12 Hilbert polynomials and the Bezout Theorem

Hilbert polynomials are the main tool for classifying projective varieties. Many invariants of topological and geometric interest, like the genus of a Riemann surface, are encoded in their coefficients. Here we will carefully analyze the Hilbert polynomials of ideals defining finite sets over algebraically closed fields. The Bezout Theorem is the main application.

Hilbert polynomials are defined in terms of the Hilbert function, but the precise relationship between the Hilbert function and the Hilbert polynomial is extremely subtle and continues to be the object of current research. The interpolation problems considered in Chapter 1 involve measuring the discrepancy between these two invariants.

12.1 Hilbert functions defined

While our main focus is homogeneous ideals in polynomial rings, Hilbert functions and polynomials are used in a much broader context:

Definition 12.1 A *graded ring* R is a ring admitting a direct-sum decomposition

$$R = \oplus_{t \in \mathbb{Z}} R_t$$

compatible with multiplication, i.e., $R_{t_1} R_{t_2} \subset R_{t_1+t_2}$ for all $t_1, t_2 \in \mathbb{Z}$. The decomposition is called a *grading* of R and the summands R_t are called its *graded pieces*; elements $F \in R_t$ are *homogeneous* of degree t.

Let k be a field. A *graded k-algebra* is a k-algebra R with a grading compatible with the algebra structure, i.e., for any $c \in k$ and $F \in R_t$ we have $cF \in R_t$.

Observe that the constants in a graded k-algebra necessarily have degree zero.

Example 12.2

1. $S = k[x_0, \ldots, x_n]$ is a graded ring with graded pieces

$$S_t = k[x_0, \ldots, x_n]_t = \text{homogeneous forms of degree } t.$$

https://doi.org/10.1017/CBO9780511755224.013 Published online by Cambridge University Press

2. Let $w_0, \ldots, w_n$ be positive integers. Then $S = k[x_0, \ldots, x_n]$ is graded with graded pieces

$$S_t = \operatorname{span}\left(x_0^{\alpha_0} \ldots x_n^{\alpha_n} : w_0\alpha_0 + \cdots + w_n\alpha_n = t\right).$$

This is called a *weighted polynomial ring*.

3. Let $J \subset S = k[x_0, \ldots, x_n]$ be a homogeneous ideal. The quotient ring $R = S/J$ is graded with graded pieces

$$R_t = \operatorname{image}(k[x_0, \ldots, x_n]_t \to S/J).$$

Here is a proof: For each t, the inclusion $k[x_0, \ldots, x_n]_t \subset k[x_0, \ldots, x_n]$ induces an inclusion $R_t \subset R$. These together give a surjective homomorphism $\oplus_{t \geq 0} R_t \to R$. We claim this is injective. Suppose we have homogeneous $F_j \in k[x_0, \ldots, x_n]_j$, $j = 0, \ldots, r$, such that $F_0 + \cdots + F_r \equiv 0$ in R, i.e., $F_0 + \cdots + F_r \in J$. By Exercise 9.1, each $F_j \in J$ and thus $F_j \equiv 0$ in R_j.

4. For any projective variety $X \subset \mathbb{P}^n(k)$ the ring

$$R(X) = k[x_0, \ldots, x_n]/J(X)$$

is graded; it is called the *graded coordinate ring* of X.

Definition 12.3 Let R be a graded k-algebra with $\dim_k R_t < \infty$ for each t. The *Hilbert function* $\mathrm{HF}_R : \mathbb{Z} \to \mathbb{Z}$ is defined

$$\mathrm{HF}_R(t) = \dim_k R_t.$$

We compute Hilbert functions in some important examples:

Example 12.4

1. For $S = k[x_0, \ldots, x_n]$ with the standard grading, we have

$$\mathrm{HF}_S(t) = \binom{t+n}{t}.$$

2. If $F \in k[x_0, \ldots, x_n]$ is homogeneous of degree d and $R = k[x_0, \ldots, x_n]/\langle F \rangle$ then

$$\mathrm{HF}_R(t) = \binom{t+n}{n} - \binom{t-d+n}{n}$$

for $t \geq d$. Indeed, the elements of $\langle F \rangle$ of degree t are of the form FG where G is an arbitrary homogeneous polynomial of degree $t - d$.

3. If $a = [a_0, \ldots, a_n] \in \mathbb{P}^n(k)$ and $R = k[x_0, \ldots, x_n]/J(a)$ then $\mathrm{HF}_R(t) = 1$ for $t \geq 0$.

Hilbert functions are invariant under projectivities:

https://doi.org/10.1017/CBO9780511755224.013 Published online by Cambridge University Press

Proposition 12.5 *Let $J \subset k[x_0, \ldots, x_n]$ be homogeneous, $\phi : \mathbb{P}^n(k) \to \mathbb{P}^n(k)$ a projectivity, and $J' = \phi^* J$. If $R = k[x_0, \ldots, x_n]/J$ and $R' = k[x_0, \ldots, x_n]/J'$ then* $\mathrm{HF}_R(t) = \mathrm{HF}_{R'}(t)$.

Proof The coordinate functions of ϕ take the form

$$\phi_i(x_0, \ldots, x_n) = \sum_{j=0}^{n} a_{ij} x_j$$

where $A = (a_{ij})$ is an $(n+1) \times (n+1)$ invertible matrix. The corresponding homomorphism

$$\phi^* : k[x_0, \ldots, x_n] \to k[x_0, \ldots, x_n]$$

restricts to invertible linear transformations

$$\begin{aligned} (\phi^*)_t : k[x_0, \ldots, x_n]_t &\to k[x_0, \ldots, x_n]_t \\ x_0^{\alpha_0} \ldots x_n^{\alpha_n} &\mapsto \left(\textstyle\sum_{j=0}^n a_{0j} x_j\right)^{\alpha_0} \ldots \left(\textstyle\sum_{j=0}^n a_{nj} x_j\right)^{\alpha_n} \end{aligned}$$

for each $t \geq 0$. It follows that

$$\dim_k J'_t = \dim_k (\phi^*)_t J_t = \dim_k J_t$$

for each t, and $\mathrm{HF}_R(t) = \mathrm{HF}_{R'}(t)$. □

Proposition 12.6 *Let $J, J' \subset k[x_0, \ldots, x_n]$ be graded ideals with intersection $J'' = J \cap J'$, and write*

$$R = k[x_0, \ldots, x_n]/J,\ R' = k[x_0, \ldots, x_n]/J',\ R'' = k[x_0, \ldots, x_n]/J''.$$

Then we have

$$\mathrm{HF}_R(t) + \mathrm{HF}_{R'}(t) \geq \mathrm{HF}_{R''}(t).$$

Equality holds for $t \gg 0$ if and only if $J + J'$ is irrelevant.

Proof Let J_t, J'_t, and J''_t denote the degree-t graded pieces of the corresponding ideals, e.g., $J_t = J \cap k[x_0, \ldots, x_n]_t$. For each $t \geq 0$, we have a surjection

$$J_t \oplus J'_t \twoheadrightarrow (J + J')_t$$

with kernel J''_t. Thus we find

$$\dim J_t + \dim J'_t = \dim (J + J')_t + \dim J''_t$$

and

$$\dim R_t + \dim R'_t = \dim k[x_0, \ldots, x_n]_t/(J + J')_t + \dim R''_t.$$

https://doi.org/10.1017/CBO9780511755224.013 Published online by Cambridge University Press

This yields the identity of Hilbert functions

$$\mathrm{HF}_R(t) + \mathrm{HF}_{R'}(t) = \mathrm{HF}_{R''}(t) + \dim k[x_0, \dots, x_n]_t/(J + J')_t,$$

and our first inequality follows. $J + J'$ is irrelevant if and only if $(J + J')_N = k[x_0, \dots, x_n]_N$ for $N \gg 0$; equality holds for precisely these values of t. □

Definition 12.7 The *Hilbert function* of a projective variety X is defined

$$\mathrm{HF}_X(t) = \mathrm{HF}_{R(X)}(t),$$

where $R(X)$ is its graded coordinate ring.

Proposition 12.8 *If $X_1, \dots, X_r \subset \mathbb{P}^n(k)$ are projective varieties then*

$$\mathrm{HF}_{\cup_j X_j}(t) \leq \sum_{j=1}^{r} \mathrm{HF}_{X_j}(t).$$

Equality holds for $t \gg 0$ provided $J(X_i) + J(X_j)$ irrelevant for each $i \neq j$.

