Computer Algebra and Gröbner Bases

Frank-Olaf Schreyer

Saarland University WS 2020/21

Overview

Today we have two quite independent topics: Mora division and products of projective spaces

1. Mora division
2. Products of projective spaces
3. Morphism

Mora's division theorem

Theorem. *Let $>$ be a local monomial order and let $f_1, \ldots, f_r \in K[x_1, \ldots, x_n]$. For every further element $g \in K[x_1, \ldots, x_n]$ there exists an element $u \in K[x_1, \ldots, x_n]$ with $u(0) = 1$, elements $g_1, \ldots, g_r \in K[x_1, \ldots, x_n]$ and a remainder $h \in K[x_1, \ldots, x_n]$ such that following holds:*

1) $ug = g_1 f_1 + \ldots + g_r f_r + h$.

2a) $\mathrm{Lt}(g) \geq \mathrm{Lt}(g_i f_i)$ *whenever both sides are non-zero.*

2b) *If $h \neq 0$, then $\mathrm{Lt}(h)$ is not divisible by any $\mathrm{Lt}(f_i)$.*

Mora's algorithm

Definition. Let $>$ be a monomial order. The **ecart** of a non-zero element $f \in K[x_1, \ldots, x_n]$ is

$$\operatorname{ecart}(f) = \deg f - \deg \operatorname{Lt}(f).$$

Algorithm.

Input. A local monomial order $>$, polynomials $f_1, \ldots, f_r$ and g

Output. A remainder h of a Mora division of g by $f_1, \ldots, f_r$.

1. Set $h := g$ and $D := \{f_1, \ldots, f_r\}$.
2. **while** ($h \neq 0$ **and** $D(h) := \{f \in D \mid \operatorname{Lt}(f) \text{ divides } \operatorname{Lt}(h)\} \neq \emptyset$) **do**
   - Choose $f \in D(h)$ with $\operatorname{ecart}(f)$ minimal.
   - **if** $\operatorname{ecart}(f) > \operatorname{ecart}(h)$, **then** $D := D \cup \{f\}$.
   - $h := h - \frac{\operatorname{Lt}(h)}{\operatorname{Lt}(f)} f$.
3. return h.

Termination of Mora's algorithm

We write h_k and D_k for the value of h and D after k iterations of the while loop. Let x_0 be a further variable. After k iteration while loop continues iff $\mathrm{Lt}(h_k) \in (\{\mathrm{Lt}(f) \mid f \in D_k\} \subset K[x_1, \ldots, x_n]$ and h_k is added to D_k iff

$$x_0^{\mathrm{ecart}(h_k)}\,\mathrm{Lt}(h_k) \notin I_k := (\{x_0^{\mathrm{ecart}(f)}\,\mathrm{Lt}(f) \mid f \in D_k\}) \subset K[x_0, x_1, \ldots, x_n].$$

Since the chain of monomial ideals

$$I_0 \subset I_1 \subset \ldots \subset I_k \subset \ldots \subset K[x_0, \ldots, x_n]$$

becomes stationary there exists an N such that

$$D_N = D_{N+1} = D_{N+2} = \ldots$$

no longer increases.

After this point we homogenize h_N and the elements of D_N with x_0.

Termination of Mora's algorithm continued

$$f^h = x_0^{\deg f} f(x_1/x_0, \ldots, x_n/x_0).$$

has lead term $\mathrm{Lt}(f^h) = x_0^{\mathrm{ecart}(f)} \mathrm{Lt}(f)$ with respect to the monomial order $>_g$ on $K[x_0, \ldots, x_n]$ defined by

$$x_0^a x^\alpha >_g x_0^b x^\beta \Leftrightarrow \deg x_0^a x^\alpha > \deg x_0^b x^\beta \text{ or}$$
$$\deg x_0^a x^\alpha = \deg x_0^b x^\beta \text{ and } x^\alpha > x^\beta.$$

Since D_N does not change after this point we get a sequence

$$(h_k^h)_{k \geq N}$$

of homogeneous elements of the same degree with lead terms

$$\mathrm{Lt}(h_N^h) = x_0^{\mathrm{ecart}(h_N)} \mathrm{Lt}(h_N) >_g \mathrm{Lt}(h_{N+1}^h) >_g \ldots.$$

After finitely many further steps the algorithm stops with an $h_M = 0$ or an h_M with $\mathrm{Lt}(h_M) \notin (\{\mathrm{Lt}(f) \mid f \in D_N\})$, since there are only finitely many monomials in $K[x_0, \ldots, x_n]$ of the same degree.

