

Hilbert Series and Free Resolutions

A Senior Project submitted to
The Division of Natural Sciences and Mathematics
of
Bard College

by
Elena Grigorescu

Annandale-on-Hudson, New York
May , 2003

Contents

Dedication	3
Abstract	4
Acknowledgments	5
1 Introduction	6
2 Preliminaries	7
2.1 Graded algebras and homogeneous ideals	7
2.2 Hilbert Functions and Hilbert Series	9
2.3 Combinatorial approaches to the study of Hilbert Series	11
3 Hilbert Series of Monomial Ideals	14
3.1 General facts in n variables	14
3.2 Characterization of the monomial ideals in two variables in terms of Hilbert series	17
3.3 Stillman & Bayer's theorem	19
3.4 From Hilbert series to Modules and Resolutions	23
4 Modules, Syzygies and Resolutions	26
4.1 Modules	26
4.2 Syzygies	28
4.3 Freeness of modules generated by matrices in polynomial rings	30
4.4 Resolutions of Modules	33
4.5 Resolutions of Graded Modules	35

<i>Contents</i>	2
4.6 Computing Hilbert Functions	41
5 Open questions	48
References	50

Dedication

To my family and to M.

Abstract

We completely characterize the Hilbert series of monomial ideals in two variables using combinatorial and algebraic techniques. Since the concepts of modules and resolutions play an important role in the study of Hilbert functions and Hilbert series, we familiarize ourselves with these mathematical objects. Along the way we obtain some results regarding freeness of modules, and we provide proofs for some classical results about graded modules and graded resolutions. These lead us to proving the Hilbert & Serre theorem for graded modules in polynomial rings, which was our initial motivation for the project.

Acknowledgments

Now the easy part...

I must first thank my adviser Lauren Rose for all the encouragements and useful suggestions I received while writing this project.

Also, I thank Bob McGrail for his valuable comments on my drafts, and for the lively spirit he brings to the math department.

I very much thank Ethan Bloch for his help with LaTeX, and for advising me when Lauren was unavailable.

Thank you mom and dad for making me happy. Thank you Miha for missing me. I miss you too. Thank you *gradma*₁ for loving me still even after having lied to you about my going to the University of Bucharest. Thank you *gradma*₁₁ for being so kind and for bearing all my naughtiness as a child. I wish I thanked you earlier.

Thank you Evelyn and Frank for being my family here.

Time for my friends...

Thank you Tanveer for your support and care. Thank you Vasi, Tim, Teo, and Noriko for sharing the most beautiful times with me at Bard. Thank you Reaz for teaching me a little Bengali. Thank you Mariana for being so amused by my comments.

1

Introduction

I started this project by analyzing the Hilbert series of monomial ideals. This is how I came across a famous theorem by Hilbert & Serre, which asserts that the Hilbert series of a monomial ideal is always a rational function. These functions are of the form

$$\frac{p(t)}{(1-t)^n},$$

where n is the number of variables of the polynomial ring in which the ideal sits, and $p(t)$ is a polynomial with integer coefficients. I became interested in the polynomial $p(t)$, so I tried to characterize $p(t)$ for monomial ideals in n variables. The main results of my Senior Project in terms of original work consists of the characterization of $p(t)$ in 2 variables that is presented in Chapter 3. In order to understand proofs about Hilbert series and Hilbert functions, I had to get familiar with new concepts such as modules, syzygies and resolutions. Along the way I managed to prove some minor results, and these are included in Chapter 4. I end the project by giving my own proof of the Hilbert & Serre Theorem for general modules.

2

Preliminaries

In this chapter we introduce some basic definitions and concepts that we will use throughout the project.

2.1 Graded algebras and homogeneous ideals

Let k be an infinite field.

Definition. A *commutative k -algebra* is a vector space A over k , which possesses a multiplication operation, such that for every $x, y, z \in A$ and $\alpha, \beta \in k$ the following hold:

1. $xy = yx$
2. $x(yx) = (xy)z$
3. $x(y + z) = xy + xz$
4. $\alpha(xy) = (\alpha x)y = x(\alpha y)$
5. $\alpha(\beta x) = (\alpha\beta)x$.

△

Note that A is in fact a ring as well.

Definition. A *graded k -algebra* is a k -algebra that has a decomposition

$$A = \bigoplus_{n \geq 0} A_n$$

as a vector space over k such that

- 1) $A_0 \cong k$;
- 2) $A_i A_j \subseteq A_{i+j}$ for all $i, j \geq 0$.

Each element $x \in A_n$ is called *homogeneous of degree n* . \triangle

Let $R = k[x_1, x_2, \dots, x_n]$ be the polynomial ring in n variables, over the field k , where each x_i has degree 1. This is the ring which we consider throughout the paper. It easily seen that R is a graded algebra and we can express it as

$$R = \bigoplus_{n \geq 0} R_n,$$

where R_n consists of the homogeneous polynomials of degree n . For a proof of this statement see [8, Theorem 2.2.5].

We will now introduce the algebraic objects that we will be studying in great detail.

Definition. A *homogeneous ideal* is an ideal generated by homogeneous polynomials. \triangle

Example 2.1.1. Let $R = k[x_1, x_2, x_3]$ and let $I = \langle x_1^4 - x_1 x_2 x_3^2 + x_2^3 x_3, x_1^2 + x_1 x_3, x_3^3 \rangle$. Since the generating polynomials are homogeneous of degree 4, 2 and 3 respectively, we have by the definition that I is homogeneous. \diamond

Definition. A *monomial ideal* I in a ring R is an ideal generated by monomials in R . \triangle

Example 2.1.2. Let $R = k[x_1, x_2, x_3, x_4]$, and $I = \langle x_4^2, x_1 x_3^2, x_2 \rangle$. Then I is a monomial ideal. \diamond

It is easily seen that a monomial ideal is also a homogeneous ideal.

Since an ideal of R is also a k -algebra, we can talk about *graded ideals*. We will then say that I is a graded ideal if $I = \bigoplus_{n \geq 0} I_n$, where $I_n = R_n \cap I$.

The following theorem establishes a relationship between homogeneous ideals and graded ideals. For a proof of the theorem as well as details of the observations that follow see [1].

