HILBERT FUNCTIONS

CALVIN HENAKU

1. Introduction [Eis95]

In the late 1800s, problems in invariant theory spurred the growth of algebraic geometry and commutative algebra. The fundamental problem of invariant theory was determining the existence of a finite system of generators for a ring of invariants for an action. Hilbert's Basis Theorem led to the resolution of this fundamental problem. Simultaneously, Hilbert also sought to determine numerical invariants of projective algebraic sets $X = V(I) \subset \mathbb{P}^n$. In particular, given an action on linear forms, he wanted to understand how the space of invariant forms of degree d varies with d. Therefore, we may reformulate the question in the context of graded modules.

Definition 1.1. If $R = R_0 \oplus R_1 \oplus \cdots$ is a graded ring, then a **graded module** over R is a module M with a decomposition into abelian subgroups

$$M = \bigoplus_{-\infty}^{\infty} M_i$$

such that $R_i M_j \subset M_{i+j}$ for all i, j.

Analogous to Hilbert's question, one may ask how the "size" of the M_i varies with i. Another question, what is an appropriate notion of size for M_i? Hilbert to the rescue! Hilbert functions, $H_M(s)$ and polynomials, $P_M(s)$, encode this information and are surprisingly well-behaved. As Eisenbud states, "all the information encoded in the infinitely many values of the function $H_M(s)$ can be read off from just finitely many of its values."

The foremost example of a graded module that one should consider is the homogeneous coordinate ring $\Gamma(X)$ where X is an irreducible projective variety in $\mathbb{P}^n$. The homogeneous coordinate ring is of great interest to us in algebraic geometry. Our homogeneous coordinate ring is graded by degree and finding the dimension of the graded components, $\Gamma(X)_d$, is geometrically equivalent to finding how many independent functions of degree d there are on X. For example, if X is a set of 3 points in the plane and $M = \Gamma(X)$, then $H_M(1)$ will be 2 if the three points are co-linear, but 3 otherwise. Although it is not obvious how $H_M(s)$ would behave asymptotically, Hilbert proved the following about $H_M(s)$ for s sufficiently large:

Theorem 1. *If M is a finitely generated graded module over $k[x_0, \cdots, x_r]$, then $H_M(s)$ agrees, for large s, with a polynomial, $P_M(s)$, of degree $\leqslant r$.*

Furthermore, the Hilbert polynomial encodes a host of invariants such as the dimension and degree of a projective variety X.

2. Hilbert Functions and Examples

Definition 2.1 (Hilbert Function). [1] Let k be an algebraically closed field and $S = k[X_0, \cdots, X_n]$. For a finitely-generated graded S-module with grading by degree. The numerical function

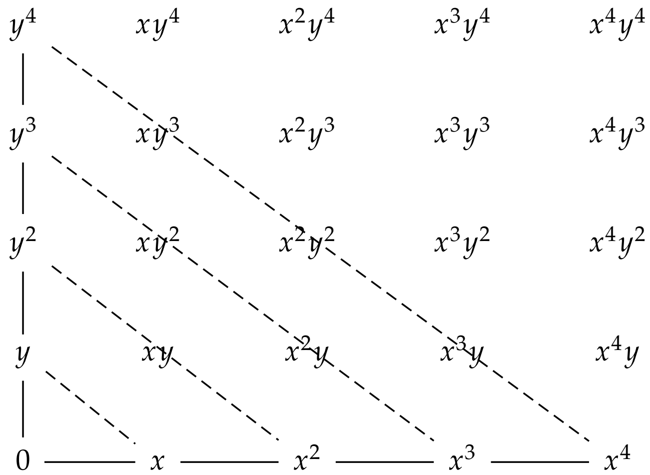
$$H_M(s) := \dim_k M_s$$

[1] Here, since k is a field, we can speak about the dimension of M_s as a vector field over k. However, in more general cases, k may not be a field. For example, if k is Artinian, then we may define a function λ such that $\lambda(M_n) = \text{length}(M_n)$ where $\lambda(M_n) \in \mathbb{Z}$. The only property such a function λ must satisfy is additivity over exact sequences, namely that if $0 \to A \to B \to C \to 0$ is an exact sequence, the $\lambda(B) = \lambda(A) + \lambda(C)$.

is called the **Hilbert function of M**.