Proof By induction, it suffices to address the $r = 2$ case. Just as for affine varieties, we have

$$J(X_1 \cup X_2) = J(X_1) \cap J(X_2).$$

Proposition 12.6 then gives the result. □

An application of the Projective Nullstellensatz (Theorem 9.25) yields

Corollary 12.9 *Let k be algebraically closed. Suppose $X_1, \dots, X_r \subset \mathbb{P}^n(k)$ are projective varieties which are pairwise disjoint. Then for $t \gg 0$*

$$\mathrm{HF}_{\cup_j X_j}(t) = \sum_{j=1}^{r} \mathrm{HF}_{X_j}(t).$$

In the special case where each X_j is a point we obtain

Corollary 12.10 *Let $S \subset \mathbb{P}^n(k)$ be finite. Then $\mathrm{HF}_S(t) = |S|$ for $t \gg 0$.*

The following case is crucial for the Bezout Theorem:

Proposition 12.11 *Let $F, G \in S = k[x_0, \dots, x_n]$ be homogeneous of degree d and e without common factors. The quotient ring $R = S/\langle F, G\rangle$ has Hilbert function*

$$\begin{aligned}\mathrm{HF}_R(t) &= \dim S_t - \dim S_{t-d} - \dim S_{t-e} + \dim S_{t-d-e}\\ &= \tbinom{t+n}{n} - \tbinom{t+n-d}{n} - \tbinom{t+n-e}{n} + \tbinom{t+n-d-e}{n}\\ &\qquad \textit{provided } t \geq d + e.\end{aligned}$$

If $n = 2$ then $\mathrm{HF}_R(t) = de$ for $t \gg 0$.

https://doi.org/10.1017/CBO9780511755224.013 Published online by Cambridge University Press

Proof Let $q : S \to R$ be the quotient homomorphism and $q(t) : S_t \to R_t$ the induced linear transformation. Recall (Exercise 2.15) that $AF + BG = 0$ for $A, B \in k[x_0, \ldots, x_n]$ if and only if $A = CG$ and $B = -CF$ for some $C \in k[x_0, \ldots, x_n]$. We have a series of linear transformations (cf. §5.4)

$$\begin{array}{ccccccc} 0 \to S_{t-d-e} & \stackrel{\delta_1(t)}{\to} & S_{t-d} \oplus S_{t-e} & \stackrel{\delta_0(t)}{\to} & S_t & \stackrel{q(t)}{\to} & R_t \to 0 \\ C & \mapsto & (CG, -CF) & & & & \\ & & (A, B) & \mapsto & AF + BG & & \end{array}$$

where $\ker(\delta_0(t)) = \operatorname{image}(\delta_1(t))$, $\ker(q(t)) = \operatorname{image}(\delta_0(t))$, $\delta_1(t)$ is injective, and $q(t)$ is surjective. Applying the rank-nullity theorem successively, we obtain

$$\dim R_t = \dim S_t - \dim S_{t-d} - \dim S_{t-e} + \dim S_{t-d-e}.$$

The formula $\dim S_r = \binom{r+n}{n}$ is valid for $r \geq 0$ and yields

$$\mathrm{HF}_R(t) = \binom{t+n}{n} - \binom{t+n-d}{n} - \binom{t+n-e}{n} + \binom{t+n-d-e}{n}$$

for $t \geq d + e$. We also have

$$\dim S_r = \frac{(r+n)(r+n-1)\ldots(r+1)}{n!}$$

for $r \geq -n$; when $n = 2$, we obtain $\mathrm{HF}_R(t) = de$ for all $t \geq d + e - 2$. □

12.2 Hilbert polynomials and algorithms

Proposition 12.12 *Let $J \subset S = k[x_0, \ldots, x_n]$ be a homogeneous ideal, $>$ a monomial order, and $\mathrm{LT}(J)$ the ideal of leading terms of J. Then $\mathrm{HF}_{S/J}(t) = \mathrm{HF}_{S/\mathrm{LT}(J)}(t)$.*

This reduces the computation of Hilbert functions to the case of monomial ideals.

Proof This follows immediately from the existence of normal forms (Theorem 2.16): The monomials not in $\mathrm{LT}(J)$ form a basis for S/J as a vector space. In particular, the monomials of degree t not in $\mathrm{LT}(J)$ form a basis for $(S/J)_t = S_t/J_t$. □

From now on, we use binomial notation to designate polynomials with rational coefficients: For each integer $r \geq 0$, we write

$$\binom{t}{r} = \begin{cases} t(t-1)\ldots(t-r+1)/r! & \text{if } r > 0 \\ 1 & \text{if } r = 0, \end{cases}$$

https://doi.org/10.1017/CBO9780511755224.013 Published online by Cambridge University Press

which is a polynomial of degree r in $\mathbb{Q}[t]$. We allow t to assume both positive and negative values.

Proposition 12.13 *Let $f : \mathbb{Z} \to \mathbb{Z}$ be a function such that*

$$(\Delta f)(t) := f(t+1) - f(t)$$

is a polynomial of degree $d-1$. Then f is a polynomial of degree d and can be written in the form

$$f(t) = \sum_{j=0}^{d} a_j \binom{t}{d-j}, \quad a_j \in \mathbb{Z}. \tag{12.1}$$

In particular, any polynomial $P(t) \in \mathbb{Q}[t]$ of degree d with $P(\mathbb{Z}) \subset \mathbb{Z}$ takes this form.

Proof The key to the proof is the identity

$$\binom{t+1}{r} - \binom{t}{r} = \binom{t}{r-1},$$

which we leave to the reader.

The argument uses induction on degree. The base case $d = 1$ is straightforward: If $(\Delta f)(t)$ is a constant a_0 then

$$f(t) = a_0 t + a_1 = a_0 \binom{t}{1} + a_1 \binom{t}{0}.$$

The inductive hypothesis implies that

$$(\Delta f)(t) = \sum_{j=0}^{d-1} a_j \binom{t}{d-1-j}$$

for some $a_j \in \mathbb{Z}$. Set

$$Q(t) = \sum_{j=0}^{d-1} a_j \binom{t}{d-j}$$

so that $(\Delta Q) = (\Delta f)$ by our identity above. It follows that $f = Q + a_d$ for some constant $a_d \in \mathbb{Z}$ and f takes the desired form. $\square$

Theorem 12.14 (Existence of Hilbert polynomial) *Let $J \subset S = k[x_0, \ldots, x_n]$ be a homogeneous ideal and $R = k[x_0, \ldots, x_n]/J$. Then there exists a polynomial $\mathrm{HP}_R(t) \in \mathbb{Q}[t]$ such that*

$$\mathrm{HF}_R(t) = \mathrm{HP}_R(t), t \gg 0.$$

This is called the Hilbert polynomial *and takes the form (12.1).*

https://doi.org/10.1017/CBO9780511755224.013 Published online by Cambridge University Press

Proof If $J \subset S$ is an ideal, write

$$\mathrm{HF}_J(t) = \dim J_t = \binom{t+n}{n} - \mathrm{HF}_{S/J}(t).$$

Of course, $\mathrm{HF}_{S/J}(t)$ is a polynomial function for $t \gg 0$ if and only if $\mathrm{HF}_J(t)$ is a polynomial function for $t \gg 0$.

We may assume J is a monomial ideal by Proposition 12.12. The argument is by induction on n. The base case $n = 0$ is straightforward: if $J = \langle x_0^N \rangle$ then $\mathrm{HF}_J(t) = 1$ for $t \geq N$. For the inductive step, assume each monomial ideal in $S' = k[x_0, \ldots, x_{n-1}]$ has a Hilbert polynomial.

Define auxilliary ideals

$$J[m] = \left\{ f \in S' : f x_n^m \in J \right\}$$

so that

$$J[0] \subset J[1] \subset J[2] \subset \ldots.$$

This terminates at some $J[\infty]$ so that $J[m] = J[\infty]$ for $m \geq M$. Assume that $\mathrm{HF}_{J[\infty]}(t) = \mathrm{HP}_{J[\infty]}(t)$ whenever $t \geq N$.

We can write each element of J_t as a sum of terms $f_m x_n^m$ where $f_m \in J[m]_{t-m}$. Hence we have

$$J_t \simeq \oplus_{m=0}^{t} J[m]_{t-m} x_n^m$$

and, for $t \gg 0$,

$$\begin{aligned}
\mathrm{HF}_J(t) &= \sum_{m=0}^{t} \mathrm{HF}_{J[m]}(t-m) \\
&= \sum_{m=0}^{M-1} \mathrm{HF}_{J[m]}(t-m) + \sum_{m=M}^{t} \mathrm{HF}_{J[m]}(t-m) \\
&= \sum_{m=0}^{M-1} \mathrm{HF}_{J[m]}(t-m) + \sum_{m=M}^{t} \mathrm{HF}_{J[\infty]}(t-m) \\
&= \sum_{m=0}^{M-1} \mathrm{HF}_{J[m]}(t-m) + \sum_{m=M}^{t-N} \mathrm{HF}_{J[\infty]}(t-m) + \sum_{m=t-N+1}^{t} \mathrm{HF}_{J[\infty]}(t-m) \\
&\quad \text{(substituting } \mathrm{HF}_{J[\infty]}(s) = \mathrm{HP}_{J[\infty]}(s) \text{ for } s \geq N) \\
&= \sum_{m=0}^{M-1} \mathrm{HF}_{J[m]}(t-m) + \sum_{m=M}^{t-N} \mathrm{HP}_{J[\infty]}(t-m) + \sum_{m=t-N+1}^{t} \mathrm{HF}_{J[\infty]}(t-m) \\
&\quad \text{(substituting } \mathrm{HF}_{J[m]}(s) = \mathrm{HP}_{J[m]}(s) \text{ for } m = 0, \ldots, M-1, s \gg 0) \\
&= \sum_{m=0}^{M-1} \mathrm{HP}_{J[m]}(t-m) + \sum_{m=M}^{t-N} \mathrm{HP}_{J[\infty]}(t-m) + \sum_{m=t-N+1}^{t} \mathrm{HF}_{J[\infty]}(t-m) \\
&= \sum_{m=0}^{M-1} \mathrm{HP}_{J[m]}(t-m) + \sum_{j=N}^{t-M} \mathrm{HP}_{J[\infty]}(j) + \sum_{j=0}^{N-1} \mathrm{HF}_{J[\infty]}(j).
\end{aligned}$$

https://doi.org/10.1017/CBO9780511755224.013 Published online by Cambridge University Press