Theorem 2.1.3. *Let $I \subset R$ be an ideal. Then I is homogeneous iff I is graded, with the grading $I_n = R_n \cap I$.*

It can be shown (see [8, Theorem 2.3.6]) that the quotient ring R/I of a graded ring R and a graded ideal I is a graded ring also. So, if we can express

$$R = R_0 \oplus R_1 \oplus \dots$$

and

$$I = I_0 \oplus I_1 \oplus \dots,$$

then

$$R/I \cong R_0/I_0 \oplus R_1/I_1 \oplus \cdots .$$

When I is a monomial ideal, each I_n is spanned by the monomials of I of degree n . Further, each R_n/I_n is spanned by equivalence classes of monomials of degree n in R/I . It is easily seen that there is a unique monomial in each equivalence class (see [8]).

Example. Let $R = k[x, y]$ and $I = \langle xy^2, x^2 \rangle$ be a monomial ideal in R . Then $I = \bigoplus I_i$. We have that I_0 is spanned by the monomials from I that are of degree 0. Therefore $I_0 = \emptyset$. Similarly, I_1 is spanned by the monomials of I of degree 1, so $I_1 = \emptyset$. Further, we have that $I_2 = \text{span}\{x^2\}$ since x^2 is the only monomial in I_2 . Also, $I_3 = \text{span}\{x^3, x^2y, xy^2\}$. It can also be shown that $I_4 = \text{span}\{x^4, x^3y, x^2y^2, xy^3\}$. Next we can compute R_n/I_n . Since $R_0 = \text{span}\{1\}$ and $I_0 = \emptyset$, we have that $R_0/I_0 = \text{span}\{\bar{1}\}$, where the bar represents the equivalence class of the element 1. Similarly, $R_1 = \text{span}\{x, y\}$ and $I_1 = \emptyset$, so $R_1/I_1 = \text{span}\{\bar{x}, \bar{y}\}$. Also, $R_3 = \text{span}\{x^3, y^3, x^2y, xy^2\}$, and $I_3 = \text{span}\{x^3, x^2y, xy^2\}$, so $R_3/I_3 = \text{span}\{\bar{y}^3\}$, and so on. In what follows we will abuse notation by omitting the bars. \diamond

2.2 Hilbert Functions and Hilbert Series

Definition. A graded k -algebra $A = \sum_{n \geq 0} A_n$ is *finitely generated* if there exist a finite number of elements y_1, y_2, \dots, y_n such that A is spanned by the set of monomials

$$\{y_1^{a_1} y_2^{a_2} \cdots y_n^{a_n} \mid 0 \leq a_i \in \mathbb{Z}\}$$

in y_1, y_2, \dots, y_n as a vector space over k . \triangle

Definition. Let $A = \bigoplus_{n \geq 0} A_n$ be a finitely generated graded k -algebra. The *Hilbert function* of A is defined to be

$$\mathcal{H}(A, n) = \dim_k(A_n)$$

where $\dim_k A_n$ is the dimension of the vector space A_n over k . If $I = I_0 \oplus I_1 \oplus \cdots$ is a homogeneous ideal of A , we can also define

$$\mathcal{H}(I, n) = \dim I_n.$$

\triangle

Note that if A is finitely generated, for each non-negative integer j there are finitely many monomials of degree j among the generators of A . The monomials of degree j from the set of generators of A generate A_j as a vector space over k , so A_j is finitely generated for each j .

A nice representation of the dimensions of the components of an algebra A is given by introducing the series having as coefficients the value of the Hilbert function at

each homogenous component. In combinatorial terms, the Hilbert series of A is the generating function of the sequence given by the Hilbert function.

Definition. Let $A = \bigoplus_{n \geq 0} A_n$ be a finitely generated k -algebra. The *Hilbert series* of A is defined to be the generating function

$$\mathcal{F}(A, t) = \sum_{n=0}^{\infty} \mathcal{H}(A, n)t^n.$$

Similarly, if I is a homogeneous ideal of A , then the Hilbert series of I is

$$\mathcal{F}(I, t) = \sum_{n=0}^{\infty} \mathcal{H}(I, n)t^n.$$

△

We do not worry about convergence since we are working in the field of power series.

Example 2.2.1. We compute the Hilbert series of $R[x]$. Since $R_i = \text{span}\{x^i\} = kx^i$, we have that

$$\begin{aligned} R &= \bigoplus_{n \geq 0} R_n \\ &= \text{span}\{1\} \oplus \text{span}\{x\} \oplus \text{span}\{x^2\} \oplus \cdots \\ &= k \oplus kx \oplus kx^2 \oplus \cdots \end{aligned}$$

Therefore, $\mathcal{H}(R, i) = 1$ for any i , and

$$\mathcal{F}(R, t) = 1 + t + t^2 + \cdots = \frac{1}{1-t}.$$

◇

When referring to Hilbert functions of ideals, algebraists like to study properties of R/I rather than of I , primarily because of its uses in algebraic geometry. We adopt the same convention in this paper. Since we are mainly going to compute the Hilbert series of quotient rings R/I , it is of interest to see how the Hilbert series of I relates to the Hilbert series of R/I .

Theorem 2.2.2. Let $R = \bigoplus_{n \geq 0} R_n$ be a graded k -algebra and $I = \bigoplus_{n \geq 0} I_n$ be a graded ideal. Then

$$\mathcal{F}(R/I, t) = \mathcal{F}(R, t) - \mathcal{F}(I, t).$$

Proof. A standard result in linear algebra states that given a vector space V and a subspace W it holds that

$$\dim(W/V) = \dim(W) - \dim(V).$$

We know that each R_n, I_n and R_n/I_n are vector spaces, and I_n is a subspace of R_n . Then,

$$\dim(R_n/I_n) = \dim(R_n) - \dim(I_n).$$

This implies that

$$\mathcal{H}(R/I, n) = \mathcal{H}(R, n) - \mathcal{H}(I, n)$$

and by summing over all n 's the theorem follows. \square

The idea of this senior project was inspired by a theorem of Hilbert & Serre (see [1, Theorem 11.1]), that makes an assertion about the Hilbert series of a module. Since a module is in a way a generalization of an ideal, and since we do not yet have the necessary background regarding modules, we will formulate the theorem in terms of ideals. The Hilbert & Serre theorem shows that for a polynomial ring R and a homogeneous ideal I , the Hilbert series of R/I always has the form of a rational function.

Theorem 2.2.3 (Hilbert, Serre). *Given a graded polynomial ring $R = k[x_1, x_2, \dots, x_n]$ and a graded ideal I in R , then the Hilbert series of R/I can be expressed as*

$$\mathcal{F}(R/I, t) = \frac{p(t)}{(1-t)^n},$$

where $p(t)$ is some polynomial in t and with integer coefficients.