To gain familiarity with the Hilbert function, let us consider examples that may elucidate some of its properties.

Example 2.2 (Monomial Ideals)**.** [Sec19] Consider the monomial ideal $I = (x, y)$ and consider I_d, the space of forms of degree d in I. The lattice points on the line $x + y = d$ represent the forms of degree d. Therefore, from the diagram, $H_I(1) = \dim_k\{x, y\} = 2$, $H_I(2) = \dim_k\{x^2, xy, y^2\} = 3$, and generally for $n \geqslant 1$, $H_I(s) = \dim_k\{x^s, x^{s-1}y, \cdots, xy^{s-1}, y^s\} = s+1$. In this case, $H_{M/I}(s) \equiv 0$. Therefore, this is consistent with Theorem 1.



Let us proceed to a slightly more complex example and suppose that $I = (x^n, y^m)$ with $m \geqslant n$. With the image of the preceding example in mind, consider a discrete lattice. Denote an arbitrary point $x^k y^l$ by (k, l) where $n, m \in \mathbb{Z}_{>0}$. Then all monomials $x^k y^l$ with $k \geqslant n$ or $l \geqslant m$ are contained in I by the properties of ideals. As mentioned earlier, the space of forms of degree d is determined by the lattice points of the line $x + y = d$. Then for $s \geqslant m$, since the lattice points of $x + y = s$ consists of monomials in the ideal, $H_I(s) = s + 1$ and H_I agrees with a polynomial. In addition to this, $H_{R/I} = 0$ for $d \geqslant m$. More generally, if we have an ideal $I = (x^{m_1}y^{m_2}, x^{n_1}y^{n_2})$, we can show that the dimension of $H_I(s)$ also stabilizes to a polynomial. Consider $a = \min\{m_1, n_1\}$ and $b = \min\{m_2, n_2\}$. For sufficiently large s, $H_{R/I} = a + b$. This is best shown pictorially. At each point (m_1, m_2) and (n_1, n_2) we can consider the union of the upper right quadrants formed with each of these points as a center. Then if $a = \min\{m_1, n_1\}$, then for a lattice point contained in the left-most boundary of the union, there will be a lattice points to the left of it. Similarly, if $b = \min\{m_2, n_2\}$, then there will only be b lattice points under the bottom-most boundary of the union. This is equivalent to saying that $H_{R/I}$ eventually stabilizes to the constant polynomial $a + b$. Therefore $H_I(s) = (s + 1) - (a + b)$ for sufficiently large s, since from the line $x + y = s$, we remove the lattice points not contained in the ideal and we know the number of lattice points on the diagonal stabilize.

Example 2.3 (d points)**.** [Cla] Let $X = \{x_1, x_2, \cdots, x_d\}$ be our variety consisting of d distinct points. We begin by calculating $H_{\Gamma(X)}(1)$ or the space of forms of degree 1 in our homogeneous coordinate ring.

$$H_X(1) = \dim_k(\Gamma(X)_1) = \dim_k(k[X_0, \cdots, X_{d-1}]) - \dim_k(I(x)_1)$$

where $I(X)_1$ consists of all homogeneous linear polynomials vanishing at $x_1, \cdots, x_d$. We note that two points are sufficient to determine a linear polynomial, and therefore for $d \geqslant 3$, our polynomial can't vanish at all the points unless they are co-linear. Therefore, $\dim_k(I(x)_1)$ is equal to 1 if and only if our points are co-linear and equal to 0 otherwise. This implies $h_X(1) = d - 1$ and d otherwise.