The first part is a finite sum of polynomials in t, hence is a polynomial in t. The third part is constant in t. As for the second part, write

$$f(t) := \sum_{j=N}^{t-M} \mathrm{HP}_{J[\infty]}(j)$$

and observe that

$$(\Delta f)(t) = f(t+1) - f(t) = \mathrm{HP}_{J[\infty]}(t+1-M)$$

is a polynomial in t. Proposition 12.13 implies f is also a polynomial in t. We conclude that $\mathrm{HF}_J(t)$ is a polynomial in t for $t \gg 0$. $\square$

Definition 12.15 Let $X \subset \mathbb{P}^n(k)$ be a projective variety. The *Hilbert polynomial* of X is defined

$$\mathrm{HP}_X(t) = \mathrm{HP}_{R(X)}$$

where $R(X) = k[x_0, \ldots, x_n/J(X)$.

In light of our previous results on Hilbert functions, we have

1. $\mathrm{HP}_X(t) = \binom{t+n}{n} - \binom{t-d+n}{n}$ when $J(X) = \langle F \rangle$ where $F \in k[x_0, \ldots, x_n]_d$;
2. $\mathrm{HP}_X(t)$ is invariant under projectivities;
3. $\mathrm{HP}_X(t) = \deg(F)\deg(G)$ when $J(X) = \langle F, G \rangle \subset k[x_0, x_1, x_2]$, where F and G are homogeneous with no common factors;
4. $\mathrm{HP}_S(t) = |S|$ for S finite;
5. $\mathrm{HP}_{\cup_j X_j}(t) = \sum_{j=1}^r \mathrm{HP}_{X_j}(t)$ when the X_j are pairwise disjoint and k is algebraically closed.

Example 12.16 Consider the ideal of the twisted cubic curve $C \subset \mathbb{P}^3(k)$

$$J(C) = \left\langle x_0x_2 - x_1^2, x_0x_3 - x_1x_2, x_1x_3 - x_2^2 \right\rangle,$$

which has leading term ideal (with respect to pure lexicographic order)

$$J = \langle x_0x_2, x_0x_3, x_1x_3 \rangle .$$

We have $J[0] = \langle x_0x_2 \rangle$ hence

$$\mathrm{HF}_{J[0]}(t) = \mathrm{HP}_{J[0]}(t) = \binom{t}{2}.$$

Furthermore,

$$J[m] = \langle x_0, x_1 \rangle = J[\infty]$$

for all $m \geq 1$ and

$$\mathrm{HF}_{J[\infty]}(t) = \mathrm{HP}_{J[\infty]}(t) = \binom{t+2}{2} - 1,$$

because $J[\infty]_t$ contains all monomials of degree t besides x_2^t. Thus we have

$$
\begin{aligned}
\mathrm{HF}_J(t) &= \sum_{j=0}^{t} \mathrm{HF}_{J[t-j]}(j) \\
&= \binom{t}{2} + \sum_{j=0}^{t-1}\left(\binom{j+2}{2} - 1\right) \\
&= \sum_{j=0}^{t}\binom{j+2}{2} - t + \binom{t}{2} - \binom{t+2}{2} \\
&= \binom{t+3}{3} - (3t+1)
\end{aligned}
$$

and $\mathrm{HP}_C(t) = 3t + 1$.

Proposition 12.17 *If $J \subset S = k[x_0, \ldots, x_n]$ is a homogeneous ideal with saturation $\tilde{J}$ then $\mathrm{HP}_{S/J}(t) = \mathrm{HP}_{S/\tilde{J}}(t)$.*

Proof Write $\mathfrak{m} = \langle x_0, \ldots, x_n \rangle$ so that

$$\tilde{J} = \{F \in k[x_0, \ldots, x_n] : F\mathfrak{m}^N \subset J \text{ for some N}\}.$$

The inclusion $J \subset \tilde{J}$ is obvious, so it suffices to show $\tilde{J}_t \subset J_t$ for $t \gg 0$. If $\tilde{J}$ is generated by homogeneous $F_1, \ldots, F_r$ then there exists an N such that $\mathfrak{m}^N F_i \subset J$ for $i = 1, \ldots, r$. For $t \geq \max_i\{\deg(F_i)\} + N$ we have $\tilde{J}_t \subset J_t$. □

12.3 Intersection multiplicities

How do we count the number of points where two varieties meet? We want this number to be constant even as the varieties vary in families. Such a method satisfies the *continuity principle.*

Example 12.18

1. Consider the complex plane curves $C_t = \{y = x^2 - t\}$ and $D = \{y = 0\}$. The intersection

$$C_t \cap D = \{(\pm\sqrt{t}, 0)\}$$

is two distinct points for $t \neq 0$ and one point for $t = 0$. This reflects the fact that C_0 is tangent to D at the origin.

2. Consider the complex plane curves $C_t = \{y = x^3 - tx\}$ and $D = \{y = 0\}$. The intersection

$$C_t \cap D = \{(0, 0), (\pm\sqrt{t}, 0)\}$$

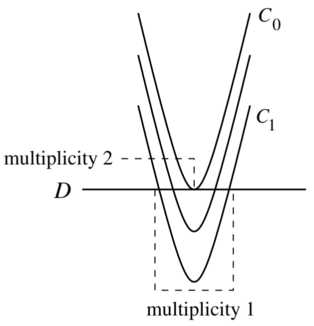

Figure 12.1 Intersections of families of plane curves.

is three distinct points for $t \neq 0$ and one point for $t = 0$. Note that D is an inflectional tangent to C_0 at the origin.

We now define the multiplicity: let $p = (a_1, \ldots, a_n) \in \mathbb{A}^n(k)$ and $\mathfrak{m}_p = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$ the corresponding maximal ideal. Let $Q \subset R := k[x_1, \ldots, x_n]$ be an ideal with

$$\mathfrak{m}_p^N \subset Q \subset \mathfrak{m}_p$$

for some N. Such ideals are precisely the primary ideals in R with associated prime $\mathfrak{m}_p$ (see Exercise 8.4). The induced quotient map $R/\mathfrak{m}_p^N \twoheadrightarrow R/Q$ is surjective and

$$\dim_k R/\mathfrak{m}_p^N = \dim_k k[x_1, \ldots, x_n]/\mathfrak{m}_p^N = \binom{n+N-1}{n},$$

so $\dim_k R/Q < \infty$. We define the *multiplicity* of Q at p by

$$\mathrm{mult}(Q, p) = \dim_k R/Q.$$

We extend this to more general classes of ideals $I \subset k[x_1, \ldots, x_n]$. Assume that $\mathfrak{m}_p$ is a minimal associated prime of I. Then the *multiplicity* of I at p is defined

$$\mathrm{mult}(I, p) = \mathrm{mult}(Q, p),$$

where Q is the primary component of I corresponding to $\mathfrak{m}_p$, which is unique by Theorem 8.32. If $\mathfrak{m}_p \not\supset I$ then we define $\mathrm{mult}(I, p) = 0$.

Remark 12.19 Assume that k is an algebraically closed field. Then $\mathfrak{m}_p$ is a minimal associated prime of I if and only if p is an irreducible component of $V(I)$ (by Corollary 8.29).

Definition 12.20 Let k be algebraically closed, $V_1, \ldots, V_n \subset \mathbb{A}^n(k)$ hypersurfaces with $I(V_i) = \langle f_i \rangle$, $i = 1, \ldots, n$. Suppose that p is an irreducible

https://doi.org/10.1017/CBO9780511755224.013 Published online by Cambridge University Press

component of $V_1 \cap \ldots \cap V_n$. The *multiplicity* of $V_1 \cap \ldots \cap V_n$ along p is defined as $\mathrm{mult}(\langle f_1, \ldots, f_n \rangle, p)$.

Example 12.21 We return to Example 12.18, computing the multiplicities of $C_t \cap D$ along each of the points of intersection:

In the first example

$$\begin{aligned} I_t &= \langle y, -y + x^2 - t \rangle = \langle y, -t + x^2 \rangle \\ &= \langle y, x - \sqrt{t} \rangle \cap \langle y, x + \sqrt{t} \rangle \\ &\quad \text{primary decomposition if } t \neq 0 \\ &= \langle y, x^2 \rangle \\ &\quad \text{primary decomposition if } t = 0. \end{aligned}$$

In the first instance each primary component has codimension 1, so the two points of intersection have multiplicity 1. In the second instance we have just one primary component with codimension 2, so there is a single intersection point of multiplicity 2.