We will prove this theorem in the more general setting of modules in Chapter 4.

The initial goal of this project was to determine $p(t)$ for certain classes of monomial ideals, in particular monomial ideals in two variables. The one-variable case is relatively easy.

We start by noting that using Theorem 2.2.2, Theorem 2.2.3 holds also for the homogeneous ideal I .

In fact, for any ideal I , we have $H(I)$ is always equal to $H(I^m)$, where I^m is some monomial ideal (see [2, Chapter 9, Section 3, Proposition 9] for details).

For this reason, the results that we obtain for monomial ideals in this project hold for any general ideals.

2.3 Combinatorial approaches to the study of Hilbert Series

In this section I will introduce some combinatorial approaches regarding Hilbert series. One of the earliest questions that appeared regarding the Hilbert series was to determine which sequences of natural numbers arise as the Hilbert series of some ideal in R . Moreover, given a sequence that is the Hilbert series of an ideal, how can one construct the ideal? Both questions were solved for ideals by Macaulay in 1927. For a quick flavor of the results I will present his theorem.

First we need to state some definitions and results([5, Lemma 1.2]) that will be used in the theorem.

Proposition 2.3.1. *Given h and d positive integers, then h can be written uniquely as*

$$h = \binom{n_0}{d} + \binom{n_1}{d-1} + \cdots + \binom{n_j}{d-j}$$

for some j where $n_0 > n_1 > \cdots > n_j \geq 1$ and $n_i \geq d - i$ for $0 \leq i \leq j$.

We will also use the following notation for simplifying the representations that follow.

Definition. Let h be a positive integer written as in Theorem 2.3.1. We will make the following notation

$$h^{(d)} = \binom{n_0+1}{d+1} + \binom{n_1+1}{d} + \cdots + \binom{n_j+1}{d-j+1},$$

where $0^{(i)} = 0$.

△

Macaulay's theorem ([4, Theorem 18.3]) gives a necessary and sufficient condition for a finite sequence H to be the Hilbert function of some monomial ideal.

Theorem 2.3.2. *$H : \mathbb{N} \rightarrow \mathbb{N}$ is the Hilbert function of some monomial ideal I iff*

i) $H(0) = 1$;

ii) for all $d > 0$, if $H(d) = h$ is written uniquely as

$$h = \binom{n_0}{d} + \binom{n_1}{d-1} + \cdots + \binom{n_j}{d-j},$$

then

$$H(d+1) \leq h^{(d)} = \binom{n_0+1}{d+1} + \binom{n_1+1}{d} + \cdots + \binom{n_j+1}{d-j+1}.$$

Note that $H(d)$ from the above theorem is actually $\mathcal{H}(I, d)$ for some unknown ideal I and some integer d . The theorem does not specifically tell one how to construct an ideal I that has its Hilbert function a given series of integers. In her Senior Project [8], Jaren Smith showed how such ideals can be determined in the two-variable case.

We will now show the method we mostly use for computing Hilbert series. In order to obtain any computational results regarding Hilbert series of monomial ideals, we first need to compute the Hilbert series of the general polynomial ring in n variables. The theorem below completely answers this question. We will find the dimension of I_n by counting the number of monomials that span I_n . Also, to compute the dimension of R_n/I_n we will count the number of monomials in R_n and subtract the number of monomials spanning I_n .

Theorem 2.3.3. *Let $R = k[x_1, x_2, \dots, x_n]$. Then*

$$\mathcal{F}(R, t) = \frac{1}{(1-t)^n}.$$

Proof. We will prove the theorem by induction on n (the number of variables). For $n = 1$ we have seen in Example 2.2.1 that the theorem holds. Suppose now that it holds in $n - 1$ variables x_1, x_2, \dots, x_{n-1} , so

$$\mathcal{F}(k[x_1, x_2, \dots, x_{n-1}], t) = \frac{1}{(1-t)^{n-1}}.$$

Let h_i and g_i be the Hilbert function $\mathcal{H}(R, i)$ and the Hilbert function $\mathcal{H}(k[x_1, x_2, \dots, x_{n-1}], i)$ respectively, for each $i \geq 0$. A monomial p of degree i in $k[x_1, x_2, \dots, x_n]$ can be written as

$$p = x_n^a m,$$

where $a \geq 0$, and m is a monomial of degree $i - a$, not involving x_n . Thus, the number of monomials of degree i that generate each R_i of $k[x_1, x_2, \dots, x_n]$ is the sum of the number of monomials of degrees less than or equal to i in $k[x_1, x_2, \dots, x_{n-1}]$. We then obtain that

$$\begin{aligned} h_0 &= g_0 \\ h_1 &= g_0 + g_1 \\ h_2 &= g_0 + g_1 + g_2 \\ &\vdots \\ h_n &= g_0 + g_1 + g_2 + \dots + g_n. \end{aligned}$$

Then the Hilbert series looks like

$$\begin{aligned} \mathcal{F}(R, t) &= h_0 + h_1 t + h_2 t^2 + \dots \\ &= g_0 + (g_0 + g_1)t + (g_0 + g_1 + g_2)t^2 + \dots \\ &= (g_0 + g_1 t + g_2 t^2 + \dots) + t(g_0 + g_1 t + g_2 t^2 + \dots) + \\ &\quad + t^2(g_0 + g_1 t + g_2 t^2 + \dots) + \dots \\ &= (\mathcal{F}(k[x_1, x_2, \dots, x_{n-1}], t))(1 + t + t^2 + \dots) \\ &= \frac{1}{(1-t)^{n-1}} \frac{1}{1-t} \\ &= \frac{1}{(1-t)^n}. \end{aligned}$$

□

Similar inductive arguments will be used later in the paper for proving more complex results.

3

Hilbert Series of Monomial Ideals

In [8], Smith completely characterized the Hilbert functions of monomial ideals in two variables. In this section we will present some general results about the Hilbert series of monomial ideals and we will completely characterize the Hilbert series of monomial ideals in two variables. As opposed to extending Smith's results to Hilbert series, we use a method completely independent from her work.

