
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 “dimension” of the affine variety $\mathcal{V}(I)$?

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

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

and

$$I_{\leq s} := I \cap k[X_1, \dots, X_n]_{\leq s}$$

We define

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

Hilbert function of I , as a function $HF_I : \mathbb{N} \rightarrow \mathbb{N}$.

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

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

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

is a polynomial of degree n .

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

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

We have

$$I_{\leq s} = \{g \cdot f \mid g \in k[X_1, \dots, X_n], \deg(g) + d \leq s\}$$

Thus, if $s < d$, then $I_{\leq s} = \{0\}$. If $s \geq d$, then $\dim_k I_{\leq s} = |\{X^\alpha : |\alpha| \leq s - d\}|$. Hence,

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

Lemma 4.15. (Macaulay) Let us equip $k[X_1, \dots, X_n]$ with graded lexicographic order $\leq_{grlex}$. Let I be an ideal, and $\text{in}(I) = (LT(f) : f \in I)$. Then,

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

Proof. $I_{\leq s}$ contains only a finite number of monomials

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

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

We will show that (a) $\{f_1, \dots, f_m\}$ is a k -basis of $I_{\leq s}$, (b) $\{LM(f_1), \dots, LM(f_m)\}$ gives a k -basis for $\text{in}(I)_{\leq s}$. (This implies the stated result.)

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

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

but $LM(f_i) < LM(f_{i_0})$, so we have a contradiction.

Linear independence for (b): clear.

Spanning property for (a): Let $f \in I_{\leq s}$. 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, $LM(f') < LM(f)$ (strictly smaller). Hence, repeat the argument with f' .

Spanning property for (b): Let $g \in \text{in}(I)_{\leq s}$. Then $g = \sum_j h_j LT(g_j)$ for some $h_j \in k[X_1, \dots, X_n]$ and $g_j \in I$. We write $h_j = \sum_{\alpha} a_{\alpha,j} X^{\alpha}$ with $a_{\alpha,j} \in k$. Hence, $g = \sum_{j,\alpha} a_{\alpha,j} X^{\alpha} LT(g_j) = \sum_{j,\alpha} a_{\alpha,j} LT(X^{\alpha} g_j)$. Since $X^{\alpha} g_j \in I$, by letting $g_{\alpha,j} = X^{\alpha} g_j$, we can write $g = \sum_{\alpha,j} a_{\alpha,j} LT(g_{\alpha,j})$ with $a_{\alpha,j} \in k$ and $g_{\alpha,j} \in I$. Now, $LT(g_{\alpha,j}) \leq LT(g)$, hence (using the graded lex order) we see that $\deg(g_{\alpha,j}) \leq \deg(g) \leq s$. Therefore, g is a linear combination of $LM(f_1), \dots, LM(f_m)$. $\square$

► 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. For example, here is how to do it in Macaulay2:

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

Thus, $\text{in}(I) = (X^2, XY, XZ, Y^3)$. From which, we deduce that $C(I) = \{1, X, Y, Z\} \cup \{Z^s, YZ^{s-1}, Y^2Z^{s-2}\}_{s \geq 2}$ and $HP_I(t) = 3t + 1$.

Theorem 4.16. Let $I \subset k[X_1, \dots, X_n]$. There exists a unique polynomial, called the Hilbert polynomial, $HP_I(t) \in \mathbb{Q}[t]$ and a positive number $s_0 \geq 0$ such that

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

If $I = k[X_1, \dots, X_n]$ then $HP_I(t) = 0$, otherwise $HP_I(t) \neq 0$. Write

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

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 $I = \text{in}(I) = (X^{\beta^{(1)}}, \dots, X^{\beta^{(m)}})$ is a monomial ideal with $\beta^{(i)} \in \mathbb{N}^n$. Now, since I is a monomial ideal, a polynomial f is in I if and only if each term of f is divisible by an $X^{\beta^{(i)}}$ for some i . Therefore $f \in I_{\leq s}$ is generated by $\{X^\alpha : |\alpha| \leq s \text{ and } X^{\beta^{(i)}} \mid X^\alpha \text{ for some } i\}$. Put $C(I) := \{\alpha \in \mathbb{N}^n : X^{\beta^{(i)}} \nmid X^\alpha \text{ for any } i\}$ and $C(I)_{\leq s} := \{\alpha \in \mathbb{N}^n : |\alpha| \leq s, \alpha \in C(I)\}$. Thus, it follows that

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

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 $J \subset \{1, 2, \dots, n\}$ and a function $\tau : J \rightarrow \mathbb{N}$, we set

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

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

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

Let $\tau = \sum_{j \in J} \tau(j)$. We have

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

provided $s > |\tau|$, in which case it is a polynomial in s of degree $d = n - |J|$.

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 $C(I) = \bigcap C(\beta^{(i)})$. We first show that $C(\beta)$ can be covered by some $C(J, \tau)$. Indeed, $\alpha \in C(\beta)$ if and only if there exists an $i \in \{1, \dots, n\}$ such that $\alpha_i < \beta_i$. Hence,

$$C(\beta) = \bigcup_{i=1}^n \bigcup_{t_i=0}^{\beta_i-1} \{(\alpha_1, \dots, \alpha_n) : \alpha_i = t_i\} = \bigcup_{i=1}^n \bigcup_{t_i} C(\{t_i\}, \tau : i \rightarrow t_i) = \bigcup_{(J, \tau)} C(J, \tau)$$

where in the last equality, we have avoided to specify which specific (J, τ) are used in order to avoid cumbersome notation. It suffices to note that there are only finitely many (J, τ) that are being used. Now, the claim follows from

$$C(I) = \bigcap_{i=1}^m C(\beta^{(i)}) = \bigcap_{i=1}^m \bigcup_{(J, \tau)} C(J, \tau) = \bigcup \{ \text{intersections of } C(J, \tau) \} = \bigcup_{(J, \tau) \in \mathcal{J}} C(J, \tau)$$

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

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

Applying this to $C(I)$ written as a union of $C(J, \tau)$ gives the desired polynomial $HP_I(t)$. Moreover, the degree can be computed as

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

□