Lecture 8. The Hilbert function and the Hilbert polynomial

4.4 Hilbert polynomial

Problem: How to measure the "size" of an ideal I, or equivalently the "dimension" of the affine variety $\mathcal{V}(I)$?

Definition 4.14. *Let $I \subset k[X_1, \ldots, X_n]$ be an ideal and $s \in \mathbb{N}$, and let us write*

$$k[X_1, \ldots, X_n]_{\leq s} \coloneqq \{f \in k[X_1, \ldots, X_n] : f = 0 \text{ or } \deg(f) \leq s\}$$

and

$$I_{\leq s} \coloneqq I \cap k[X_1, \ldots, X_n]_{\leq s}.$$

The **Hilbert function** *of I is the function $HF_I : \mathbb{N} \to \mathbb{N}$,*

$$HF_I(s) = \dim_k \left(\frac{k[X_1, \ldots, X_n]_{\leq s}}{I_{\leq s}} \right) < \infty.$$

▶ (a) Let $I = k[X_1, \ldots, X_n]$. Then $HF_I(s) = 0$ for all $s \in \mathbb{N}$.

(b) Let $I = \{0\}$. Then

$$\begin{aligned} HF_I(s) &= \dim_k k[X_1, \ldots, X_n]_{\leq s} \\ &= \text{ number of monomials } X^\alpha \text{ with } |\alpha| \leq s \\ &= |\{(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n : \alpha_1 + \ldots + \alpha_n \leq s\}| = \binom{s+n}{n} \\ &= \frac{1}{n!}(s+n)(s+n-1)\cdots(s+1) = \frac{1}{n!}s^n + \frac{1}{n!}\binom{n+1}{2}s^{n-1} + \ldots + \sum_{i=1}^{n} \frac{1}{i}s + 1 \end{aligned}$$

is a polynomial of degree n.

(c) Suppose that $I = (f)$ where $0 \neq f \in k[X_1, \ldots, X_n]$ with $\deg(f) = d$. Then

$$HF_I(s) = \dim_k k[X_1, \ldots, X_n]_{\leq s} - \dim_k I_{\leq s}.$$

Since $\deg(gf) = \deg(g) + d$ for $g \neq 0$, we have

$$I_{\leq s} = \{g \cdot f : g \in k[X_1, \ldots, X_n]_{\leq s-d}\},$$

which is $\{0\}$ if $s < d$. If $s \geq d$, then $g \mapsto gf$ is an injective linear map from $k[X_1, \ldots, X_n]_{\leq s-d}$ onto $I_{\leq s}$, so $\dim_k I_{\leq s} = |\{X^\alpha : |\alpha| \leq s-d\}| = \binom{n+s-d}{n}$. Hence

$$HF_I(s) = \begin{cases} \binom{n+s}{n} & \text{if } s < d, \\ \binom{n+s}{n} - \binom{n+s-d}{n} = \dfrac{d}{(n-1)!}s^{n-1} + \text{lower order terms} & \text{if } s \geq d. \end{cases}$$

Lemma 4.15. *(Macaulay) Let us equip $k[X_1, \ldots, X_n]$ with the graded lexicographic order $\leq_{grlex}$ (any graded monomial order would do). Let I be an ideal, and $\mathrm{in}(I) = (LT(f) : f \in I)$. Then*

$$HF_I(s) = HF_{\mathrm{in}(I)}(s) \quad \text{for all} \quad s \geq 0.$$

Proof. Since the order is graded, $\deg LM(f) = \deg f$ for every non-zero f. Hence the set of leading monomials

$$\{LM(f) : 0 \neq f \in I_{\leq s}\} = \{LM(f_1), \ldots, LM(f_m)\}$$

is finite, where $f_1, \ldots, f_m \in I_{\leq s}$ and $LM(f_1) > LM(f_2) > \ldots > LM(f_m)$.

We will show that (a) $\{f_1, \ldots, f_m\}$ is a k-basis of $I_{\leq s}$, (b) $\{LM(f_1), \ldots, LM(f_m)\}$ is a k-basis of $\mathrm{in}(I)_{\leq s}$. Then $\dim_k I_{\leq s} = m = \dim_k \mathrm{in}(I)_{\leq s}$, which implies the stated result.