3.1 General facts in n variables

Theorem 3.1.1. *Let I be an ideal in $R = k[x_1, x_2, \dots, x_r]$ and let*

$$\frac{f(t)}{(1-t)^r}$$

be the Hilbert series of R/I , where f is a polynomial in t . Let I' be the monomial ideal in $R' = k[x_1, x_2, \dots, x_r, \dots, x_n]$, with $n > r$, such that I' is generated by the same monomials as I . Then the Hilbert series of R'/I' is

$$\mathcal{F}(R'/I', t) = \frac{f(t)}{(1-t)^n}.$$

Proof. Note that it suffices to prove the theorem for $n = r + 1$. For $n = r + 1$, let h_0, h_1, \dots and g_0, g_1, \dots be the coefficients of the Hilbert series of the ideal R/I , and R'/I' respectively. Let m be a monomial of degree $i \geq 0$ in R'/I' . Then

$$m = m_1 x_{r+1}^j, \text{ with } \deg(m_1) = i - j,$$

where $i \geq j \geq 0$, and m_1 involves only x_1, x_2, \dots, x_r . Thus, the number of monomials of degree i in R'/I' is the sum of the number of monomials of degrees less than or

equal to i in R/I . Therefore, for degree $i \geq 0$ we have that

$$g_i = h_0 + h_1 + h_2 + \dots + h_i,$$

hence

$$\begin{aligned} g_0 &= h_0 \\ g_1 &= h_0 + h_1 \\ g_2 &= h_0 + h_1 + h_2 \\ &\vdots \end{aligned}$$

Then we obtain

$$\begin{aligned} \mathcal{F}(R'/I', t) &= g_0 + g_1 t + g_2 t^2 + \dots \\ &= h_0 + (h_0 + h_1)t + (h_0 + h_1 + h_2)t^2 + \dots \\ &= (h_0 + h_1 t + \dots) + t(h_0 + h_1 t + \dots) + \dots \\ &= \mathcal{F}(R/I, t) + \mathcal{F}(R/I, t)t + \mathcal{F}(R/I, t)t^2 + \dots \\ &= \mathcal{F}(R/I, t)(1 + t + t^2 + \dots) \\ &= \frac{f}{(1-t)^r} \frac{1}{(1-t)} \\ &= \frac{f}{(1-t)^{r+1}}. \end{aligned}$$

Note that the general theorem follows by a simple inductive argument. \square

We next compute the Hilbert series of some special types of monomial ideals. In the next section we quote a more general result by Stillman & Bayer [9] that computes the Hilbert series of a any monomial ideal recursively. For what follows $R = k[x_1, x_2, \dots, x_n]$.

Theorem 3.1.2. *Let $I = \langle m_1, m_2, \dots, m_k, m \rangle$ be a monomial ideal of R , such that m does not contain any variable of m_1, m_2, \dots, m_k . Let $I' = \langle m_1, m_2, \dots, m_k \rangle$, and let $a = \deg(m)$. Then*

$$\mathcal{F}(R/I, t) = \mathcal{F}(R/I', t)(1 - t^a).$$

Proof. As before, let $h_0, h_1, h_2 \dots$ and g_0, g_1, \dots be the coefficients of $\mathcal{F}(R/I', t)$ and $\mathcal{F}(R/I, t)$ respectively. For $i < a$ no monomial in R/I' is divisible by m , thus, such monomials in R/I' are identical to the ones of the same degree i in R/I , and therefore, $h_i = g_i$. Otherwise, if $i \geq a$, let p be a monomial of degree i in R/I' . Some of the monomials of degree i in the generating set of R/I' are divisible by m , and some are not. Those that are not divisible by m are identical to the monomials of degree i in R/I , since no variable contained in m is involved in them. Let p be a

monomial included in the generating set of the i th homogenous ideal of R/I' , such that $p = mp_1$ for some monomial p_1 in R/I' , with $\deg(p_1) = i - a$. Then p_1 is not divisible by any m_i , and hence p_1 is in the generating set of the $i - a$ th homogenous ideal of R/I' . The number of monomials of degree i in R/I is obtained from the number of monomials of degree i in R/I' by subtracting the number of monomials divisible by m , thus of those of degree $i - a$ in R/I' . Henceforth, for $i \geq a$ we obtain that

$$g_i = h_i - h_{i-a}$$

and

$$\begin{aligned} \mathcal{F}(R/I, t) &= g_0 + g_1t + g_2t^2 + \dots \\ &= h_0 + h_1t + \dots + h_{a-1}t^{a-1} + (h_a - h_0)t^a + (h_{a+1} - h_1)t^{a+1} + \dots \\ &= \mathcal{F}(R/I', t) - t^a\mathcal{F}(R/I', t) \\ &= \mathcal{F}(R/I', t)(1 - t^a). \end{aligned}$$

□

Corollary 3.1.3. *Let $R = k[x_1, x_2, \dots, x_n]$ and let $I = \langle m \rangle$, where m is a monomial of degree a . Then*

$$\mathcal{F}(R/I, t) = \frac{1}{(1-t)^n}(1-t^a).$$

Proof. Using the notation of the theorem, $I' = 0$ and so $R/I' = R$. From Theorem 2.3.3 we obtain that

$$\mathcal{F}(R/I', t) = \frac{1}{(1-t)^n},$$

so

$$\mathcal{F}(R/I, t) = \frac{1}{(1-t)^n}(1-t^a).$$

□

We can now derive $p(t)$ in the one-variable case.

Corollary 3.1.4. *Let $R = k[x]$ and let $I = \langle x^a \rangle$. Then*

$$\mathcal{F}(R/I, t) = \frac{1-t^a}{1-t}.$$

Proof. The proof follows directly from Corollary 3.1.3, by taking $n = 1$. □

Corollary 3.1.5. *Let $R = k[x_1, x_2, \dots, x_n]$, and let $I = \langle x_1^{a_1}, x_2^{a_2}, \dots, x_n^{a_n} \rangle$ be an ideal of R , with $a_i \in \mathbb{Z}^+$. Then*

$$\mathcal{F}(R/I, t) = \frac{1}{(1-t)^n}(1-t^{a_1})(1-t^{a_2}) \dots (1-t^{a_n}).$$

Proof. Use n applications of the Theorem 3.1.2. Since all the variables are distinct, the corollary follows. □

3.2 Characterization of the monomial ideals in two variables in terms of Hilbert series

In the case of a polynomial ring R in two variables and an ideal $I \subset R$ we completely determine the expression of the Hilbert series of R/I . First note that if, say $m_1 = x^{a_1}y^{b_1}$ and $m_2 = x^{a_2}y^{b_2}$ are among the minimal generators of I , then we cannot have either of them dividing the other and so we must have either $a_1 < a_2$ and $b_1 > b_2$, or $a_1 > a_2$ and $b_1 < b_2$. We are now ready for the theorem.

