Computer Algebra and Gröbner Bases

Frank-Olaf Schreyer

Saarland University WS 2020/21

Overview

Today's topic is Hilbert's syzygy theorem and the Hilbert polynomial

1. The syzygy theorem
2. Maps between graded modules
3. The Hilbert polynomial

Hilbert's syzygy theorem

Theorem. *Let M be a finitely generated $S = k[x_1, \ldots, x_n]$ module. Then M has a finite free resolution*

$$0 \longleftarrow M \longleftarrow F_0 \xleftarrow{\varphi_1} F_1 \xleftarrow{\varphi_2} \ldots \xleftarrow{\varphi_{c-1}} F_{c-1} \xleftarrow{\varphi_c} F_c \longleftarrow 0$$

of length $c \leq n$.

Here the $F_i = S^{b_i}$ are free S-modules and the maps $\varphi_i : F_i \to F_{i-1}$ satisfy

$$\ker(\varphi_i) = \operatorname{im}(\varphi_{i+1})$$

and the map φ_1 gives a free presentation of $M \cong \operatorname{coker}(\varphi_1)$:

$$0 \longleftarrow M \longleftarrow F_0 \xleftarrow{\varphi_1} F_1 .$$

Proof of the syzygy theorem

We give an algorithm which computes from a presentation

$$0 \longleftarrow M \longleftarrow F_0 \xleftarrow{\varphi_1'} F_1$$

of M a finite free resolution. Choose a global monomial order on F_0 and compute a Gröbner basis $f_1, \dots, f_{b_1}$ of $\operatorname{im}(\varphi_1')$. In first step we replace φ_1' by $\varphi_1 = (f_1|f_2|\dots|f_{b_1})$. The Buchberger test syzygies $G^{(i,\alpha)}$ form a Gröbner basis of $\ker(\varphi_1)$ with respect to the induced order and we take φ_2 as the matrix which has these test syzygies as columns. Computing the Buchberger test syzygies of the $G^{(i,\alpha)}$ yields the φ_3 and continuing in this way produces a free resolution. We still have a lot of choice in this process. We will show that under a suitable ordering of the Gröbner basis elements the process will stop after $c \leq n$ steps with a matrix φ_c which has a trivial kernel.

Proof of the syzygy theorem continued

Choose ℓ minimal such that

$$\mathrm{Lt}(f_1), \dots, \mathrm{Lt}(f_{b_1}) \in k[x_1, \dots, x_\ell]^{b_0} \subset k[x_1, \dots, x_n]^{b_0}.$$

In the worst case $\ell = n$. Now sort $f_1, \dots, f_{b_1}$ such that for every p

$$x_\ell^p | \mathrm{Lt}(f_j) \implies x_\ell^p | \mathrm{Lt}(f_i) \text{ for } j < i$$

holds. Then

$$\mathrm{Lt}(G^{(i,\alpha)}) \in k[x_1, \dots, x_{\ell-1}]^{b_1} \subset k[x_1, \dots, x_n]^{b_1}$$

because the power of x_ℓ in $\mathrm{Lt}(f_i)$ is at least as large as the power of x_ℓ in any $\mathrm{Lt}(f_j)$ with $j < i$. Sorting the $G^{(i,\alpha)}$ and the higher test syzygies similarly we obtain for the columns $H_j = H^{(i,\alpha)}$ of φ_c

$$\mathrm{Lt}(H^{(i,\alpha)}) \subset k[x_1]^{b_{c-1}} \subset k[x_1, \dots, x_n]^{b_{c-1}}$$

after $c \le \ell \le n$ steps and there are no more tests to do: Each lead term has a different component part since the column ideal $M_i = (x_1^{\alpha_1}) \subset k[x_1]$ is a principal ideal. $\square$

Example

We consider the ideal $J \subset S = k[w, x, y, z]$ generated by the entries of the first column in the following table

$w^2 - xz$	$-x$	y	0	$-z$	0	$-y^2 + wz$
$wx - yz$	w	$-x$	$-y$	0	z	z^2
$x^2 - wy$	$-z$	w	0	$-y$	0	0
$xy - z^2$	0	0	w	x	$-y$	$-yz$
$y^2 - wz$	0	0	$-z$	$-w$	x	w^2
	0	y	$-x$	w	$-z$	1
	$-y^2 + wz$	z^2	$-wy$	yz	$-w^2$	x

The original generators turn out to be a Gröbner basis and the algorithm produces a free resolution of shape

$$0 \longleftarrow S/J \longleftarrow S \xleftarrow{\varphi_1} S^5 \xleftarrow{\varphi_2} S^6 \xleftarrow{\varphi_3} S^2 \longleftarrow 0$$

with matrices

φ_1^t	φ_2
	φ_3^t

as above.