Correctness of the output.

Recursively, starting with $u_0 = 1$, $g_i^{(0)} = 0$ and $h_0 = g$ suppose that we already have expressions

$$u_\ell g = g_1^{(\ell)} f_1 + \ldots + g_r^{(\ell)} f_r + h_\ell \quad \text{with } u_\ell(0) = 1$$

for $\ell = 0, \ldots, k-1$. Then, if the test condition for the k-th iteration of the while loop is fulfilled, choose a polynomial $f = f^{(k)}$ as in the algorithm and set

$$h_k = h_{k-1} - m_k f^{(k)} \text{ where } m_k = \frac{\mathrm{Lt}(h_{k-1})}{\mathrm{Lt}(f^{(k)})}.$$

There are two possibilities

(a) $f^{(k)}$ is one of $f_1, \ldots, f_r$ or

(b) $f^{(k)}$ is one of $h_1, \ldots, h_{k-1}$.

Thus substituting $h_{k-1} = h_k + m_k f^{(k)}$ into the expression for $u_{k-1} g$ we obtain the desired expression for $u_k g$ with

(a) $u_k = u_{k-1}$ and $g_j^{(k)} = g_j^{(k-1)} + m_k$ if $f^{(k)} = f_j$ or

(b) $u_k = u_{k-1} + m_k u_\ell$ for some ℓ and $g_j^{(k)} = g_j^{(k-1)} + m_k g_j^{(\ell)}$ $\forall j$

Correctness of the output continued

In both cases we have $u_k(0) = u_{k-1}(0) = 1$. In case (b) this follows from

$$\mathrm{Lt}(h_\ell) > \mathrm{Lt}(h_k) = \mathrm{Lt}(m_k h_\ell) = m_k \,\mathrm{Lt}(h_\ell).$$

Hence $1 > m_k$ and $u_k(0) = u_{k-1}(0) + 0u_\ell(0) = 1$.

The final expression satisfies condition 2a) because the lead terms of the h_k decrease in each round of the while loop. Finally, condition 2b) is satisfied due to the stopping condition of the while loop. □

Example. Consider $g = x$ and $f_1 = x - x^2$ in $K[x]$ the Mora algorithm proceeds as follows:

$$h_0 = x, D_0 = \{x - x^2\}, 1 \cdot g = 0 \cdot f_1 + x,$$
$$f^{(1)} = x - x^2, m_1 = 1, D_1 = \{x - x^2, x\}, 1 \cdot g = 1 \cdot f_1 + x^2,$$
$$f^{(2)} = x, m_2 = x, D_2 = D_1, (1 - x) \cdot g = 1 \cdot f_1 + 0.$$

Products of algebraic sets

For two affine algebraic sets $A \subset \mathbb{A}^n$ and $B \subset \mathbb{A}^m$ the product

$$A \times B \subset \mathbb{A}^n \times \mathbb{A}^m = \mathbb{A}^{n+m}$$

is simply the algebraic set defined by

$$(\mathrm{I}(A) \cup \mathrm{I}(B)) \subset K[x_1, \ldots x_n, y_1, \ldots y_m]$$

where $\mathrm{I}(A) \subset K[x_1, \ldots, x_n]$ and $\mathrm{I}(B) \subset K[y_1, \ldots, y_m]$ are the vanishing ideals of A and B respectively.

For projective algebraic sets the definition of a product is not so clear. To start with, it is not a priori clear how to give $\mathbb{P}^n \times \mathbb{P}^m$ the structure of an algebraic set. One uses the **Segre embedding**.