In the second example

$$\begin{aligned} I_t &= \langle y, y - x^3 + tx \rangle = \langle y, -x^3 + tx \rangle \\ &= \langle y, x \rangle \cap \langle y, x + \sqrt{t} \rangle \cap \langle y, x - \sqrt{t} \rangle \\ &\quad \text{primary decomposition if } t \neq 0 \\ &= \langle y, x^3 \rangle \\ &\quad \text{primary decomposition if } t = 0. \end{aligned}$$

In the first instance each of the three intersection points has multiplicity 1; in the second, there is one point with multiplicity 3.

Example 12.22 Consider the ideal $I = \langle yx, (x-2)^2 x \rangle$ with primary decomposition

$$I = \langle x \rangle \cap \langle y, (x-2)^2 \rangle,$$

thus

$$V(I) = \{y - \text{axis}\} \cup \{(2, 0)\}.$$

The second component is associated with $\mathfrak{m}_p$ for $p = (2, 0)$ and $\mathrm{mult}(I, p) = 2$.

12.3.1 Methods for computing multiplicities

We describe an algorithm for computing intersection multiplicities. Let $I \subset k[x_1, \ldots, x_n]$ be an ideal, $p \in \mathbb{A}^n(k)$ a point, and $\mathfrak{m}_p$ the corresponding maximal ideal. Assume that $\mathfrak{m}_p$ is a minimal prime of I. Fix an irredundant primary decomposition

$$I = Q \cap Q_1 \cap \ldots \cap Q_l,$$

where is Q the primary component associated to $\mathfrak{m}_p$.

https://doi.org/10.1017/CBO9780511755224.013 Published online by Cambridge University Press

1. Localize to Q. Find some

$$f \in Q_1 \cap \ldots \cap Q_l$$

with $f \notin Q$, so that

$$Q = \langle uf - 1 \rangle + I.$$

We can interpret this geometrically when k is algebraically closed: throw out the irreducible components of $V(I)$ other than p.

2. Compute a Gröbner basis for Q: since $k[x_1, \ldots, x_n]/Q$ is finite dimensional, the monomials *not* appearing in $\mathrm{LT}(Q)$ form a basis for the quotient (Theorem 2.16). The number of these mononials equals $\mathrm{mult}(I, p)$.

Example 12.23 Consider the ideal

$$I = \langle y, y - x^2 + x^3 \rangle$$

so that $V(I) = \{(0,0), (1,0)\}$. To compute $\mathrm{mult}(I, (0,0))$ we first extract the primary component

$$Q_{(0,0)} = \langle u(x-1) - 1 \rangle + I = \langle u(x-1), y, y - x^2 + x^3 \rangle,$$

which has Gröbner basis

$$\{y, x^2, u + x + 1\}.$$

The monomials not in $\mathrm{LT}(Q_{(0,0)})$ are $\{1, x\}$ so $\mathrm{mult}(I, (0,0)) = 2$.

The primary component

$$Q_{(1,0)} = \langle ux - 1, y, y - x^2 + x^3 \rangle$$

has Gröbner basis

$$\{u - 1, x - 1, y\}.$$

The only monomial not in $\mathrm{LT}(Q_{(1,0)})$ is $\{1\}$ so $\mathrm{mult}(I, (1,0)) = 1$.

12.3.2 An interpolation result

Theorem 12.24 *Let $I \subset k[y_1, \ldots, y_n]$ be an ideal whose associated primes are all of the form $\mathfrak{m}_p$ for some $p \in \mathbb{A}^n(k)$. Then we have*

$$\dim k[y_1, \ldots, y_n]/I = \sum_{p \in V(I)} \mathrm{mult}(I, p).$$

Proof We fix some notation. Choose an irredundant primary decomposition

$$I = Q_1 \cap \ldots \cap Q_s$$

https://doi.org/10.1017/CBO9780511755224.013 Published online by Cambridge University Press

with associated primes $\mathfrak{m}_{p_1}, \ldots, \mathfrak{m}_{p_s}$. We have the linear transformation

$$\begin{aligned}\Pi : k[y_1, \ldots, y_n] &\to \oplus_{j=1}^{s} k[y_1, \ldots, y_n]/Q_j \\ f &\to (f(\bmod\ Q_1), \ldots, f(\bmod\ Q_s)).\end{aligned}$$

It suffices to show Π is surjective: since $\ker \Pi = I$, the definition of the multiplicity and the rank-nullity theorem yield our result.

Recall that for large N each $Q_j \supset \mathfrak{m}_{p_j}^N$, so the quotients

$$k[y_1, \ldots, y_n]/\mathfrak{m}_{p_j}^N \to k[y_1, \ldots, y_n]/Q_j$$

are surjective. Thus Π is surjective provided

$$\begin{aligned}\Psi : k[y_1, \ldots, y_n] &\to \oplus_{j=1}^{s} k[y_1, \ldots, y_n]/\mathfrak{m}_{p_j}^N \\ f &\to \left(f\ \left(\bmod\ \mathfrak{m}_{p_1}^N\right), \ldots, f\ \left(\bmod\ \mathfrak{m}_{p_s}^N\right)\right)\end{aligned}$$

is surjective. This means there exists a polynomial with prescribed Taylor series of order N at the points $p_1, \ldots, p_s$ (at least over a field of characteristic zero where Taylor series make sense). Note that the $N = 1$ case, i.e., finding a polynomial with prescribed values on a finite set, was addressed in Exercise 3.6.

The proof is by induction on the number of points s. The base case $s = 1$ is straightforward, since after translation we may assume p_1 is the origin. For the inductive step, consider the polynomials mapping to zero in

$$k[y_1, \ldots, y_n]/\mathfrak{m}_{p_j}^N$$

for $j = 1, \ldots, s-1$, which form an ideal $\tilde{I}$. It suffices to show that the induced map

$$\Psi_s : \tilde{I} \to k[y_1, \ldots, y_n]/\mathfrak{m}_{p_s}^N$$

is surjective. The image of Ψ_s is an ideal, so it suffices to check it contains a unit, i.e., an element that does not vanish at p_s. Let $\ell_i, i = 1, \ldots, s-1$, be linear forms with $\ell_i(p_i) = 0$ by $\ell_i(p_s) \neq 0$. The polynomial

$$P = \prod_{j=1}^{s-1} \ell_j^N \in \tilde{I}$$

but $P(p_s) \neq 0$. □

12.4 Bezout Theorem

Our first task is to analyze ideals with constant Hilbert polynomial:

Proposition 12.25 *Let $J \subset k[x_0, \ldots, x_n]$ be a homogeneous ideal and $R = k[x_0, \ldots, x_n]/J$. If $\mathrm{HP}_R(t)$ has degree zero then $X(J)$ is finite.*

https://doi.org/10.1017/CBO9780511755224.013 Published online by Cambridge University Press

Proof Suppose $X(J)$ is infinite. Then one of the distinguished open sets $U_i \subset \mathbb{P}^n(k)$ (say U_0) contains an infinite number of points in $X(J)$. Let $I \subset k[y_1, \ldots, y_n]$ be the dehomogenization of J with respect to x_0, which is contained in $I(U_0 \cap X(J)$. We therefore have surjections

$$k[x_0, \ldots, x_n]/J \stackrel{\mu_0}{\to} k[y_1, \ldots, y_n]/I \to k[U_0 \cap X(J)].$$

For each t, write

$$W_t = \mathrm{image}(R_t = k[x_0, \ldots, x_n]_t/J_t \to k[U_0 \cap X(J)]),$$

i.e., the functions on $U_0 \cap X(J)$ that can be realized as polynomials of degree $\leq t$. We have $\dim W_t \leq \dim R_t$.

By Exercise 3.6, $\dim_k k[U_0 \cap X(J)] = |U_0 \cap X(J)| = \infty$ and W_t is unbounded for $t \gg 0$. On the other hand, $\dim R_t$ is bounded because $\mathrm{HP}_R(t)$ is constant, a contradiction. □

Over algebraically closed fields, we can sharpen this:

Proposition 12.26 *Suppose k is algebraically closed, $J \subset k[x_0, \ldots, x_n]$ is a homogeneous ideal with $R = k[x_0, \ldots, x_n]/J$, and $\mathrm{HP}_R(t)$ is constant and nonzero. Then the minimal associated primes of J are the ideals $J(p)$ for $p \in X(J) \subset \mathbb{P}^n(k)$.*

Proof Irrelevant ideals yield trivial Hilbert polynomials (Proposition 12.17), so our hypothesis guarantees J is not irrelevant. The Projective Nullstellensatz (Theorem 9.25) then guarantees that $X(J)$ is nonempty.

Lemma 12.27 *If $J \subset k[x_0, \ldots, x_n]$ is homogeneous then each associated prime of J is homogeneous.*

We can put this into geometric terms using Corollary 8.29. Recall that $V(J) \subset \mathbb{A}^{n+1}(k)$ is the cone over the projective variety $X(J)$. Irreducible components of $V(J)$ correspond to the cones over irreducible components of $X(J)$.