Theorem 3.2.1. *Let $R = k[x, y]$ and let $I^{(n)} = \langle x^{a_1}y^{b_1}, x^{a_2}y^{b_2}, \dots, x^{a_n}y^{b_n} \rangle$ be such that $a_1 < a_2 < \dots < a_n$ and $b_1 > b_2 > \dots > b_n$. Then, the Hilbert series of $R/I^{(n)}$ is*

$$\mathcal{F}(R/I^{(n)}, t) = \frac{1}{(1-t)^2} (1 - \sum_{k=1}^n t^{a_k+b_k} + \sum_{k=2}^n t^{a_k+b_{k-1}}).$$

We will first prove a technical lemma.

Lemma 3.2.2. *Let $R = k[x, y]$, let $I^{(n)} = \langle x^{a_1}y^{b_1}, x^{a_2}y^{b_2}, \dots, x^{a_n}y^{b_n} \rangle$ and let $I^{(n-1)} = \langle x^{a_1}y^{b_1}, x^{a_2}y^{b_2}, \dots, x^{a_{n-1}}y^{b_{n-1}} \rangle$, be such that $a_1 < a_2 < \dots < a_n$ and $b_1 > b_2 > \dots > b_n$. Then*

$$\mathcal{F}(I^{(n)}, t) = \mathcal{F}(I^{(n-1)}, t) + \mathcal{F}(\langle x^{a_n}, y^{b_n} \rangle, t) - \mathcal{F}(\langle x^{a_n}, y^{b_{n-1}} \rangle, t)$$

holds.

Proof. We represent the monomials $x^a y^b$ as the elements (a, b) of \mathbb{R}^2 , as in Figure 3.2.1. The monomials included in an ideal $\langle x^a y^b \rangle$ are all the monomials $x^\alpha y^\beta$ with $\alpha \geq a$, and $\beta \geq b$. We can represent in \mathbb{R}^2 the monomial ideal $\langle x^a y^b \rangle$ as the set of all ordered pairs (α, β) where $x^\alpha y^\beta$ is a monomial in $\langle x^a y^b \rangle$.

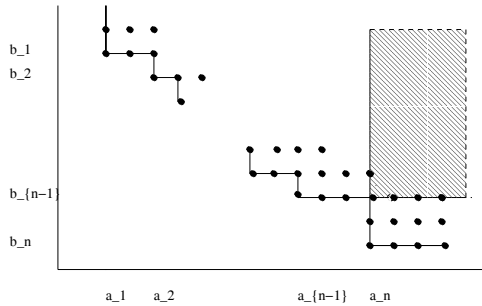


Figure 3.2.1. Graphical representation of the ideal intersections

Let

$$A = \{(a, b) \in \mathbb{Z}^2 \mid x^a y^b \in I^{(n-1)}\},$$

given by points in and to the left of the shaded region of Figure 3.2.1, and let

$$B = \{(a, b) \in \mathbb{Z}^2 \mid x^a y^b \in \langle x^{a_n}, y^{b_n} \rangle\},$$

given by points in and below the shaded region of Figure 3.2.1. It is easy to see that

$$A \cap B = \{(a, b) \in \mathbb{Z}^2 \mid a \geq a_n, b \geq b_{n-1}\},$$

which is the representation in \mathbb{R}^2 of the ideal $\langle x^{a_n} y^{b_{n-1}} \rangle$, given by the shaded region of Figure 3.2.1. For each positive integer i let A_i and B_i be the sets $\{(a, b) \in A \mid a + b = i\}$ and $\{(a, b) \in B \mid a + b = i\}$ respectively. Then

$$|A_i \cup B_i| = |A_i| + |B_i| - |A_i \cap B_i|,$$

where $|X|$ denotes the cardinality of the set X . Thus, the number of monomials of degree i in $I^{(n)}$ can be obtained by adding the number of monomials of degree i in $I^{(n-1)}$ to the number of monomials of degree i in $\langle x^{a_n}, y^{b_n} \rangle$ from which we subtract the number of monomials of degree i of $\langle x^{a_n} y^{b_{n-1}} \rangle$. We can then write

$$\mathcal{H}(I^{(n)}, i) = \mathcal{H}(I^{(n-1)}, i) + \mathcal{H}(\langle x^{a_n}, y^{b_n} \rangle, i) - \mathcal{H}(\langle x^{a_n}, y^{b_{n-1}} \rangle, i).$$

By taking the sums over all i 's we obtain

$$\sum_{i \geq 0} \mathcal{H}(I^{(n)}, i) t^i = \sum_{i \geq 0} \mathcal{H}(I^{(n-1)}, i) t^i + \sum_{i \geq 0} \mathcal{H}(\langle x^{a_n}, y^{b_n} \rangle, i) t^i - \sum_{i \geq 0} \mathcal{H}(\langle x^{a_n}, y^{b_{n-1}} \rangle, i) t^i.$$

□

Proof of Theorem 3.2.1. We will use an inductive argument on n . For $n = 1$ we have

$$I^{(1)} = \langle x^{a_1} y^{b_1} \rangle$$

and so

$$\mathcal{F}(R/I^{(1)}, t) = \frac{1}{(1-t)^2} (1 - t^{a_1+b_1}).$$

Suppose the theorem holds for any ideal generated by $n - 1$ monomials. Then

$$\mathcal{F}(R/I^{(n-1)}, t) = \frac{1}{(1-t)^2} (1 - \sum_{k=1}^{n-1} t^{a_k+b_k} + \sum_{k=2}^{n-1} t^{a_k+b_{k-1}}).$$

By using the lemma we obtain that

$$\mathcal{F}(I^{(n)}, t) = \mathcal{F}(I^{(n-1)}, t) + \mathcal{F}(\langle x^{a_n}, y^{b_n} \rangle, t) - \mathcal{F}(\langle x^{a_n}, y^{b_{n-1}} \rangle, t).$$

Since

$$\mathcal{F}(R/I, t) = \mathcal{F}(R, t) - \mathcal{F}(I, t),$$

for any ideal I of R , it follows that

$$\mathcal{F}(R/I^{(n)}, t) = \mathcal{F}(R/I^{(n-1)}, t) + \mathcal{F}(R/\langle x^{a_n}, y^{b_n} \rangle, t) - \mathcal{F}(R/\langle x^{a_n}, y^{b_{n-1}} \rangle, t).$$