Linear independence for (a): Suppose there exist $a_i \in k$, not all zero, such that $\sum_{i=1}^m a_i f_i = 0$. Choose the smallest i_0 such that $a_{i_0} \neq 0$. Then

$$0 = a_{i_0} f_{i_0} + a_{i_0+1} f_{i_0+1} + \ldots + a_m f_m$$

but $LM(f_i) < LM(f_{i_0})$ for $i > i_0$, so the term $a_{i_0} LT(f_{i_0})$ cannot cancel, a contradiction.

Linear independence for (b): distinct monomials are linearly independent.

Spanning property for (a): Let $0 \neq f \in I_{\leq s}$. Then $LM(f) = LM(f_i)$ for some i. Hence $LT(f) = cLT(f_i)$ for some $c \in k$. Consider $f' = f - cf_i \in I_{\leq s}$. If $f' = 0$, then $f = cf_i$ as desired. Otherwise $LM(f') < LM(f)$, and we repeat the argument with f'. By Lemma 4.5 this terminates after finitely many steps.

Spanning property for (b): Let $g \in \mathrm{in}(I)_{\leq s}$. Since $\mathrm{in}(I)$ is the monomial ideal generated by $\{LM(f) : f \in I\}$, by Lemma 4.4 each term of g is divisible by some $LM(f)$ with $f \in I$: say the term is cX^γ with $X^\gamma = X^\alpha LM(f) = LM(X^\alpha f)$. Now $X^\alpha f \in I$ and $\deg(X^\alpha f) = |\gamma| \leq \deg g \leq s$, so $X^\alpha f \in I_{\leq s}$ and X^γ is one of $LM(f_1), \ldots, LM(f_m)$. Therefore g is a linear combination of $LM(f_1), \ldots, LM(f_m)$. □

▶ The hypothesis that the order is graded cannot be dropped. Let $I = (X - Y^2) \subset k[X, Y]$ with the lex order, $X > Y$. Then $\mathrm{in}(I) = (X)$ and $HF_{\mathrm{in}(I)}(s) = s + 1$, since the monomials of degree $\leq s$ not in (X) are $1, Y, \ldots, Y^s$, but $HF_I(s) = \binom{s+2}{2} - \binom{s}{2} = 2s + 1$ by Example (c). The proof breaks down in the spanning property for (b): $X \in \mathrm{in}(I)_{\leq 1}$, but the elements of I with leading monomial X are the $c(X - Y^2)$, $c \in k^*$, which are not in $I_{\leq 1}$.

▶ Let $I = (Y - X^2, Z - X^3) \subset k[X, Y, Z]$. Using $\leq_{grlex}$, one can show that $G = \{X^2 - Y, XY - Z, XZ - Y^2, Y^3 - Z^2\}$ is a Gröbner basis. Here is how to check this in Macaulay2:

```
R = QQ[x,y,z, MonomialOrder => GLex];
I = ideal (y-x^2,z-x^3);
gens gb I
```

Thus, $\mathfrak{in}(I) = (X^2, XY, XZ, Y^3)$. By Macaulay's lemma and Lemma 4.4, $HF_I(s)$ is the number of standard monomials of degree $\leq s$, that is, monomials of degree $\leq s$ not in $\mathfrak{in}(I)$. These are $1, X, Y, Z$ and $Z^r, YZ^{r-1}, Y^2Z^{r-2}$ for $r \geq 2$, so $HF_I(s) = 3s+1$ for all $s \geq 0$. The next theorem shows that $HF_I(s)$ is always given by a polynomial for large s.

Theorem 4.16. *Let $I \subset k[X_1, \ldots, X_n]$ be an ideal. There exist a unique polynomial $HP_I(t) \in \mathbb{Q}[t]$, called the Hilbert polynomial of I, and an integer $s_0 \geq 0$ such that*

$$HF_I(s) = HP_I(s) \quad \text{for all} \quad s \geq s_0.$$

If $I = k[X_1, \ldots, X_n]$ then $HP_I(t) = 0$. Otherwise $HP_I(t) \neq 0$, and if we write

$$HP_I(t) = a_d t^d + a_{d-1} t^{d-1} + \ldots + a_0$$

with $a_d \neq 0$, then $a_i d! \in \mathbb{Z}$ for all i and $a_d d! > 0$.