Proof of lemma By Theorem 8.22, each associated prime of J can be written $P = \sqrt{J : f}$ for some $f \in k[x_0, \ldots, x_n]$. Write $f = F_0 + \cdots + F_d$ as a sum of homogeneous pieces and $K_i = \sqrt{J : F_i}$. Since J is homogeneous,

$$J : f = J : F_0 \cap J : F_1 \cap \ldots \cap J : F_d$$

and Exercise 7.18 gives

$$\sqrt{J : f} = \sqrt{J : F_0} \cap \sqrt{J : F_1} \cap \ldots \cap \sqrt{J : F_d}.$$

Since prime ideals are irreducible (Proposition 8.4), $P = \sqrt{J : F_i}$ for some i, and thus is homogeneous. □

https://doi.org/10.1017/CBO9780511755224.013 Published online by Cambridge University Press

Each irreducible component of $X(J)$ is a point $p \in \mathbb{P}^n(k)$ (by Proposition 12.25). Thus each irreducible component of $V(J)$ is the line $\ell \subset \mathbb{A}^{n+1}(k)$ parametrized by that point. The description of the minimal associated primes of J follows. □

Corollary 12.28 *Retain the assumptions of Proposition 12.26 and assume in addition that J is saturated. Then the associated primes of J are the ideals $J(p)$ for $p \in X(J)$.*

Proof The only possible embedded prime is $\mathfrak{m} = \langle x_0, \ldots, x_n \rangle$, which would correspond to an irrelevant primary component. In the saturated case, these do not occur (see Exercise 10.2). □

Our next task is to tie Hilbert polynomials and multiplicities together. We start with a fun fact from linear algebra:

Lemma 12.29 *Assume k is infinite and let $S \subset \mathbb{P}^n(k)$ be a finite set. Then there exists a linear $L \in k[x_0, \ldots, x_n]_1$ such that $L(p) \neq 0$ for each $p \in S$.*

Proof First, we construct an infinite collection of points $p_1, p_2, \ldots, p_N, p_{N+1}, \ldots$ in $\mathbb{P}^n(k)$ such that any $n+1$ of the points are in linear general position. Given distinct $\alpha_1, \alpha_2, \ldots \in k$ set

$$p_i = [1, \alpha_i, \alpha_i^2, \ldots, \alpha_i^n] \in \mathbb{P}^n(k).$$

Recall the formula for determinant of the *Vandermonde matrix*

$$\det \begin{pmatrix} 1 & u_0 & u_0^2 & \ldots & u_0^n \\ 1 & u_1 & u_1^2 & \ldots & u_1^n \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & u_{n-1} & u_{n-1}^2 & \ldots & u_{n-1}^n \\ 1 & u_n & u_n^2 & \ldots & u_n^n \end{pmatrix} = \prod_{0 \leq i < j \leq n} (u_j - u_i).$$

In particular, the determinant is nonzero unless $u_i = u_j$ for some $i \neq j$. Taking $u_0, \ldots, u_n$ to be any of $n+1$ distinct values of the α_i, we get the desired linear independence. In geometric terms, the images of any collection of distinct points in $\mathbb{P}^1(k)$ under the Veronese embedding

$$\nu_n : \mathbb{P}^1(k) \to \mathbb{P}^n(k)$$

are in linear general position.

There exists then a collection of $n+1$ points in $\mathbb{P}^n(k)$ in linear general position, but not contained in S. There exists a projectivity taking these to the coordinate vectors

$$e_0 = [1, 0, \ldots, 0], e_1 = [0, 1, 0, \ldots, 0], \ldots, e_n = [0, \ldots, 0, 1].$$

We may then assume that S does not include any of these points.

https://doi.org/10.1017/CBO9780511755224.013 Published online by Cambridge University Press

We finish by induction on n. Suppose $n = 1$ and $S = \{(a_1, b_1), \ldots, (a_N, b_N)\}$. If $t \in k$ is distinct from each b_j/a_j then $L = x_1 - tx_0$ has the desired property. For the inductive step, project from $e_n = [0, \ldots, 0, 1]$

$$\begin{aligned}\pi_{e_n} : \mathbb{P}^n(k) &\dashrightarrow \mathbb{P}^{n-1}(k) \\ [x_0, \ldots, x_n] &\mapsto [x_0, \ldots, x_{n-1}],\end{aligned}$$

which is well-defined along S. By induction, there exists $L \in k[x_0, \ldots, x_{n-1}]_1$ that is nonzero at each point of $\pi_{e_n}(S)$. Regarding $L \in k[x_0, \ldots, x_n]$, we get a form non-vanishing at each point of S. □

Our next task is to explain how Hilbert polynomials and multiplicities are related.

Proposition 12.30 *Suppose k is algebraically closed, $J \subset k[x_0, \ldots, x_n]$ is a homogeneous ideal with $R = k[x_0, \ldots, x_n]/J$, and $\mathrm{HP}_R(t)$ is constant. Assume in addition that $X(J) \subset U_0$. If $I \subset k[y_1, \ldots, y_n]$ denotes the dehomogenization of J then*

$$\sum_{p \in X(J) = V(I)} \mathrm{mult}(I, p) = \mathrm{HP}_R(t).$$

Proof We may replace J by its saturation without changing either the Hilbert polynomial or the dehomogenization (see Proposition 12.17). From now on, we assume that J is saturated.

Proposition 12.25 implies that $X(J)$ finite and consequently $V(I)$ is finite. The minimal associated primes of I are all of the form $\mathfrak{m}_p$, where $p \in V(I)$ (see Corollary 8.29). Our interpolation result (Theorem 12.24) implies

$$\dim_k k[y_1, \ldots, y_n]/I = \sum_{p \in I} \mathrm{mult}(I, p).$$

Again, consider the dehomogenizations

$$R := k[x_0, \ldots, x_n]/J \stackrel{\mu_0}{\to} k[y_1, \ldots, y_n]/I$$

and the images of the induced

$$R_t := k[x_0, \ldots, x_n]_t/J_t \to k[y_1, \ldots, y_n]/I$$

for each t. We claim that these are isomorphisms for $t \gg 0$, which implies our result.

Surjectivity is not too difficult. The quotient $k[y_1, \ldots, y_n]/I$ has finite dimension, with a basis consisting of monomials of bounded degree. To prove injectivity, suppose that F is homogeneous of degree d and dehomogenizes to a polynomial $f \in I$. This is the dehomogenization of some homogeneous $F' \in J$, with $F' = x_0^e F$ for some e.

https://doi.org/10.1017/CBO9780511755224.013 Published online by Cambridge University Press

To show that F is also in J, we establish that the multiplication map

$$\begin{aligned} R_t &\to R_{t-1} \\ F &\mapsto x_0 F \end{aligned}$$

is injective.

Corollary 12.28 gives the primary decomposition of J. If $X(J) = \{p_1, \ldots, p_s\}$ then

$$J = Q_1 \cap \ldots \cap Q_s,$$

where Q_i is associated to $P_i := J(p_i)$ for $i = 1, \ldots, s$. However, $x_0(p_i) \neq 0$ for each i by assumption, so $x_0 \notin P_i$. The only zero divisors in R are in the images of the associated primes of J (Corollary 8.24); thus x_0 is not a zero divisor in R. □

Theorem 12.31 (Bezout Theorem) *Let k be an algebraically closed field, $F, G \in k[x_0, x_1, x_2]$ homogeneous polynomials without common factors, and $J = \langle F, G \rangle$. There exist coordinates z_0, z_1, z_2 such that $z_0(p) \neq 0$ for each $p \in X(J)$. If I is the dehomogenization of J with respect to z_0 then*

$$\sum_{p \in X(J)} \text{mult}(I, p) = \deg(F) \deg(G).$$

Proof Lemma 12.29 guarantees the existence of coordinates with the desired property. Then the theorem is just the combination of Propositions 12.11 and 12.30. □

Corollary 12.32 *Two plane curves of degrees d and e with no common components meet in de points, when counted with multiplicities.*

Étienne Bézout (1733–1783) wrote the *Théorie générale des équations algébraiques* in 1779. An English translation [3] was published in 2006.

12.4.1 Higher-dimensional generalizations

Theorem 12.33 *Let $F_1, \ldots, F_n$ be homogeneous in $S = k[x_0, x_1, \ldots, x_n]$, $J = \langle F_1, \ldots, F_n \rangle$, and $R = S/J$. Suppose either of the following equivalent conditions holds*

1. *for each $j = 2, \ldots, n$, F_j is not a zero divisor* $\pmod{\langle F_1, \ldots, F_{j-1} \rangle}$*;*
2. *$X(J)$ has a finite number of points over an algebraically closed field.*

Then we have

$$\text{HP}_R(t) = \deg(F_1) \ldots \deg(F_n).$$

https://doi.org/10.1017/CBO9780511755224.013 Published online by Cambridge University Press

Idea of proof Let d_j denote the degree of F_j. The computation of $\mathrm{HP}_R(t)$ requires knowledge of the *Koszul complex*

$$0 \to K_n \stackrel{\delta_n(t)}{\to} K_{n-1} \dots K_r \stackrel{\delta_r(t)}{\to} K_{r-1} \dots K_0 \stackrel{\delta_0}{\to} R_t \to 0.$$

Here the terms are

$$\begin{aligned}
K_0 &= S_t \\
K_1 &= \textstyle\sum_j S_{t-d_j} \\
K_2 &= \textstyle\sum_{j(1)<j(2)} S_{t-d_{j(1)}-d_{j(2)}} \\
\vdots\ &\quad \vdots \\
K_r &= \textstyle\sum_{j(1)<j(2)<\dots<j(r)} S_{t-d_{j(1)}-\dots-d_{j(r)}} \\
\vdots\ &\quad \vdots \\
K_n &= S_{t-d_1-\dots-d_n}
\end{aligned}$$

and the maps $\delta_r(t)$ are direct sums of multiplication maps

$$\begin{aligned}
S_{t-d_{j(1)}-\dots-d_{j(r)}} &\to S_{t-d_{j(1)}-\dots-d_{j(s-1)}-d_{j(s+1)}-\dots-d_{j(r)}} \\
G &\mapsto (-1)^s F_{j(s)} G.
\end{aligned}$$

The signs are chosen so that image $\delta_r(t) \subset \ker\, \delta_{r-1}(t)$ for each r; see §5.4 for a special case.

