z_0 & z_1 \\ x & y \end{pmatrix} \in K[z_0, z_1, x, y]$$

and let $\sigma : X \to \mathbb{A}^2$ denote the projection onto the second component. σ is called the **blow-up** of $\mathbb{A}^2$ at the origin o.
X is covered by two affine charts $U_j = X \cap (U_{z_j} \times \mathbb{A}^2)$ which are both isomorphic to $\mathbb{A}^2$.

$$K[U_0] \cong K[z, x, y]/(y - xz) \cong K[x, z]$$

and the map $\sigma|_{U_0} : U_0 \to \mathbb{A}^2$ is given by $(x, z) \mapsto (x, xz)$. Similary

$$K[U_1] \cong K[w, y] \text{ and } \sigma|_{U_1} : U_1 \to \mathbb{A}^2, (w, y) \mapsto (wy, y).$$

The fiber of σ over $o = (0, 0) \in \mathbb{A}^2$ is $E = \mathbb{P}^1 \times \{o\} \cong \mathbb{P}^1$. E is called the **exceptional curve of** σ. Outside E the map σ restricts to an isomorphism $X \setminus E \cong \mathbb{A}^2 \setminus \{o\}$.

Strict and total transform

$X \setminus E \subset \mathbb{P}^1 \times \mathbb{A}^2 \setminus \{o\}$ is isomorphic to the graph of the morphism

$$\mathbb{A}^2 \setminus \{o\}, (x, y) \mapsto [x : y].$$

In other words we may think of

$$X = V(\det \begin{pmatrix} z_0 & z_1 \\ x & y \end{pmatrix}) \subset \mathbb{P}^1 \times \mathbb{A}^2$$

as obtained from $\mathbb{A}^2$ by replacing the origin o by the projective space $E \cong \mathbb{P}^1$ of lines through o.

Definition. Let $C \subset \mathbb{A}^2$ be a plane curve. Then the closure $C' = \overline{\sigma^{-1}(C \setminus \{o\})} \subset X$ is called the **strict transform** of C. The **total transform** is $\sigma^{-1}(C)$.

Proposition. *Let $C = V(f)$ be a curve of multiplicity m at the origin. Then the strict transform $C' \subset X$ intersects E in precisely m points counted with multiplicities.*

Proof of the proposition

Suppose $f = f_m + \ldots + f_d \in K[x, y]$ with f_j homogeneous of degree j. The total transform of C in the chart U_0 is defined

$$f(x, xz) = x^m(f_m(1, z) + xf_{m+1}(1, z) + \ldots + x^{d-m}f_d(1, z)) = 0.$$

The exceptional curve is E is defined by $x = 0$ on U_0. So the strict transform C' is defined by

$$f_m(1, z) + xf_{m+1}(1, z) + \ldots + x^{d-m}f_d(1, z) = 0.$$

Thus the intersection point of $E \cap C'$ contained in U_0 are defined by $V(f_m(1, z), x)$. Let $f_m = \prod_{i=1}^r \ell_i^{e_i}$ be the factorization of f_m into distinct linear factors. The intersection multiplicity

$$i(C', E; p_i) = e_i$$

at the point $p_i = [a_i : b_i] \in \mathbb{P}^1 = E$ corresponding to the tangent line $V(\ell_i)$ with $\ell_i = b_i x - a_i y$ since the factors ℓ_j for $j \neq i$ are units in $\mathcal{O}_{X,p_i}$. The result follows because $\sum_{i=1}^r e_i = m$. □

The effect of the blow-up on curves

Corollary. *If o is an ordinary m-fold point, then E and C' have transversal intersections and C' is non-singular at the intersection points.* □

Since X is covered by charts isomorphic to $\mathbb{A}^2$ we can iterate this process.

Example. Consider $C = V(y^3 - x^5)$ the strict transform of C is contained in the chart U_0 where total transform is defined by $x^3(z^3 - x^2)$.

The further blow-up $(x, z) = (uz, u)$ yields $u^5z^3(u - z^2)$.
Blowing-up the intersection point of the second exceptional curve $E_2 = \{u_2 = 0\}$ with C'' via $(u, z) = (wz, z)$ yields the local equation $w^5z^9(w - z)$, and all curves intersect transversal.