Free resolution over noetherian rings

Let R be a noetherian ring and M a finitely generated R-module. Then M has a free resolution

$$0 \leftarrow M \leftarrow R^{b_0} \leftarrow R^{b_1} \leftarrow \ldots \leftarrow R^{b_j} \leftarrow \ldots$$

where b_0 is the number of generators and b_1 the number of generators of the kernel of $R^{b_0} \to M$ and so on. What is so remarkable about $k[x_1, \ldots, x_n]$ is that the free resolution ends after finitely many steps. In general this is not true.

Example. Consider $R = k[x, y]/(xy)$ and the R-module $M = R/(\overline{x})$. The kernel of the presentation matrix

$$0 \longleftarrow M \longleftarrow R \xleftarrow{\overline{x}} R$$

is generated by $\overline{y}$. The kernel of the matrix $(\overline{y})$ is generated by $\overline{x}$ and the free resolution becomes periodic

$$0 \longleftarrow M \longleftarrow R \xleftarrow{\overline{x}} R \xleftarrow{\overline{y}} R \xleftarrow{\overline{x}} R \xleftarrow{\overline{y}} \ldots$$

Graded modules

Definition. Let $R = \bigoplus_d R_d$ be a graded ring. A **graded** R**-module** is an R-module with a decomposition

$$M = \bigoplus_{d \in \mathbb{Z}} M_d$$

as abelian group satisfying

$$R_e \cdot M_d \subset M_{e+d}$$

for the multiplication. A **homomorphism** $\varphi : M \to N$ **of graded** R**-modules** is an R-module homomorphism which respects the degree:

$$\varphi(M_d) \subset N_d.$$

Degree shift

With this notation, the R-module homomorphism

$$R \xrightarrow{f} R$$

given by multiplication with a homogeneous element $f \in R_d$ of degree $d \neq 0$ is not an homomorphism of graded R-modules. To remedy this situation we define $M(d)$ as the graded R-module with $M(d)_e = M_{d+e}$. The multiplication with an homogeneous element $f \in R_d$ induces graded R-module homomorphisms

$$M \xrightarrow{f} M(d) \quad \text{and} \quad M(-d) \xrightarrow{f} M$$

Example. Let $S = k[x_0, \ldots, x_n]$ be the standard graded polynomial ring in $n+1$ variables. Then $S(-j)$ is the free graded S-module with generator in degree j:

$$1 \in S(-j)_j = S_{-j+j} = S_0.$$

Hilbert's syzygy theorem in the graded case

Theorem. *Let* $S = k[x_0, \ldots, x_n]$ *be the standard graded polynomial ring in* $n+1$ *variables and let* M *be a finitely generated graded* S*-module. The* M *has a finite free resolution*

$$0 \longleftarrow M \longleftarrow F_0 \xleftarrow{\varphi_1} F_1 \xleftarrow{\varphi_2} \ldots \xleftarrow{\varphi_{c-1}} F_{c-1} \xleftarrow{\varphi_c} F_c \longleftarrow 0$$

of length $c \leq n+1$ *where*

$$F_i = \bigoplus_j S(-j)^{\beta_{ij}}$$

is a free graded S*-module with* β_{ij} *generators in degree* j*.*

Proof. The same procedure as before, we just keep track of the degrees in addition. □

The β_{ij} are called **graded Betti numbers** of the the resolution $F_\bullet$

Example

The ideal $J \subset S = k[w, x, y, z]$ from above is generated by homogeneous forms of degree 2

$w^2 - xz$	$-x$	y	0	$-z$	0	$-y^2 + wz$
$wx - yz$	w	$-x$	$-y$	0	z	z^2
$x^2 - wy$	$-z$	w	0	$-y$	0	0
$xy - z^2$	0	0	w	x	$-y$	$-yz$
$y^2 - wz$	0	0	$-z$	$-w$	x	w^2
	0	y	$-x$	w	$-z$	1
	$-y^2 + wz$	z^2	$-wy$	yz	$-w^2$	x

and the resolution is graded:

$$0 \leftarrow S/J \leftarrow S \leftarrow S(-2)^5 \leftarrow S(-3)^5 \oplus S(-4) \leftarrow S(-4) \oplus S(-5) \leftarrow 0.$$

The Hilbert function

Let $S = k[x_0, \ldots, x_n]$ be the standard graded polynomial ring in $n+1$ variables and let M be a finitely generated graded S-module. Then each M_d is a finite-dimensional k-vector space.