Now suppose we want to compute $H_{\Gamma(X)}(d-1)$. Choose representatives of our points $\{v_1, \cdots, v_d\} \in \mathbb{A}^d \backslash \{0\}$.Then define a map ϕ

$$k[X_0, \cdots, X_{d-1}]_{d-1} \to k^d$$

given by valuation at $(v_1, v_2, \cdots, v_d)$. Then the kernel of our evaluation map is the ideal $I(X)_{d-1}$, which is the set of polynomials vanishing at $\{v_1, \cdots, v_d\}$. Our map is also surjective because of the following: we can multiply linear homogeneous polynomials vanishing at p_k, $1 \leqslant k \leqslant d-1$, but not vanishing p_d. This gives us a degree $d-1$ homogeneous polynomial vanishing at all points on our set except p_d. Using the same process, we can find a degree $d-1$ polynomial vanishing at all points on our set except at p_k for $1 \leqslant k \leqslant d$ and therefore our image must contain the basis vectors for k^d. Then our map is surjective and $H_{\Gamma(X)}(d-1) = \dim_k(\Gamma(X)_{d-1}) = \dim_k k[X_0, \cdots, X_{d-1}]_{d-1} - \dim_k \ker(\phi) = \dim_k \operatorname{img}(\phi) = \dim_k(k^d) = d$

Example 2.4 (Polynomial Ring)**.** If $R = k[x_1, \cdots, x_n]$, then $H_R(I) = \binom{n+i-1}{i}$. This is equivalent to the stars and bars combinatorial theorem since we are essentially asking the number of solutions $(x_1, \cdots, x_n)$ of non-negative integers to $x_1 + x_2 + \cdots + x_n = i$.

3. Hilbert-Poincare Series

Definition 3.1. The *Hilbert-Poincare series* of a graded module M is a formal power series

$$P(t) = \sum_{i \geqslant 0} \lambda(M_i) t^i$$

Theorem 3.2 (Hilbert-Serre)**.** *If M is a finitely generated graded module over $R[x_1, \cdots, x_n]$, $\deg x_i = d_i$ with an Artinian ring R, then*

$$\lambda_M(t) = \frac{f(t)}{\prod(1-t^{d_i})} \quad \textit{for some } f(t) \in \mathbb{Z}[t].$$

Proof. The proof of this theorem is recorded in Atiyah-MacDonald and we copy it here for convenience. [AM16]

By induction on s, the number of generators of $R = \bigoplus_{n=0}^{\infty} R_n$ over R_0. If $s = 0$, then for all $n > 0$, $R_n = 0$ and $R = R_0$ and M if a finitely generated R_0 module, then for $n >> 0$, $M_n = 0$ and $P(M, t)$ is a polynomial.

Now suppose $s > 0$ and the theorem is true for $s-1$ generators. Then multiplication by x_s is an R-module homomorphism of M_n into M_{n+k_s} since x_s has degree k_s. Then we have the exact sequence

$$0 \longrightarrow K_n \longrightarrow M_n \xrightarrow{x_s} M_{n+k_s} \longrightarrow L_{n+k_s} \longrightarrow 0$$

where $K = \bigoplus_n K_n$ and $L = \bigoplus_n L_n$; these are both finitely-generated R-modules and are both annihilated by x_s, and therefore they are $R_0[x_1, \cdots, x_{s-1}]$-modules. Then we can apply λ to our exact sequence to obtain

$$\lambda(K_n) - \lambda(M_n) + \lambda(M_{n+k_s}) - \lambda(L_{n+k_s}) = 0$$

Then if we multiply by t^{n+k_s} and sum over n, then we obtain

$$(1 - t^{k_s}) P(M, t) = P(L, t) - t^{k_s} P(K, t) + g(t)$$

where $g(t)$ is a polynomial. Applying the inductive hypothesis the result now follows. $\square$

Example 3.3 (Polynomial Case)**.** Suppose all of the x_i are of degree 1, where $k_i = 1$. Then $P(t) = \frac{f(t)}{(1-t)^s}$ and $\frac{1}{(1-t)^s} = \sum_{n \geqslant 0} t^n \binom{n+s-1}{s-1}$ which is a polynomial in n if $n \geqslant 0$. Then the coefficients of t^n in $P(t)$ are polynomials of n when we take n sufficiently large, namely when n is bigger than the degree of any of terms in $f(t)$.