Segre embedding 1

Define

$$\sigma_{n,m} : \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^N \text{ with } N = (n+1)(m+1) - 1$$

by

$$([a_0 : \ldots : a_m], [b_0 : \ldots : b_n]) \mapsto [a_0 b_0 : \ldots : a_i b_j : \ldots : a_m b_n].$$

This is a well-defined map. For any pair of points at least one component $a_i b_j \neq 0$.
We will use variables $\mathbf{x} = x_0, \ldots, x_n$, $\mathbf{y} = y_0, \ldots, y_m$ and $\mathbf{z} = z_{00}, \ldots, z_{0m}, z_{10}, \ldots, z_{nm}$ for the homogeneous coordinate rings of $\mathbb{P}^n, \mathbb{P}^m$ and $\mathbb{P}^N$. Moreover we call a polynomial

$$f = \sum_{|\alpha|=d, |\beta|=e} f_{\alpha,\beta} x^\alpha y^\beta \in K[\mathbf{x}, \mathbf{y}]$$

bihomogeneous (in x and y) of bidegree (d, e)**.**

Segre embedding 2

Proposition. *Let $\Sigma_{n,m} \subset \mathbb{P}^N$ be the projective algebraic set defined by the 2×2-minors of the $(n+1) \times (m+1)$-matrix (z_{ij}). Then*

$$\sigma_{n,m} : \mathbb{P}^n \times \mathbb{P}^m \to \Sigma_{m,n}$$

is a bijection which induces isomorphisms $U_i \times U_j \cong \Sigma_{n,m} \cap U_{ij}$ on the standard charts. Moreover $\Sigma_{n,m} \subset \mathbb{P}^N$ is irreducible and the ideal of 2×2-minors coincides with the homogeneous ideal of $\Sigma_{m,m}$.

Proof. The minor

$$\det \begin{pmatrix} z_{i_1 j_1} & z_{i_1 j_2} \\ z_{i_2 j_1} & z_{i_2 j_2} \end{pmatrix}$$

vanishes on the image of $\sigma_{n,m}$ because

$$\det \begin{pmatrix} x_{i_1} y_{j_1} & x_{i_1} y_{j_2} \\ x_{i_2} y_{j_1} & x_{i_2} y_{j_2} \end{pmatrix} = 0.$$

Thus the image of $\sigma_{m,n}$ is contained in $\Sigma_{m,n}$.

Segre embedding 3

The points $r = [1 : c_{01} : \ldots : c_{nm}] \in \Sigma_{n,m} \cap U_{00}$ satisfies

$$c_{ij} = c_{i0}c_{0j}.$$

Thus the pair of points

$$(p, q) = ([1 : c_{10} : \ldots, c_{n0}], [1 : c_{01} : \ldots : c_{0m}]) \in U_0 \times U_0 \subset \mathbb{P}^n \times \mathbb{P}^m$$

is the unique preimage point of r and $\Sigma_{n,m} \cap U_{00} \cong U_0 \times U_0$. The same argument in other charts gives that $\sigma_{n,m} : \mathbb{P}^n \times \mathbb{P}^m \to \Sigma_{n,m}$ is bijective and gives isomorphisms $\Sigma_{n,m} \cap U_{ij} \cong U_i \times U_j$.

To prove that $\Sigma_{m,n}$ is irreducible and that the ideal J of 2×2-minors of (z_{ij}) is its homogeneous ideal, it suffices to prove that J is a prime ideal.

Segre embedding 4

Consider the ring homorphism

$$\varphi : K[\mathbf{z}] \to K[\mathbf{x}, \mathbf{y}], z_{ij} \mapsto x_i y_j$$

Clearly, $J \subset \ker \varphi$. To prove equality we consider a reverse lexicographic order $>_{\mathrm{rlex}}$ which refines the following order on the variables

$$\begin{array}{ccccccc}
z_{00} & > & z_{01} & > & \dots & > & z_{0m} \\
\vee & & \vee & & & & \vee \\
z_{10} & > & z_{11} & > & \dots & > & z_{1m} \\
\vee & & \vee & & & & \vee \\
\vdots & & \vdots & & & & \vdots \\
\vee & & \vee & & & & \vee \\
z_{n0} & > & z_{n1} & > & \dots & > & z_{nm}
\end{array}$$

We have

$$\mathrm{Lt}(\det \begin{pmatrix} z_{i_1 j_1} & z_{i_1 j_2} \\ z_{i_2 j_1} & z_{i_2 j_2} \end{pmatrix}) = -z_{i_2 j_1} z_{i_1 j_2}$$

whenever $i_1 < i_2$ and $j_1 < j_2$.