Proof. By the previous lemma, we may assume without loss of generality that $I = \mathfrak{in}(I) = (X^{\beta^{(1)}}, \ldots, X^{\beta^{(m)}})$ is a monomial ideal with $\beta^{(i)} \in \mathbb{N}^n$ (generated by the leading monomials of a Gröbner basis). By Lemma 4.4, a polynomial f is in I if and only if each term of f is divisible by $X^{\beta^{(i)}}$ for some i. Therefore $I_{\leq s}$ has k-basis $\{X^\alpha : |\alpha| \leq s \text{ and } X^{\beta^{(i)}} \mid X^\alpha \text{ for some } i\}$. Put $C(I) := \{\alpha \in \mathbb{N}^n : X^{\beta^{(i)}} \nmid X^\alpha \text{ for all } i\}$ and $C(I)_{\leq s} := \{\alpha \in C(I) : |\alpha| \leq s\}$. Then the monomials X^α with $\alpha \in C(I)_{\leq s}$ form a basis of $k[X_1, \ldots, X_n]_{\leq s}/I_{\leq s}$, so

$$HF_I(s) = |C(I)_{\leq s}|.$$

Next, we need to compute $|C(I)_{\leq s}|$. We will show that $C(I)$ is a finite union of translates of coordinate subspaces, which we denote as follows: for $J \subset \{1, 2, \ldots, n\}$ and a function $\tau : J \to \mathbb{N}$, we set

$$C(J, \tau) := \{(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n : \alpha_j = \tau(j) \text{ for all } j \in J\}.$$

Extend τ to $\{1, \ldots, n\}$ by setting $\tau(i) = 0$ for $i \notin J$. Then

$$C(J, \tau) = \{(\alpha_1 + \tau(1), \ldots, \alpha_n + \tau(n)) : \alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n \text{ such that } \alpha_j = 0 \text{ for all } j \in J\}.$$

Let $|\tau| = \sum_{j \in J} \tau(j)$ and $e = n - |J|$. For $s \geq |\tau|$ we have

$$\begin{aligned} |C(J, \tau)_{\leq s}| &= |\{\alpha \in \mathbb{N}^n : |\alpha| \leq s - |\tau| \text{ and } \alpha_j = 0 \text{ for all } j \in J\}| \\ &= \binom{e + s - |\tau|}{e} = \frac{1}{e!}(s^e + \text{ lower order terms}), \end{aligned}$$

a polynomial in s of degree e with positive leading coefficient, and $e!$ times it has integer coefficients.

We also note that for two pairs (J, τ) and (J', τ'), we have

$$C(J, \tau) \cap C(J', \tau') = \begin{cases} \emptyset \text{ if } J \cap J' \neq \emptyset \text{ and } \tau(j) \neq \tau'(j) \text{ for some } j \in J \cap J' \\ C(J \cup J', \tau \cup \tau') \text{ otherwise.} \end{cases}$$

Claim: There exists a finite collection $\mathcal{J}$ of pairs (J,τ) such that

$$C(I) = \bigcup_{(J,\tau)\in\mathcal{J}} C(J,\tau).$$

For $\beta \in \mathbb{N}^n$ let $C(\beta) = \{\alpha \in \mathbb{N}^n : X^\beta \nmid X^\alpha\}$. Then $C(I) = \bigcap_{i=1}^m C(\beta^{(i)})$. Now $\alpha \in C(\beta)$ if and only if $\alpha_i < \beta_i$ for some $i \in \{1,\dots,n\}$. Hence

$$C(\beta) = \bigcup_{i=1}^{n}\bigcup_{t=0}^{\beta_i-1} \{\alpha \in \mathbb{N}^n : \alpha_i = t\} = \bigcup_{i=1}^{n}\bigcup_{t=0}^{\beta_i-1} C(\{i\}, i \mapsto t)$$

is a finite union of sets of the form $C(J,\tau)$. Therefore $C(I)$ is a finite intersection of finite unions of such sets, hence a finite union of finite intersections of such sets, and by the formula above each of these intersections is empty or again of the form $C(J,\tau)$. This proves the claim.