Remark 3.4 (Integer Valued Polynomials)**.** Any integer-valued polynomial of degree d is a linear combination of $\binom{n}{0},\binom{n}{1},\cdots,\binom{n}{d}$

Proof. Suppose that we are given a degree d integer-valued polynomial,

$$f(n)=\sum_{0}^{d}a_in^i.$$

Then $f(0)=a_0$, then choose $g(n)=\sum_0^d g_i\binom{n}{i}$ with $g(0)=a_0=g_0\in\mathbb{Z}$. Now $f(1)=a_0+a_1+a_2+\cdots+a_d$, then specify $g_2=a_2+\cdots+a_d$. Then we can continue specifying the values for g_i such that $f(k)=g(k)$ for $0\leqslant k\leqslant d$ since $\binom{n}{i}$. Since g and f are polynomials of degree d, then since they agree at $d+1$ points they must be the same. □

An interesting property of the Hilbert-Poincare series is that it encodes interesting invariants of our variety.

Theorem 3.5. *Let $X\subseteq\mathbb{P}^n$ be a projective variety with $\dim(X)=D$. Then $\deg(P_{\Gamma(X)})=D$ and if $X\neq 0$, then the leading term of $P_{\Gamma(X)}(s)$ is*

$$\frac{dx^D}{D!}$$

for some $d\in\mathbb{N}$ is called the degree of X and if $X=V(F)$ is a hypersurface, then $d=\deg(F)$.

The following example from Clader will help to clarify.

Example 3.6. [Cla] Let $S=k[X_0,\cdots,X_n]_d$. If $F\in S_d$, then $X=V(F)$ is a degree d hypersurface in $\mathbb{P}^n$. Then there is an exact sequence of graded S-modules

$$0\longrightarrow S[-d]\xrightarrow{\times F}S\longrightarrow\Gamma(X)\longrightarrow 0$$

. Then

$$\dim_k(\Gamma(X)_m)=\dim_k(S_m)-\dim_k(S_{m-d})=\binom{m+n}{n}-\binom{m+n-d}{n}=\frac{d}{(n-1)!}m^{n-1}+\cdots$$

Then since hypersurfaces have degree $n-1$, this aligns with Theorem 3.5 and our variety is of degree d by initial assumptions and therefore d is indeed the degree of F.

4. Open Questions [Sec19]

This section is taken directly from Seceleanu and I include select problems of interest.

Conjecture 4.1 (The Hilbert function of a generic algebra)**.** *Let $F_1,\cdots,F_r$ be homogeneous polynomials of degrees $d_1,\cdots,d_r\geqslant 1$ in a polynomial ring $R=F[x_1,\cdots,x_n]$. If $F_1,\cdots,F_r$ are chosen "randomly" and $I=(F_1,\cdots,F_r)$ then*

$$HS_{R/I}(t)=\frac{\prod_{i=1}^r(1-t^d)}{(1-t)^n}$$

Definition 4.2. An ideal defining a set of **fat points** is an ideal of the form

$$I=I_{p_1}^{m_1}\cap I_{p_2}^{m_2}\cap\cdots\cap I_{p_r}^{m_r}$$

where I_{p_i} is the ideal defining a point $p_i\in\mathbb{P}^n$.

The following conjecture states that any hypersurface vanishing at points $p_1,\cdots,p_4\in\mathbb{P}^n$ with to order $m_1,\cdots,m_r$ respectively must have degree $d\geqslant\frac{m_1+m_2+\cdots+m_r}{\sqrt{n}}$

Conjecture 4.3 (Nagata's Conjecture on Curves)**.** *If $I=I_{p_1}^{m_1}\cap I_{p_2}^{m_2}\cap\cdots\cap I_{p_r}^{m_r}$ is an ideal defining r fat points in $\mathbb{P}^n$ and $d>0$ is an integer such that $H_1(d)>0$ then*

$$\sqrt{n}\cdot d\geqslant m_1+m_2+\cdots m_r$$

References

[AM16] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, economy ed., Addison-Wesley Series in Mathematics, Westview Press, Boulder, CO, 2016, For the 1969 original see [MR0242802]. MR 3525784

[Cla] Emily Clader, *Hilbert polynomials and the degree of a projective variety*.

[Eis95] David Eisenbud, *Commutative algebra*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995, With a view toward algebraic geometry. MR 1322960

[Sec19] Alexandra Seceleanu, *Hilbert functions in algebra and geometry*, Apr 2019.

Department of Mathematics & Statistics, Washington University in St. Louis, St. Louis, MO, 63130, USA
Email address: chenaku@wustl.edu