Resolution of singularities

Theorem. *Let $C \subset \mathbb{P}^2$ be a plane algebraic curve. Then there exists a sequence*

$$X_r \xrightarrow{\sigma_r} X_{r-1} \longrightarrow \dots \longrightarrow X_1 \xrightarrow{\sigma_1} \mathbb{P}^2$$

of blow-ups, such that the strict transform $C^{(r)}$ of C in X_r is a non-singular curve.

The main difficulty in proving this theorem is to prove that some numerical invariant improves along the process of blow-ups. In the example above such invariant was the multiplicity of the singular points. However in general a more subtle invariant is needed.

Resolution of singularities

Theorem. *Let $C \subset \mathbb{P}^2$ be a plane algebraic curve. Then there exists a sequence*

$$X_r \xrightarrow{\sigma_r} X_{r-1} \longrightarrow \dots \longrightarrow X_1 \xrightarrow{\sigma_1} \mathbb{P}^2$$

of blow-ups, such that the strict transform $C^{(r)}$ of C in X_r is a non-singular curve.

Example. Consider $y^2 - x^4 + x^6 = 0$. Substituting $(x, y) = (x, xz)$ leads to the strict transform $z^2 - x^2 + x^4 = 0$, which still has a double point at the origin. A second blow $(x, z) = (uz, z)$ gives the strict transform $u^2 - 1 + u^4 z^2 = 0$ which actually is now a smooth curve.

Birational maps between smooth surfaces

A second place where the blow-up plays a crucial role is in the description of birational maps between smooth surfaces.

Theorem(Castelnuovo)

1. *Let $\varphi : Z \to X$ be a birational morphism between smooth projective surfaces. Then there exist a sequence of blow-ups*

$$X_r \xrightarrow{\sigma_r} X_{r-1} \longrightarrow \dots \longrightarrow X_1 \xrightarrow{\sigma_1} X$$

   such that $Z \cong X^{(r)}$

2. *Every birational map $Y \dashrightarrow X$ between smooth projective surfaces can be factored into birational morphisms from a smooth projective surface Z as follows:*

$$\begin{array}{ccc} & Z & \\ \swarrow & & \searrow \\ Y & & X \end{array} .$$

   where both morphisms are sequences of blow-ups.

The birational projection of $\mathbb{P}^1 \times \mathbb{P}^1 \dashrightarrow \mathbb{P}^2$

Consider a point $p = (a, b) \in \mathbb{P}^1 \times \mathbb{P}^1 \subset \mathbb{P}^3$ and the rational map

$$\pi_p : \mathbb{P}^1 \times \mathbb{P}^1 \dashrightarrow \mathbb{P}^2$$

which maps a point $q \in \mathbb{P}^1 \times \mathbb{P}^1$ to the line $\overline{pq} \in \mathbb{P}^2$ where we identify $\mathbb{P}^2$ with the set of lines in $\mathbb{P}^3$ through p. Its factorization is

$$\begin{array}{ccc} & Z & \\ \swarrow & & \searrow \\ \mathbb{P}^1 \times \mathbb{P}^1 & & \mathbb{P}^2. \end{array}$$

where $Z \to \mathbb{P}^1 \times \mathbb{P}^1$ is the blow-up of $\mathbb{P}^1 \times \mathbb{P}^1$ in p and $Z \to \mathbb{P}^2$ collaps the strict transforms of the lines $\mathbb{P}^1 \times \{b\}$ and $\{a\} \times \mathbb{P}^1$ to two points $p_1, p_2 \in \mathbb{P}^2$. The exceptional curve E over p is mapped to the line $\overline{p_1 p_2}$.

Projection of $\mathbb{P}^1 \times \mathbb{P}^1 \dashrightarrow \mathbb{P}^2$

$$\begin{aligned}
\mathbb{P}^2 \setminus \overline{p_1 p_2} &= \mathbb{A}^2 = \mathbb{A}^1 \times \mathbb{A}^1 \\
&\cong (\mathbb{P}^1 \setminus \{a\}) \times (\mathbb{P}^1 \setminus \{b\}) \\
&= \mathbb{P}^1 \times \mathbb{P}^1 \setminus (\{a\} \times \mathbb{P}^1 \cup \mathbb{P}^1 \times \{b\})
\end{aligned}$$