Segre embedding 5

Thus the remainder of a monomial in $K[\mathbf{z}]$ divided by the 2×2-minors has the form

$$z_{i_1 j_1} z_{i_2 j_2} \cdots z_{i_d j_d} \text{ with } i_1 \leq i_2 \leq \ldots \leq i_d \text{ and } j_1 \leq j_2 \leq \ldots \leq j_d.$$

Since φ induces a bijection between such monomials and bihomogeneous monomials of bidegree (d, d) we conclude that the 2×2-minors form a Gröbner basis of $\ker \varphi$. In particular $J = \ker \varphi$ and this is a prime ideal because $K[\mathbf{z}]/\ker \varphi$ is isomorphic to a subring of the domain $K[\mathbf{x}, \mathbf{y}]$. □

Definition. We give $\mathbb{P}^n \times \mathbb{P}^m$ the structure of a projective variety by identifying $\mathbb{P}^n \times \mathbb{P}^m$ and $\Sigma_{n,m}$.

Example. We identify $\mathbb{P}^1 \times \mathbb{P}^1$ with the quadric

$$\Sigma_{1,1} = V(z_{00} z_{11} - z_{10} z_{01}) \subset \mathbb{P}^3.$$

Hypersurface in $\mathbb{P}^n \times \mathbb{P}^m$ of bidegree (d, e).

Notice that the Zariski topology on $\mathbb{P}^n \times \mathbb{P}^m$ is finer than product of the Zariski topologies of the factors. For example if

$$f = \sum_{|\alpha|=d, |\beta|=e} f_{\alpha,\beta} x^\alpha y^\beta \in K[\mathbf{x}, \mathbf{y}]$$

is a bihomogeneous polynomial of bidegree (d, e), then

$$V(f) = \{(a, b) \in \mathbb{P}^n \times \mathbb{P}^m \mid f(a, b) = 0\}$$

is an Zariski closed subset, which for general f is not closed in the product topology. To see that $V(f)$ is an algebraic subset of $\mathbb{P}^n \times \mathbb{P}^m$ we argue as follows: Suppose $d \geq e$. Then multiplying f with monomials $y^\beta \in K[\mathbf{y}]$ of degree $d - e$ we get $\binom{d-e+m}{m}$ polynomials fy^β of bidegree (d, d), each of which is the image of a polynomial in $F_\beta \in K[\mathbf{z}]$ of degree d. $V(f)$ coincides with the zero-loci of $(\{F_\beta \mid \ |\beta| = d - e\}) + \ker \varphi$.

$V(f)$ is called a **hypersurface of bidegree** (d, e) in $\mathbb{P}^n \times \mathbb{P}^m$.

Algebraic subsets of $\mathbb{P}^n \times \mathbb{P}^m$

Definition. Let $A \subset \mathbb{P}^n \times \mathbb{P}^m$ be a subset. The **bihomogeneous vanishing ideal** of A is

$$\mathrm{I}(A) = (\{f \in K[\mathbf{x}, \mathbf{y}] \text{ bihomogeneous} \mid f(a, b) = 0 \ \forall (a, b) \in A\})$$

and $V(\mathrm{I}(A)) = \overline{A}$ is its Zariski closure. For an algebraic subset $A \subset \mathbb{P}^n \times \mathbb{P}^m$ the bigraded ring $K[\mathbf{x}, \mathbf{y}]/\mathrm{I}(A)$ is called the **bihomogeneous coordinate ring** of A.

Remark. For $J \subset K[\mathbf{x}, \mathbf{y}]$ a bihomogenous ideal we have

$$\mathrm{I}(V(J)) = ((\mathrm{rad}(J) : (x_0, \ldots, x_n)) : (y_0, \ldots, y_m). \quad \square$$

We now are ready to define the product of two arbitrary projective algebraic sets $A \subset \mathbb{P}^n$ and $B \subset \mathbb{P}^m$:

$$A \times B \subset \mathbb{P}^n \times \mathbb{P}^m \subset \mathbb{P}^N$$

is the algebraic set defined by the bihomgeneous polynomials $f_i \in \mathrm{I}(A) \subset K[\mathbf{x}]$ of bidegree $(d_i, 0)$ and $g_j \in \mathrm{I}(B) \subset K[\mathbf{y}]$ of bidegree $(0, e_j)$.