Then we obtain

$$\begin{aligned} \mathcal{F}(R/I^{(n)}, t) &= \frac{1}{(1-t)^2} (1 - \sum_{k=1}^{n-1} t^{a_k+b_k} \\ &\quad + \sum_{k=2}^{n-1} t^{a_k+b_{k-1}}) + \frac{1}{(1-t)^2} (1 - t^{a_n+b_n}) - \frac{1}{(1-t)^2} (1 - t^{a_n+b_{n-1}}) \\ &= \frac{1}{(1-t)^2} (1 - \sum_{k=1}^n t^{a_k+b_k} + \sum_{k=2}^n t^{a_k+b_{k-1}}). \end{aligned}$$

□

3.3 Stillman & Bayer's theorem

Stillman and Bayer developed the computer algebra software Macaulay, which is one of the main tools used in algebraic geometry and commutative algebra for computing Groebner Bases, resolution of ideals, varieties, and so on. In the latest version called Macaulay 2 they improved the performance of some algorithms used by the earlier version. The algorithm used by Macaulay 2 to compute Hilbert Series of monomial ideals is based on the results of the theorem that we present in this section.

In order to introduce the general Stillman & Bayer's theorem, we first define some notation.

Definition. Let I, J be ideals in R . We define the *colon* (or *quotient*) *ideal* of I by J , denoted by $I : J$, to be

$$I : J = \{f \in k[x_1, x_2, \dots, x_n] \mid fg \in I \text{ for all } g \in J\}.$$

If m is a monomial, we define $I : m$ to be $I : \langle m \rangle$.

△

Note that by construction, $I : J$ is an ideal of $k[x_1, x_2, \dots, x_n]$.

For the next result we need the following definition.

Definition. Let f, m be monomials. Then let

$$f/m$$

denote the monomial $\frac{f}{\gcd(m, f)}$.

△

Example 3.3.1. $x_1^3 x_2 / x_1^2 = x_1 x_2$ and $x_1^3 x_2^5 / x_1 x_2 x_3 = x_1^2 x_2^4$

◇

The next proposition characterizes $I : m$ for a monomial ideal I and a monomial m .

Proposition 3.3.2. *Let $I = \langle f_1, f_2 \dots f_r \rangle$ be a monomial ideal and let m be a monomial in R .*

Then

$$I : m = \langle f_1/m, f_2/m, \dots, f_r/m \rangle.$$

Proof. Let $f \in I : m$. Then $fm \in I$, and so $fm = \sum_{i=1}^r f_i g_i$, where $g_i \in R$ for each i . Since m is a monomial, it is true that m dividing $\sum_{i=1}^r f_i g_i$ implies $m \mid f_i g_i$ for every $1 \leq i \leq r$. Let f'_i , and g'_i be such that $f'_i g'_i = m$ and $f'_i \mid f_i$, $g'_i \mid g_i$, where f'_i is the greatest common divisor of f_i and m . It then follows that

$$f = \frac{\sum_{i=1}^r (f_i g_i)}{m} = \sum_{i=1}^r \frac{f_i g_i}{f'_i g'_i}.$$

Note that f_i/m defined above is the same as f_i/f'_i , therefore,

$$f \in \langle (f_1/f'_1), (f_2/f'_2), \dots, (f_n/f'_n) \rangle,$$

implies

$$f \in \langle f_1/m, f_2/m, \dots, f_r/m \rangle.$$

Now if

$$f \in \langle (f_1/f'_1), (f_2/f'_2), \dots, (f_n/f'_n) \rangle,$$

then $f = \sum (f_i/f'_i)g_i$ for some g_i in R . We have that

$$fm = \sum (f_i/f'_i)g_i m = \sum f_i g_i (m/f'_i) = \sum f_i p_i,$$

where $p_i = g_i(m/f'_i)$, and $1 \leq i \leq r$. In conclusion,

$$fm \in \langle f_1, f_2 \dots f_r \rangle,$$

so $fm \in I$ and therefore $f \in I : m$. This ends the proof of the proposition. \square

Example 3.3.3. Let $I = \langle x_1^3 x_2^5, x_3^4, x_1 x_3^2 \rangle$ and let $m = x_1 x_2 x_3$. Then $I : m = \langle x_1^2 x_2^4, x_3^3, x_3 \rangle = \langle x_1^2 x_2^4, x_3 \rangle$. \diamond

Finally, we can state the theorem that provides an algorithm for computing the Hilbert function of general monomial ideals. The sequential algorithm that implements the theorem is used by the algebra software Macaulay 2. See [9, Proposition 2.2]

Theorem 3.3.4. *Let $I = \langle J, m \rangle$ be a monomial ideal in $k[x_1, x_2, \dots, x_d]$, with J a monomial ideal, and m a monomial of degree a . For any monomial ideal I let $n(I)$ be the numerator $p(t)$ of the Hilbert series of R/I . Then*

- i) $n(J \cap \langle m \rangle) = 1 - t^a + t^a n(J : m)$
- ii) $n(I) = n(J) - t^a n(J : m)$.

We will first prove a lemma that will be useful in proving this theorem.

Lemma 3.3.5. *Let $J = \langle f_1, f_2 \dots f_r \rangle$ be a monomial ideal, and h be a monomial in $R = k[x_1, x_2, \dots, x_n]$. Then*

$$J \cap \langle h \rangle = h [J : h].$$

Proof. Let $f \in J \cap \langle h \rangle$. Then $f = hp$ for some $p \in R$. Then $f = hp \in J$, implies that $p \in J : h$ (by definition of $J : h$), and therefore $f \in h [J : h]$.

Now let $f \in h [J : h]$. This implies $f \in \langle h \rangle$, where $p \in J : h$, which implies $f = hp \in J$, again by definition of $J : h$. We conclude $f \in J \cap \langle h \rangle$, and this ends the proof of the lemma. \square

Proof of Theorem 3.3.4. i) Let A, B be two subsets of a set C . Then

$$C/(A \cap B) = (C/A) \cup (A/(A \cap B)).$$

In our case C is the set of monomials in R , A is the set of monomials in $\langle m \rangle$, B is the set of monomials in J . We then have

$$\begin{aligned} & \{\text{monomials in } R\} / \{\text{monomials in } (\langle m \rangle \cap J)\} \\ &= \{\text{monomials in } (R/\langle m \rangle)\} \cup \{\text{monomials in } (\langle m \rangle/(\langle m \rangle \cap J))\}. \end{aligned}$$

So, the monomials in $R/(\langle m \rangle \cap J)$ are those in $R/\langle m \rangle$ and those lying in $\langle m \rangle$ but not in J . By a previous theorem we know that

$$n(\langle m \rangle) = 1 - t^a,$$

where $\deg(m) = a$. Also, by the lemma we have that

$$\langle m \rangle \cap J = m[J : m],$$

implying that

$$n(\langle m \rangle \cap J) = n(m) + n(J : m).$$

So, to count the rest of the monomials we only need to count those in $R/(J : m)$. We will now prove that $D = \langle m \rangle/m[J : m]$ is isomorphic to $R/(J : m)$. Note first that every monomial in D has degree at least $\deg(m) = a$, and so $\mathcal{H}(D, k) = 0$ for $k < a$.