Definition. The function

$$h_M \colon \mathbb{Z} \to \mathbb{Z},\ d \mapsto h_M(d) = \dim_k M_d$$

is called the Hilbert function of M.

Example.

$$h_S(d) = \binom{d+n}{n}.$$

Proof.

$$\longleftrightarrow x^\alpha = x_0^{\alpha_0} \cdot \ldots \cdot x_n^{\alpha_n}$$

$\square$

Polynomial nature of the Hilbert function

Theorem. *Let $S = k[x_0, \ldots, x_n]$ be the standard graded polynomial ring in $n+1$ variables and let M be a finitely generated graded S-module. Then there exists a polynomial $p_M(t) \in \mathbb{Q}[t]$ and an $d_0 \in \mathbb{Z}$ such that*

$$h_M(d) = p_M(d) \text{ for all } d \geq d_0.$$

$p_M(t)$ is called the **Hilbert polynomial** of M.

Example.

$$p_S(t) = \frac{(t+n)(t+n-1)\cdot \ldots \cdot (t+1)}{n!} = \binom{t+n}{n}$$

for $t \geq -n$.

Proof

Let

$$0 \longleftarrow M \longleftarrow F_0 \xleftarrow{\varphi_1} F_1 \xleftarrow{\varphi_2} \dots \xleftarrow{\varphi_{c-1}} F_{c-1} \xleftarrow{\varphi_c} F_c \longleftarrow 0$$

be a finite free resolution of M with $F_i = \oplus_j S(-j)^{\beta_{ij}}$. Then for each $d \in \mathbb{Z}$ the sequence

$$0 \leftarrow M_d \leftarrow (F_0)_d \leftarrow (F_1)_d \leftarrow \dots \leftarrow (F_c)_d \leftarrow 0$$

is an exact complex of finite-dimensional k-vectorspaces. Thus

$$\begin{aligned} \dim M_d &= \sum_{i=0}^{c} (-1)^i \dim (F_i)_d \\ &= \sum_{i=0}^{c} (-1)^i \sum_j \beta_{ij} \binom{d-j+n}{n} \end{aligned}$$

Proof continued

Interpreting the binomial coefficients as polynomials

$$\binom{t-j+n}{n} = \frac{(t-j+n)\cdot \ldots \cdot (t-j+1)}{n!} \in \mathbb{Q}[t]$$

the formula

$$p_M(t) = \sum_{i=0}^{c} (-1)^i \sum_j \beta_{ij} \binom{t-j+n}{n} \in \mathbb{Q}[t]$$

defines the Hilbert polynomial, and $h_M(d) = p_M(d)$ holds for all $d \geq d_0$ with

$$d_0 = \min\{j \mid \exists i \text{ with } \beta_{ij} \neq 0\}.$$

$\square$

Corollary. *S/J and $S/\operatorname{Lt}(J)$ have the same Hilbert function and Hilbert polynomial.*

Proof. The graded Betti numbers of our resolution of S/J depend only on $\operatorname{Lt}(J)$. $\square$

Example: Hypersurfaces

Let $X = V(f)$ be a hypersurface defined by a (square free) homogeneous polynomial of degree d. Then

$$0 \longleftarrow S/(f) \longleftarrow S \xleftarrow{f} S(-d) \longleftarrow 0$$

is a free resolution and

$$\begin{aligned} p_{S/(f)}(t) &= \binom{t+n}{n} - \binom{t-d+n}{n} \\ &= \frac{t^n + \frac{n^2+n}{2}t^{n-1}}{n!} - \frac{t^n + (\frac{n^2+n}{2} - dn)t^{n-1}}{n!} + O(t^{n-2}) \\ &= d\frac{t^{n-1}}{(n-1)!} + \text{ lower terms.} \end{aligned}$$

In particular

$$\deg P_{S/(f)} = n-1 = \dim X$$

and the leading coefficient has the form $\frac{d}{(n-1)!}$.