Quasi-projective algebraic sets and regular functions

Definition. A **quasi-affine algebraic set** is an open subset of an affine algebraic set. Similarly we have the notion of a **quasi-projective algebraic set**. Every quasi-affine algebraic set is also quasi-projective because $\mathbb{A}^n = \mathbb{P}^n \setminus V(x_0)$.

The product of two quasi-affine (quasi-projective) algebraic sets $A = A_1 \setminus A_2$ and $B = B_1 \setminus B_2$ is again quasi-affine (quasi-projective).

$$A \times B = A_1 \times B_1 \setminus (A_2 \times B_1 \cup A_1 \times B_2).$$

For $A \subset \mathbb{P}^n$ a quasi-projective algebraic set we define the **ring of regular functions** $\mathcal{O}(A)$ as the ring of functions

$$f : A \to K$$

such that for every point $p \in A$ there exist an open neighbourhood $U \subset A$ and homogeneous polynomials $g, h \in K[x_0, \ldots, x_n]$ of the same degree with $h(p) \neq 0$ for all $p \in U$ such that

$$f(p) = \frac{g(p)}{h(p)}.$$

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 neighbarhood $U \subset A$ and regular functions $f_0, \ldots, f_m \in \mathcal{O}(U)$ such that

$$\varphi(p) = [f_0(p) : \ldots : f_m(p)] \; \forall p \in U$$

Examples

1. Let $A \subset \mathbb{P}^n$ be a quasi-projective algebraic set, and let $f_0, \ldots, f_m \in K[x_0, \ldots, x_n]$ be homogeneous polynomials of the same degree d such that $V(f_0, \ldots, f_m) \cap A = \emptyset$. Then

$$\varphi : A \to \mathbb{P}^m, p \mapsto [f_0(p) : \ldots : f_m(p)]$$

is a well-defined morphism. Indeed on the open set $U = A \cap (\mathbb{P}^n \setminus V(f_i))$ the map φ is given by the regular functions

$$[\frac{f_0}{f_i} : \ldots : \frac{f_m}{f_i}]$$

and these open sets cover A since $V(f_0, \ldots, f_m) \cap A = \emptyset$.

In particular we see that the regular functions in $\mathcal{O}(U)$ which define φ on U might not exist globally.

2. More specifically, consider the morphism $\rho_d : \mathbb{P}^1 \to \mathbb{P}^d$ defined by

$$[t_0 : t_1] \mapsto [t_0^d : t_0^{d-1} t_1 : \ldots : t_1^d]$$

Examples

The image of ρ_d is the so-called **rational normal curve of degree** d. It has the homogeneous ideal generated by the 2×2-minors of the $2 \times d$-matrix

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

Remark. Morphisms $\varphi : A \to B$ between affine algebraic sets are easier to describe because they simply correspond to K-algebra homomorphisms $\varphi^* : K[B] \to K[A]$.
Morphism $\varphi : A \to B$ between projective algebraic sets have a more complicated description. However they are better behaved:

We will see in one of the next lectures that the image of a projective algebraic set under a morphism is always an algebraic subset of the target.
This was not the case for morphisms between affine algebraic sets.

Example

Consider $A = V(xy - z^2) \subset \mathbb{P}^2$. On the affine chart $U_{z=1}$ we saw that the projection

$$\mathbb{A}^2 \supset V(xy - 1) \to \mathbb{A}^1, (a, b) \mapsto a$$

is not surjective, because the origin o is not in the image.
The map

$$A \setminus \{[0 : 1 : 0]\} \to \mathbb{P}^1, [x : y : z] \mapsto [x : z]$$

extends to a surjective morphism $\pi : A \to \mathbb{P}^1$ because

$$[x : z] = [xy : yz] = [z^2 : yz] = [z : y]$$

holds on $A \setminus V(yz)$. Thus the missing preimage point of $o = [0 : 1] \in \mathbb{A}^1 \subset \mathbb{P}^1$ is the point $p = [0 : 1 : 0]$ on the line $V(z)$ at infinity.