Let $\phi: R/(J : m) \rightarrow D$ be such that $\phi(g) = mg$. Notice that if $g \in R/(J : m)$ then $g \notin (J : m)$, and so $mg \in \langle m \rangle / (J : m)$. Clearly ϕ is bijective, therefore we proved the isomorphism. Each monomial $f \in R/(J : m)$ with $\deg(f) = \alpha$ corresponds to a monomial $f' \in D$ with $\deg(f') = \alpha + a$. This implies that

$$n(J \cap \langle m \rangle) = 1 - t^a + t^a n(J : m),$$

and concludes the proof.

ii) We have that

$$\begin{aligned} n(I) &= n(\langle J, m \rangle) = n(J) + n(\langle m \rangle) - n(J \cap \langle m \rangle) \\ &= n(J) + 1 - t^a - (1 - t^a + t^a n(J : m)) \\ &= n(J) - t^a n(J : m). \end{aligned}$$

□

Let's view our results so far, which are special cases of this theorem.

Example 3.3.6. Let's verify Theorem 3.1.2.

Let

$$I = \langle m_1, m_2, \dots, m_k, m \rangle = \langle J, m \rangle.$$

By using ii) of Theorem 3.3.4 we have

$$\begin{aligned} n(I) &= n(\langle m_1, m_2, \dots, m_k \rangle) - t^a n(J : m) \\ &= n(\langle m_1, m_2, \dots, m_k \rangle) - t^a n(\langle m_1, m_2, \dots, m_k \rangle) \\ &= n(\langle m_1, m_2, \dots, m_k \rangle)(1 - t^a), \end{aligned}$$

which is in conformity with our result.

In the case of Theorem 3.2.1, if

$$I = \langle x^{a_1} y^{b_1}, x^{a_2} y^{b_2}, \dots, x^{a_n} y^{b_n} \rangle,$$

with a_n the minimum a_i and b_n the maximum b_i . Let the m from Theorem 3.3.4 be

$$m = x^{a_n} y^{b_n},$$

and so

$$J = \langle x^{a_1} y^{b_1}, \dots, x^{a_{n-1}} y^{b_{n-1}} \rangle.$$

Then

$$\begin{aligned} J : m &= \langle x^{a_1 - a_n}, x^{a_2 - a_n}, \dots, x^{a_{n-1} - a_n} \rangle \\ &= \langle x^{a_{n-1} - a_n} \rangle, \end{aligned}$$

since $a_1 \leq a_2, \dots \leq a_{n-1} \leq a_n$. Then by the above theorem

$$\begin{aligned} n(I) &= n(J) - t^{a_n + b_n} n(\langle x^{a_{n-1} - a_n} \rangle) \\ &= n(J) - t^{a_n + b_n} (1 - t^{a_{n-1} - a_n}). \end{aligned}$$

Notice that by repeating the method inductively the result is identical to ours. ◇

Now, given a monomial ideal $I = \langle J, m \rangle$ in three variables, we can easily deduce the form of $n(I)$, by considering the m from Theorem 3.3.4 as the monomial from the generators of I that contains the highest power of one of the variables, say x_1 . In this case, when the ‘division’ of J by m is performed, the variable x_1 vanishes, and so $J : m$ would be a monomial ideal in only two variables which we have completely classified in Theorem 3.2.1.

Example 3.3.7. Let

$$I = \langle x_1^2 x_2, x_1 x_3^4, x_2^5 \rangle,$$

and choose

$$J = \langle x_1 x_3^4, x_2^5 \rangle$$

and

$$m = \langle x_1^2 x_2 \rangle.$$

Note that m contains the highest power of the variable x_1 . Then

$$\begin{aligned} n(I) &= n(\langle J, m \rangle) \\ &= n(J) - t^3 n(\langle x_3^4, x_2^5 \rangle). \end{aligned}$$

By applying again the theorem, take

$$J_1 = \langle x_1 x_3^4 \rangle \text{ and } m_1 = \langle x_2^5 \rangle.$$

Then,

$$\begin{aligned} n(J) &= n(J_1) - t^5 n(\langle x_1 x_3^4 \rangle) \\ &= 1 - t^5 - t^5(1 - t^5). \end{aligned}$$

And now we can go back and compute $n(I)$. ◇

Having a relatively easy formula that enables us to compute the Hilbert series of a monomial ideal in 2 variables, we first attempted to find a similar formula for 3 and more variables. Unfortunately, we realized that our method does not generalize. The reason for this is that we could not find a general form of expressing the ideals that we were working with. More exactly, we could not find an ordering of the powers of each variable occurring on the monomials of a similar form to $a_1 \leq a_2 \leq \dots \leq a_n$, and $b_1 \leq b_2 \leq \dots \leq b_n$ that occurs in the two-variable case. So for three or more variables we only can make repeated use of the Stillman & Bayer’s theorem presented above.

3.4 From Hilbert series to Modules and Resolutions

Until now we have proved theorems using mostly combinatorial means. In almost every proof we have presented so far, we computed Hilbert series by computing the Hilbert function as the number of monomials in each homogeneous component.

There is another classical way of computing the Hilbert functions and Hilbert series of monomial ideals. We are only going to sketch this approach in the current section, without providing the necessary background for now. We do so to motivate our further work in the area of homological algebra.

We will start by presenting an example that illustrates some of the concepts that we will be working with.