Degree of projective varieties

Theorem. *Let $J \subset S = k[x_0, \dots, x_n]$ be a homogeneous ideal, and let $X = V(J) \subset \mathbb{P}^n$ be the algebraic set defined by J. The Hilbert polynomial of S/J has degree $r = \dim X$ and leading term*

$$d\frac{t^r}{r!}$$

for some positive integer d. We call d the **degree** of J.

Definition. For a projective algebraic set $X \subset \mathbb{P}^n$ the degree is defined by

$$\deg X = \deg \mathrm{I}(X)$$

where $\mathrm{I}(X) \subset K[x_0, \dots, x_n]$ denotes its homogeneous ideal.

Proof

Let $C(J) \subset \mathbb{A}^{n+1}$ be the cone defined by J. Since the Hilbert function of S/J depends only on $\mathrm{Lt}(J)$ we may assume that $k = K$ is algebraically closed, in particular we may assume that k is an infinite field. Then there exists a triangular linear change of coordinates such that in these new coordinates J satisfies the assumption of the tower of projection theorem: There exist an r such that projection $\mathbb{A}^{n+1} \to \mathbb{A}^{r+1}$ onto the last $r+1$ coordinates induces a finite surjection

$$C(J) \to \mathbb{A}^{r+1}$$

and the elimination ideals $J_k = K[x_k, \ldots, x_n] \cap J$ contain an x_k-monic polynomial for $k = 0, \ldots, n-r-1$. Thus S/J is a finite $T = k[x_{n-r}, \ldots, x_n]$-module.

Proof continued 1

Thus as an graded T-module S/J has a finite free resolution

$$0 \longleftarrow S/J \longleftarrow G_0 \xleftarrow{\varphi_1} G_1 \xleftarrow{\varphi_2} \dots \xleftarrow{\varphi_{c-1}} G_{c-1} \xleftarrow{\varphi_c} G_{c'} \longleftarrow 0$$

of length $c' \leq r+1$ where

$$G_i = \bigoplus_j T(-j)^{\beta'_{ij}}$$

is a free graded T-module with β'_{ij} generators in degree j and

$$p_{S/J}(t) = \sum_{i=0}^{c'} (-1)^i \sum_j \beta'_{ij} \binom{t-j+r}{r}$$

is an alternating sum of polynomials of degree r. Thus

$$p_{S/J}(t) = d\frac{t^r}{r!} + \text{ lower terms}$$

with $d \in \mathbb{Z}$.

Proof continued 2

To see that $d > 0$ holds, we notice that $T \cdot 1 \subset S/J$ is a T-submodule. Thus

$$h_{S/J}(t) \geq h_T(t) = \binom{t+r}{r}$$

growths at least as fast as a polynomial of degree r for $t \to \infty$.

It remains to identify r with the dimension of X. For this consider the charts $U_i = \{x_i \neq 0\} \cong \mathbb{A}^n$ for $i = n-r, \ldots, n$ and the corresponding substitution homomorphism

$$\varphi_i : S \to k[x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n],\ x_i \mapsto 1.$$

$\varphi_i(J)$ satisfies the assumption of the tower of projections theorem. Thus $X \cap U_i \to \mathbb{A}^r$ is a finite surjection and all the affine algebraic sets $X \cap U_i$ have dimension r.

Proof continued 3

Since $\operatorname{rad}(J + (x_{n-r}, \ldots, x_n)) = (x_0, \ldots, x_n)$ due to the monic polynomials in the elimination ideals we see that

$$V(J) \cap V(x_{n-r}, \ldots, x_n) = \emptyset \text{ equivalently } X \subset U_{n-r} \cup \ldots \cup U_n$$

Thus $\dim X = r$ if we define

$$\dim X = \max\{\dim X \cap U_j \mid j = 0, \ldots, n\}.$$

□

Corollary. *Let $J \subsetneq K[x_0, \ldots, x_n]$ be a proper homogeneous ideal. Then dimension of the projective algebraic set $V(J) \subset \mathbb{P}^n$ and the affine cone $C(J) \subset \mathbb{A}^{n+1}$ differ by one:*

$$\dim C(J) = \dim V(J) + 1.$$

□

Here we use the convention that $\dim \emptyset = -1$.