Under our assumptions, the only syzygies among the F_j are the 'obvious' ones, e.g., $F_i(F_j) - F_j(F_i) = 0$. In this context, the Koszul complex is exact, i.e., the kernel of each map equals the image of the one before. We then have

$$\begin{aligned}
\dim R_t &= \sum_{r=0}^{n} (-1)^r \sum_{j(1)<\dots<j(r)} \dim S_{t-d_{j(1)}-\dots-d_{j(r)}} \\
&= \sum_{r=0}^{n} (-1)^r \sum_{j(1)<\dots<j(r)} \binom{t-d_{j(1)}-\dots-d_{j(r)}+n}{n} \\
&= d_1 \dots d_n,
\end{aligned}$$

where the last step is a formal combinatorial identity. □

This granted, our proof of Theorem 12.31 yields the following.

Theorem 12.34 (Higher-dimensional Bezout Theorem) *Let k be an algebraically closed field, $F_1, \dots, F_n \in k[x_0, \dots, x_n]$ homogeneous polynomials, and let $J = \langle F_1, \dots, F_n \rangle$. Assume that $X(J)$ is finite and $x_0(p) \neq 0$ for each $p \in X(J)$. If I is the dehomogenization of J with respect to x_0 then*

$$\sum_{p \in X(J)} \mathrm{mult}(I, p) = \prod_{i=1}^{n} \deg(F_i).$$

https://doi.org/10.1017/CBO9780511755224.013 Published online by Cambridge University Press

12.4.2 An application to inflectional tangents

Let $C \subset \mathbb{P}^2(\mathbb{C})$ be a smooth plane curve over the complex numbers with homogeneous equation $F \in \mathbb{C}[x, y, z]$ of degree d.

A line $\ell \subset \mathbb{P}^2$ is *tangent* to C at p if the multiplicity of $\ell \cap C$ at p is greater than or equal to 2. It is an *inflectional tangent* to C at p if the multiplicity is greater than or equal to 3. In our discussion of the Plücker formulas in §11.2.1, we observed that the number of inflectional tangents to C equals the number of cusps in the dual curve $\check{C}$.

How do we count the number of inflectional tangents? Recall that the dual curve is the image of the morphism

$$\begin{aligned} \phi : C &\to \check{\mathbb{P}}^2 \\ [x, y, z] &\to [\partial F/\partial x, \partial F/\partial y, \partial F/\partial z]. \end{aligned}$$

The inflectional tangents are precisely the critical points of this map. The differential of ϕ has nontrivial kernel when the *Hessian*

$$H(F) = \det \begin{pmatrix} \frac{\partial^2 F}{\partial x^2} & \frac{\partial^2 F}{\partial x \partial y} & \frac{\partial^2 F}{\partial x \partial z} \\ \frac{\partial^2 F}{\partial x \partial y} & \frac{\partial^2 F}{\partial y^2} & \frac{\partial^2 F}{\partial y \partial z} \\ \frac{\partial^2 F}{\partial x \partial z} & \frac{\partial^2 F}{\partial y \partial z} & \frac{\partial^2 F}{\partial z^2} \end{pmatrix} = 0.$$

This is a polynomial of degree $3(d-2)$. We conclude therefore that

$$\begin{aligned} \#\{\text{inflectional tangents of } C\} &= \#\{\text{critical points of } \phi : C \to \check{\mathbb{P}}^2\} \\ &= \#\{\text{solutions of } F = H(F) = 0\} \\ &= 3d(d-2), \end{aligned}$$

where the last equality is the Bezout Theorem. We obtain the following table:

$\deg(F)$	#{inflectional tangents}
2	0
3	9
4	24
5	45

The Bezout Theorem counts intersection points with multiplicity. The points where C intersects $\{H(F) = 0\}$ with multiplicity > 1 include inflectional tangent ℓ meeting C with multiplicity ≥ 4.

For more information on multiplicities and plane curves, see [11].

12.5 Interpolation problems revisited

We apply some of these ideas to the interpolation problem first considered in Chapter 1. Before stating the General Interpolation Problem, we need a definition:

https://doi.org/10.1017/CBO9780511755224.013 Published online by Cambridge University Press

Definition 12.35 Let $f \in k[y_1, \ldots, y_n]$ and $p = (b_1, \ldots, b_n) \in \mathbb{A}^m(k)$. The polynomial f has *multiplicity* $\geq m$ *at* p (or *vanishes to order* m *at* p) if

$$f \in \mathfrak{m}_p^m = \langle y_1 - b_1, \ldots, y_n - b_n \rangle^m.$$

When k has characteristic zero, this means the the Taylor series for f at p only has terms of degree $\geq m$.

Problem 12.36 (General Interpolation Problem) Fix interpolation data

$$\mathcal{S} = (p_1, m_1; \ldots; p_N, m_N)$$

consisting of distinct points $p_1, \ldots, p_N \in \mathbb{A}^n(k)$ and positive integers $m_1, \ldots, m_N$. What is the dimension of the vector space of polynomials of degree $\leq d$ vanishing at each p_i to order m_i?

Let $P_{n,d}$ denote the polynomials of degree $\leq d$ and

$$I_d(\mathcal{S}) = P_{n,d} \cap \left(\cap_{j=1}^N \mathfrak{m}_{p_j}^{m_j} \right)$$

denote the polynomials satisfying the interpolation data.

Definition 12.37 The number of conditions imposed by

$$\mathcal{S} = (p_1, m_1; \ldots; p_N, m_N)$$

on polynomials of degree $\leq d$ is defined as

$$C_d(\mathcal{S}) := \dim P_{n,d} - \dim I_d(\mathcal{S}).$$

$\mathcal{S}$ is said to *impose independent conditions on* $P_{n,d}$ if

$$C_d(\mathcal{S}) = \sum_{j=1}^N \binom{n + m_j - 1}{n}.$$

It *fails to impose independent conditions* otherwise.

The expected number of conditions is given by naively counting the Taylor coefficients we set equal to zero!

Fix N and $m_1, \ldots, m_N$. It may not be possible to choose $p_1, \ldots, p_N$ such that the data $\mathcal{S}$ impose independent conditions on $P_{n,d}$. There are counterexamples even when the expected number of conditions is less than the dimension:

$$\sum_{j=1}^N \binom{n + m_j - 1}{n} \leq \binom{n+d}{n}.$$

Example 12.38

1. Let $p_1 = (0, 0)$, $p_2 = (1, 0) \in \mathbb{A}^2(k)$ and consider the conditions imposed by $(p_1, 2; p_2, 2)$ on quadrics. Since x_2^2 vanishes to order 2 at p_1 and p_2, we have

$$C_2(\mathcal{S}) \leq 6 - 1 = 5.$$

On the other hand,

$$2\binom{2+2-1}{2} = 6.$$

2. Let $p_1, \ldots, p_5 \in \mathbb{A}^2(k)$ and consider the conditions imposed by

$$(p_1, 2; p_2, 2; p_3, 2; p_4, 2; p_5, 2)$$

on quartics ($d = 4$). There is a unique (up to scalar) nonzero $f \in P_{2,2}$ such that f vanishes at each of the p_j. Hence $f^2 \in P_{2,4}$ vanishes to order 2 at each of the p_j and $C_4(\mathcal{S}) \leq 15 - 1 = 14$. However, the expected number of conditions is

$$5\binom{2+2-1}{2} = 15.$$

We recast these problems using Hilbert functions and polynomials. Realize $\mathbb{A}^n(k)$ as the distinguished affine open $U_0 \subset \mathbb{P}^n(k)$ and consider $p_1, \ldots, p_N \in \mathbb{P}^n(k)$. We write $S = k[x_0, \ldots, x_n]$. Dehomogenization with respect to x_0

$$\mu_0 : k[x_0, \ldots, x_n] \to k[y_1, \ldots, y_m]$$

identifies $J(p_i)$ with $\mathfrak{m}_{p_i}$ and S_d with $P_{n,d}$. Homogeneous forms of degree d with multiplicity m_j at each p_j (cf. Exercise 10.8) are identified with $I_d(\mathcal{S})$. Writing

$$J(\mathcal{S}) = \cap_{j=1}^N J(p_i)^{m_i}, \quad R(\mathcal{S}) = S/J(\mathcal{S}),$$

we have an isomorphism

$$\mu_0 : R(\mathcal{S})_d \xrightarrow{\sim} P_{n,d}/I_d(\mathcal{S})$$

and thus the equality

$$\mathrm{HF}_{R(\mathcal{S})}(d) = C_d(\mathcal{S}).$$

Proposition 12.39 *Let $\mathcal{S} = (p_1, m_1; \ldots; p_N, m_n)$ be a collection of distinct points in $\mathbb{P}^n(k)$ and positive integers $m_1, \ldots, m_N$. Write*

$$J(\mathcal{S}) = \cap_{j=1}^N J(p_i)^{m_i}, \quad R(\mathcal{S}) = S/J(\mathcal{S}).$$

https://doi.org/10.1017/CBO9780511755224.013 Published online by Cambridge University Press