The theorem now follows from the inclusion-exclusion principle: if $A_1,\dots,A_k$ are finite sets then

$$|A_1 \cup A_2 \cup \ldots \cup A_k| = \sum_{r=1}^{k} \sum_{1\le i_1<\ldots<i_r\le k} (-1)^{r-1} |A_{i_1} \cap \ldots \cap A_{i_r}|.$$

Apply this to $C(I)_{\le s} = \bigcup_{(J,\tau)\in\mathcal{J}} C(J,\tau)_{\le s}$. For $(J_1,\tau_1),\dots,(J_r,\tau_r) \in \mathcal{J}$, the intersection $C(J_1,\tau_1) \cap \ldots \cap C(J_r,\tau_r)$ is empty or of the form $C(J,\tau)$ with $J = J_1 \cup \ldots \cup J_r$, and there are finitely many such intersections; let s_0 be the largest $|\tau|$ that occurs. By the computation of $|C(J,\tau)_{\le s}|$, for $s \ge s_0$ the function $HF_I(s) = |C(I)_{\le s}|$ agrees with a $\mathbb{Z}$-linear combination $HP_I(s)$ of polynomials $\binom{e+s-|\tau|}{e}$ with $e = n - |J|$. The polynomial HP_I is unique, since a polynomial is determined by its values at infinitely many points.

If $I = k[X_1,\dots,X_n]$ then $C(I) = \emptyset$ and $HP_I = 0$. Otherwise $0 \in C(I)$, so $\mathcal{J} \ne \emptyset$, and we let $D = \max\{n-|J| : (J,\tau) \in \mathcal{J}\}$. Each e above is at most D, so $\deg HP_I \le D$, and since $e!$ divides $D!$, the polynomial $D!\,HP_I(t)$ has integer coefficients. On the other hand, if (J,τ) is any pair with $C(J,\tau) \subset C(I)$, then

$$HP_I(s) = HF_I(s) \ge |C(J,\tau)_{\le s}| = \binom{n-|J|+s-|\tau|}{n-|J|} \quad \text{for } s \ge \max(s_0,|\tau|),$$

and the right hand side is a polynomial in s of degree $n-|J|$ with positive leading coefficient. Hence $\deg HP_I \ge n-|J|$, and the leading coefficient of HP_I is positive. Taking $(J,\tau) \in \mathcal{J}$ with $n-|J| = D$ gives $d = \deg HP_I = D$, so $a_d d! > 0$ and $a_i d! \in \mathbb{Z}$ for all i. We have also shown that

$$\deg HP_I(t) = \max\{n-|J| : \exists (J,\tau) \text{ with } C(J,\tau) \subset C(I)\},$$

which will be used in the next lecture. □

► The proof can be visualised on the staircase diagram of a monomial ideal; see Figure 3 for $I = (XY^3, X^2Y, X^5) \subset k[X,Y]$, the ideal of Figure 2. The points of $C(I)$ lie below the staircase, and they form the α_2-axis $C(\{1\}, 1 \mapsto 0)$ together with six isolated points $C(\{1,2\},\tau)$. Now

$HF_I(s)$ counts the points of $C(I)$ on or below the line $\alpha_1 + \alpha_2 = s$: the axis contributes $s+1$ and each isolated point contributes 1 once $s \geq |\tau|$. Hence $HF_I(s) = s + 7$ for $s \geq 4$, and $HP_I(t) = t + 7$ with $s_0 = 4$. In general, $\deg HP_I(t)$ is the largest dimension of a translated coordinate subspace fitting under the staircase, and for an irredundant decomposition $d!\, a_d$ is the number of such subspaces of dimension d.

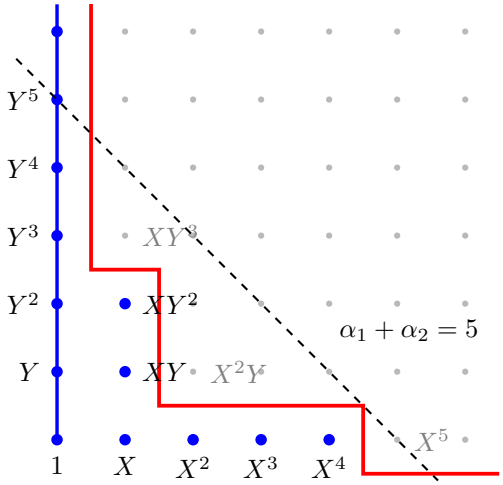

Figure 3: The points of $C(I)$ for $I = (XY^3, X^2Y, X^5)$, in blue: the α_2-axis and six isolated points. $HF_I(5) = 12$ counts those on or below the dashed line.