Then we have

$$\mathrm{HP}_{R(\mathcal{S})}(t) = \sum_{j=1}^{N} \binom{n+m_j-1}{n}.$$

Proof Let $p = [0, \ldots, 0, 1] \in \mathbb{P}^n(k)$ so that $J(p) = \langle x_0, \ldots, x_{n-1} \rangle$ and the monomials

$$\left\{ x_0^{\alpha_0} \ldots x_{n-1}^{\alpha_{n-1}} x_n^{\alpha_n} : \alpha_0 + \cdots + \alpha_{n-1} < m \right\}$$

form a basis for $S/J(p)^m$. It follows that

$$\mathrm{HF}_{S/J(p)^m}(t) = \binom{n+m-1}{n}$$

for $t \geq m$. By Proposition 12.5, this analysis applies to each $p \in \mathbb{P}^n(k)$; Proposition 12.6 the gives the result. □

Corollary 12.40 *Consider interpolation data $\mathcal{S} = (p_1, m_1; \ldots; p_N, m_N)$ in $\mathbb{P}^n(k)$ and the corresponding graded ring $R(\mathcal{S})$. $\mathcal{S}$ imposes independent conditions on polynomials of degree $\leq d$ if and only if $\mathrm{HP}_{R(\mathcal{S})}(d) = \mathrm{HF}_{R(\mathcal{S})}(d)$. Thus $\mathcal{S}$ imposes independent conditions on polynomials of degree $\leq t$ provided $t \gg 0$.*

The last assertion is the defining property of the Hilbert polynomial (Theorem 12.14). Thus our General Interpolation Problem reduces to the following.

Problem 12.41 (Projective Interpolation Problem) Fix interpolation data

$$\mathcal{S} = (p_1, m_1; \ldots; p_N, m_N)$$

consisting of distinct points $p_1, \ldots, p_N \in \mathbb{P}^n(k)$ and positive integers $m_1, \ldots, m_N$. If we write

$$J(\mathcal{S}) = \cap_{j=1}^{N} J(p_i)^{m_i}, \quad R(\mathcal{S}) = k[x_0, \ldots, x_n]/J(\mathcal{S}),$$

for which t is

$$\mathrm{HF}_{R(\mathcal{S})}(t) = \mathrm{HP}_{R(\mathcal{S})}(t)?$$

Lemma 12.29 implies we can always choose coordinates such that $p_1, \ldots, p_N \in U_0 \simeq \mathbb{A}^n(k)$, so the Projective Interpolation Problem reduces to the affine case.

Even for generic points in the plane, the General Interpolation Problem is still open! There are precise conjectures of Hirschowitz [21] and Harbourne [15, 16] predicting which interpolation data fail to impose independent conditions on polynomials of degree $\leq d$. A good survey can be found in [31].

12.6 Classification of projective varieties

The importance of the Hilbert polynomial is that most important invariants of projective varieties can be defined in terms of it.

Definition 12.42 Let X be a projective variety.

1. The *dimension* $\dim(X)$ is defined as the degree of HP_X.
2. The *degree* of $\deg(X)$ defined as the normalized leading term of HP_X:

$$\mathrm{HP}_X(t) = \frac{\deg(X)}{\dim(X)!} t^{\dim(X)} + \text{ lower-order terms.}$$

In our discussion of Hilbert polynomials, we showed that each can be expressed in the form

$$\mathrm{HP}_X(t) = \sum_{i=0}^{\dim(X)} a_i \binom{t}{\dim(X) - i},$$

with the a_i integers. The coefficient $a_0 = \deg(X)$.

These definitions can be related to existing notions of 'dimension' and 'degree', when these can be easily formulated. A finite set X has dimension zero and degree $|X|$. Projective space $\mathbb{P}^n(k)$ has dimension n and degree 1. As for hypersurfaces, the following holds.

Proposition 12.43 *Let $X \subset \mathbb{P}^n(k)$ be a hypersurface with $J(X) = \langle F \rangle$, with F a polynomial of degree d. Then $\dim(X) = n - 1$ and $\deg(X) = d$.*

Proof We have already computed the Hilbert polynomial

$$\begin{aligned}
\mathrm{HP}_X(t) &= \binom{t+n}{n} - \binom{t-d+n}{n} \\
&= \frac{(t+n)(t+n-1)\ldots(t+1)}{n!} - \frac{(t-d+n)\ldots(t+1-d)}{n!} \\
&= t^{n-1} \frac{n + (n-1) + \cdots + 1 - (n-d) - (n-1-d) - \cdots - (1-d)}{n!} \\
&\quad + \text{lower-order terms} \\
&= t^{n-1} \frac{nd}{n!} + \text{ lower-order terms.}
\end{aligned}$$

In particular, the Hilbert polynomial has degree $n - 1$ and $a_0 = d$. □

It takes some work to prove in general that the Hilbert-polynomial definition of dimension agrees with the transcendence-base definition given in Chapter 7. See [9, ch. 8] for a discussion of the various notions of dimension.

Not only the leading term of the Hilbert polynomial gets a special name. The constant term is also significant:

https://doi.org/10.1017/CBO9780511755224.013 Published online by Cambridge University Press

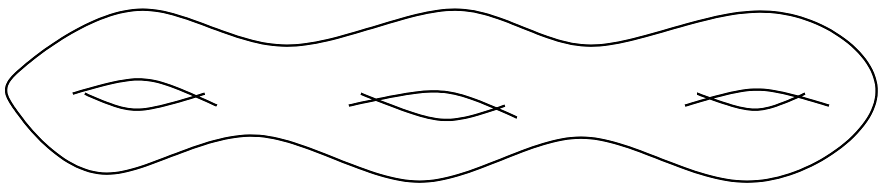

Figure 12.2 A curve of genus 3.

Definition 12.44 The *arithmetic genus* of an irreducible projective variety X is defined as

$$p_a(X) = (-1)^{\dim(X)}(\mathrm{HP}_X(0) - 1).$$

Example 12.45

1. The curve $X \subset \mathbb{P}^3(k)$ with equations

$$\{x_0x_2 - x_1^2, x_0x_3 - x_1x_2, x_2^2 - x_1x_3\}$$

has $\deg(X) = 3$, $p_a(X) = 0$.

2. Let $X \subset \mathbb{P}^2(k)$ be a plane curve of degree d. Then we have

$$\begin{aligned}\mathrm{HP}_X(t) &= \binom{t+2}{2} - \binom{t-d+2}{2} \\ &= dt + \left[1 - \frac{(d-1)(d-2)}{2}\right]\end{aligned}$$

so that $p_a(X) = (d-1)(d-2)/2$.

The geometric meaning of the arithmetic genus is a bit elusive in general. However, for curves it has a very nice geometric interpretation.

Theorem 12.46 *Let $X \subset \mathbb{P}^n(\mathbb{C})$ be a smooth irreducible complex projective curve. Then $X(\mathbb{C})$ is an oriented compact Riemann surface of genus $p_a(X)$.*

The proof, which uses the Riemann–Roch Theorem and significant analysis, would take us too far afield. We refer the interested reader to a book on complex Riemann surfaces, e.g., [30, p. 192].

Example 12.47 Consider the plane curve $X \subset \mathbb{P}^2(\mathbb{C})$ given by the equations $x_0^4 + x_1^4 = x_2^4$. This is smooth (and thus irreducible by the Bezout Theorem!) with genus

$$\frac{3 \cdot 2}{2} = 3.$$

The complex points $X(\mathbb{C})$ are displayed in Figure 12.2.

We sketch briefly how projective varieties are classified using Hilbert polynomials. Fix a polynomial $f(t) \in \mathbb{Q}[t]$ with $f(\mathbb{Z}) \subset \mathbb{Z}$, and consider all varieties $X \subset \mathbb{P}^n$ with $\mathrm{HP}_X(t) = f(t)$. Choose $M \gg 0$ such that $\mathrm{HP}_X(M) = f(M)$; while it appears that M depends on X, it is possible to choose a uniform value for all the varieties with Hilbert polynomial f. Let

$$\mathrm{Gr} := \mathrm{Gr}(\binom{n+M}{M} - f(M), k[x_0, \ldots, x_n]_M)$$

denote the Grassmannian of codimension-$f(M)$ subspaces of the space of polynomials of degree M. The homogeneous polynomials of degree M vanishing on X define a point

$$[X]_M := J(X)_M \in \mathrm{Gr}.$$

For $M \gg 0$, the set of all projective varieties with Hilbert polynomial f are parametrized by a locus

$$\mathcal{H}ilb_{f(t)} \subset \mathrm{Gr}$$

known as the *Hilbert scheme*. For details on the construction and discussion of $\mathcal{H}ilb_{f(t)}$ as a projective variety see [32, ch. 14].

Example 12.48 Consider all plane curves $X \subset \mathbb{P}^2(k)$ of degree d. These have Hilbert polynomial

$$f(t) = \binom{t+2}{2} - \binom{t-d+2}{2}$$

so that $f(d) = \binom{2+d}{d} - 1$. If X is defined by $F \in k[x_0, x_1, x_2]_d$ then

$$[X]_d = [F] \in \mathrm{Gr}(1, k[x_0, x_1, x_2]_d) = \mathbb{P}^{\binom{d+2}{2}-1}.$$

A similar analysis applies to arbitrary hypersurfaces of degree d in $\mathbb{P}^n$.

12.7 Exercises

12.1 Consider the ideal

$$J = \langle x_0 x_1, x_2^2 \rangle \subset k[x_0, x_1, x_2].$$

Compute the Hilbert polynomial $\mathrm{HP}_J(t)$.

12.2 Let $f = x^3 + y^3$ and $g = x^4 + y^5$ and write

$$I = \langle f, g \rangle, \quad p = (0, 0).$$

Compute the multiplicity $\mathrm{mult}(I, p)$.

https://doi.org/10.1017/CBO9780511755224.013 Published online by Cambridge University Press

12.3 Consider the interpolation data $\mathcal{S} = ((0,0), 2; (0,1), 2; (1,0), 2)$ for $\mathbb{A}^2(\mathbb{R})$. Show that this imposes independent conditions on polynomials in $P_{2,3}$.

12.4 (a) Let $p_1, \ldots, p_7$ be any distinct points in $\mathbb{A}^2(\mathbb{R})$. Show that there exists a nonzero cubic polynomial vanishing at p_1 to order 2 and at $p_2, \ldots, p_7$ to order 1.

(b) Compute the expected number of conditions $C_6(\mathcal{S})$ imposed on $P_{2,6}$ by the interpolation data

$$\mathcal{S} = (p_1, 4; p_2, 2; p_3, 2; p_4, 2; p_5, 2; p_6, 2; p_7, 2)$$

for generic points $p_1, \ldots, p_7 \in \mathbb{A}^2(\mathbb{R})$.

(c) Show that $\mathcal{S}$ fails to impose independent conditions on $P_{2,6}$.

12.5 Compute Hilbert polynomials for the following varieties:

(a) the quadratic Veronese varieties

$$\nu(2)(\mathbb{P}^n(k)) \subset \mathbb{P}^{\binom{n+2}{2}-1}(k);$$

(b) the Segre variety

$$X = \mathbb{P}^m(k) \times \mathbb{P}^m(k) \subset \mathbb{P}^{nm+n+m}(k);$$

(c) the Grassmannian

$$\mathrm{Gr}(2,4) \subset \mathbb{P}^5(k).$$

Compute the degree and dimension from the Hilbert polynomial.

12.6 Let $X = \{p_1, p_2, p_3, p_4\} \subset \mathbb{P}^2(\mathbb{Q})$ be a collection of four distinct points. List all possible Hilbert functions $\mathrm{HF}_X(t)$.

12.7 Let $S = k[x_0, x_1]$ be a weighted polynomial ring, where x_0 has weight w_0 and x_1 has weight w_1.

(a) Assume that $w_0 = 2$ and $w_1 = 3$. For each $t \geq 0$, express $t = 6q + r$ where $0 \leq r \leq 5$. Show that

$$\mathrm{HF}_S(t) = \begin{cases} q+1 & \text{if } r \neq 1 \\ q & \text{if } r = 1. \end{cases}$$

Explain why this does not contradict Theorem 12.14.

(b) Let M denote the least common multiple of w_0 and w_1 and pick an integer R with $0 \leq R \leq M-1$. Show that $\mathrm{HF}_S(Mq + R)$ is a degree-1 polynomial function in q for $q \gg 0$.

12.8 Show that any smooth plane curve is irreducible. *Hint:* The irreducible components of a plane curve are themselves plane curves! Check that the following complex plane curves $C \subset \mathbb{P}^2(\mathbb{C})$ are irreducible:

$$x_0^5 + x_1^5 + x_2^5 = 0$$
$$x_0^3 + x_1^3 + x_2^3 = \lambda x_0 x_1 x_2, \quad \lambda^3 \neq 27.$$

https://doi.org/10.1017/CBO9780511755224.013 Published online by Cambridge University Press

12.9 Find all points of intersection of the following pairs of plane curves $\{F = 0\}$, $\{G = 0\} \subset \mathbb{P}^2(\mathbb{C})$, and the multiplicities of the intersections.
(a) $F = x_0^2 + x_1^2 + x_2^2$ and $G = x_0x_2 - x_1^2$;
(b) $F = x_0x_2^2 - x_1^3$ and $G = x_0x_2^2 - x_0x_1^2 - x_1^3$;

12.10 Compute the inflectional tangents of the curve $C \subset \mathbb{P}^2(\mathbb{C})$ given by

$$x_0^3 + x_1^3 + x_2^3 = 2x_0x_1x_2.$$

12.11 Consider the complex projective curves

$$C = \left\{(x_0, x_1, x_2) : x_0^2 + x_1^2 = x_2^2\right\} \subset \mathbb{P}^2(\mathbb{C})$$
$$D = \left\{(x_0, x_1, x_2) : x_0^2 - x_1^2 = x_2^2\right\} \subset \mathbb{P}^2(\mathbb{C}).$$

Describe the intersection $C \cap D$ and compute the multiplicity of each point. Make sure you prove that you have found every point of the intersection!

12.12 Let V be an affine variety with $p \in V$ and $\mathfrak{m}_p \subset k[V]$ the corresponding maximal ideal. Consider the graded ring

$$R = \oplus_{t\geq 0} R_t = k[V]/\mathfrak{m}_p \oplus \mathfrak{m}_p/\mathfrak{m}_p^2 \oplus \mathfrak{m}_p^2/\mathfrak{m}_p^3 \ldots \oplus \mathfrak{m}_p^t/\mathfrak{m}_p^{t+1} \oplus \ldots,$$

i.e., $R_0 = k$ and $R_t = \mathfrak{m}_p^t/\mathfrak{m}_p^{t+1}$ for $t > 0$. This is called the *graded ring associated* to $k[V]$ and $\mathfrak{m}_p$.
(a) Let $x_0, \ldots, x_n$ be generators of $R_1 = \mathfrak{m}_p/\mathfrak{m}_p^2$ as a vector space over k. Show that $x_0, \ldots, x_n$ generate R as a k-algebra. *Hint:* Check that the monomials x^α with $|\alpha| = t$ span R_t.
(b) Show that the kernel $J = \ker(k[x_0, \ldots, x_n] \twoheadrightarrow R)$ is homogeneous. The corresponding affine variety

$$V(J) \subset \mathbb{A}^{n+1}(k)$$

is the *tangent cone* to V at p and the projective variety

$$X(J) \subset \mathbb{P}^n(k)$$

is called the *projective tangent cone.*
(c) Suppose that $0 = p \in V \subset \mathbb{A}^m(k)$ and $I(V) = \langle f \rangle$ for some $f \in k[y_1, \ldots, y_m]$ with graded pieces

$$f = F_M + F_{M+1} + \cdots + F_d, \quad F_M \neq 0.$$

Show that the associated graded ring is $k[y_1, \ldots, y_m]/\langle F_M \rangle$.
(d) Draw the graph of $V = \{(y_1, y_2) : y_2^2 = y_1^2 + y_1^3\} \subset \mathbb{A}^2(\mathbb{R})$ and its tangent cone. Do the same for $V' = \{y_2^2 = y_1^3 + y_1^4\} \subset \mathbb{A}^2(\mathbb{R})$.

12.13 Find an explicit formula for the arithmetic genus of a degree d hypersurface $X \subset \mathbb{P}^3(\mathbb{C})$.

12.14 Extract equations for $\mathcal{H}ilb_{f(t)}$ for the following classes of varieties:

https://doi.org/10.1017/CBO9780511755224.013 Published online by Cambridge University Press

(a) Lines $\ell \in \mathbb{P}^3$ with $f(t) = t + 1$. *Hint:* Use $\mathrm{Gr}(2, k[x_0, x_1, x_2, x_3]_1)$.
(b) Pairs of points $X = \{p_1, p_2\} \subset \mathbb{P}^2$ with $f(t) = 2$. *Hint:* Use the Grassmannian $\mathrm{Gr}(4, k[x_0, x_1, x_2]_2)$.

Is $\mathcal{H}ilb_{f(t)}$ closed in the Grassmannian? If not, describe the points in the closure.

12.15 *Challenge:* Each bihomogeneous $F \in \mathbb{C}[x_0, x_1, y_0, y_1]$ defines a curve in $\mathbb{P}^1(\mathbb{C}) \times \mathbb{P}^1(\mathbb{C})$. State and prove a Bezout Theorem for a pair of bihomogeneous forms F, G without common factors.

https://doi.org/10.1017/CBO9780511755224.013 Published online by Cambridge University Press