Example 3.4.1. Let $R = k[x, y]$ and let $I = \langle x, y \rangle \subset R$. We will compute a free resolution of I , that is, a sequence of free modules R^i and maps between these modules

$$\dots \rightarrow R^{n_i} \xrightarrow{f_i} R^{n_{i-1}} \xrightarrow{f_{i-1}} \dots \xrightarrow{f_1} I \rightarrow 0.$$

We also need the sequence to be exact, that is, $\text{im}(f_i) = \ker(f_{i-1})$. Since we have two generators of I , choose the first free module in the sequence to be R^2 and let $f_1: R^2 \rightarrow I$, be defined by $f_1(e_1) = x$, and $f_1(e_2) = y$, where e_1, e_2 are the standard basis in R^2 , namely $e_1 = (1, 0), e_2 = (0, 1)$.

We now need to find the number of generators of $\ker(f_1)$. With a bit of work one can prove that $e_{12} = (-y, x)$ generates the kernel of f_1 , and so, we choose the second module in the sequence to be R . Now define $f_2: R \rightarrow R^2$ by $f_2(1) = e_{12}$. Since $\ker(f_2) = 0$, we take the last module in the sequence to be 0. So we have obtained the following free resolution of I

$$0 \xrightarrow{f_3} R \xrightarrow{f_2} R^2 \xrightarrow{f_1} I \rightarrow 0.$$

Notice that the degrees of the generating monomials of I and of $\ker(f_1)$ are 1. In the next chapter we will formally define modules that are denoted by $R(d)$ for some integer d . For now, you should just know that this notation keeps track of degrees of generators, and it is called a shifting in the grading of R . What the notation $R(d)$ basically means is that all the polynomials of degree t in R are considered of degree $d+t$ in $R(d)$. Another way of presenting the above free resolution, by keeping track of the degrees of the generators of the kernels of these maps, is

$$0 \xrightarrow{f_3} R(-1) \xrightarrow{f_2} R(-1)^2 \xrightarrow{f_1} I \rightarrow 0.$$

Having the resolution of I and the shift in grading, by a theorem that we will prove later, we can compute the Hilbert function of I , as

$$\mathcal{H}(I, i) = \mathcal{H}(R(-1)^2, i) - \mathcal{H}(R(-1), i),$$

where i is a positive integer. Thus, knowing $\mathcal{H}(I, m)$ one can easily compute $\mathcal{H}(R/I, m)$ and $\mathcal{F}(I, t)$. \diamond

In general for any ideal I of R , it is a fact that there exists a free resolution of I , that is, an exact sequence of free modules and homomorphisms

$$0 \xrightarrow{f_{r+2}} R^{n_r} \xrightarrow{f_{r+1}} R^{n_{r-1}} \xrightarrow{f_r} \dots \xrightarrow{f_3} R^{n_1} \xrightarrow{f_2} R^{n_0} \xrightarrow{f_1} I \xrightarrow{f_0} 0,$$

where the R^{n_i} 's are free modules and the arrows represent the existence of homomorphisms between these modules. The sequence is defined iteratively, by taking R^{n_1} to be the free module that contains the kernel of f_1 , and similarly R^{n_2} as the kernel of f_2 and so on. Moreover, the sequence contains a lot of information about the structure of the ideal and about its grading, as we have seen in the above example. In this general case of a degree 0 map, one can compute the Hilbert functions of I in the following way

$$\mathcal{H}(R/I, i) = \mathcal{H}(R, i) - \sum_{j=0}^r (-1)^j \mathcal{H}(R^{n_j}, i).$$

We will provide a proof of the above equality in the next chapter.

Now that we have introduced the concepts of resolution and module we are going to present them in a more formal way. In the next chapter we will go a bit astray from the Hilbert functions and Hilbert series, and try to achieve an understanding of the new theory tasted in this section.

4

Modules, Syzygies and Resolutions

4.1 Modules

In this section we move from the Hilbert Series area to a different interest domain, that of modules over polynomial rings. We will first provide a friendly introduction to the field and present further areas of interest. Our approach is faithful to the one of [7].

A module is an algebraic structure that behaves over a ring in a similar way to the way a vector space behaves over a field. In a more formal way we describe modules over a ring as it follows.

Definition. A *module over a ring* R (or R -module) is a set M together with an action $R \times M \rightarrow M$ (the image of (r, a) being denoted by ra) satisfying the following properties for all $r, s \in R$ and $a, b \in M$.

- 1) M is abelian group under addition.
- 2) $r(a + b) = ra + rb$
- 3) $(r + s)a = ra + sa$.
- 4) $r(sa) = (rs)a$.
- 5) if 1_R is the multiplicative identity in R , then $1_R a = a$ for all $a \in M$. \triangle

Note that if R is a field then the properties above describe a vector space.

One of the differences between vector spaces and modules is that, while a vector space always has a basis (assuming the Axiom of Choice), modules might not have one. For example, consider the ideal $I = \langle x^2, y^4 \rangle$ in $k[x, y]$. Note that I is a vector space over k , and that x^2, y^4 are linearly independent over k . Now consider I as a module $\langle x^2, y^4 \rangle$ over $R = k[x, y]$. In this case x^2 and y^4 are the generators of the module, but there exist polynomials $f = -y^4, g = x^2$ such that $fx^2 + gy^4 = 0$. Therefore, x^2 and y^4 do not form a basis for the module M .

Given a ring R , a simple check shows R is a module over itself. Also, R^n is an R -module, with the addition and scalar multiplication operations being the component-wise ones. By a simple verification of the properties of a module given in Definition 4.1 one can deduce that if I is an ideal of a ring R , then I and R/I are R -modules. This fact entitles one to say that modules are generalizations of ideals.

We have seen above that modules do not always have linearly independent generating sets or base. The modules that do have linearly independent generators are called free.

Definition. A module M over a ring R is said to be *free* if it has a basis. \triangle

Example 4.1.1. Let R be a ring and let $M = R^n$. Then R is a free module with the standard basis

$$\begin{aligned} e_1 &= (1, 0, 0 \dots 0) \\ e_2 &= (0, 1, 0 \dots 0) \\ &\vdots \\ e_n &= (0, 0, 0, \dots 1). \end{aligned}$$

\diamond

Definition. An R -module homomorphism between two R -modules M and N is an R -linear map between M and N . More precisely, $\phi : M \rightarrow N$ is an R -module homomorphism if for all $a \in R$ and all f, g in M , we have

$$\phi(af + g) = a\phi(f) + \phi(g).$$

\triangle

We recall next the definitions of the kernel and image of a map of modules, which are identical to the similar definitions of maps between other algebraic structures such as groups and rings.

Definition. Let $\phi : M \rightarrow N$ be an R -module homomorphism. We define the *kernel* of ϕ , denoted $\ker(\phi)$, to be

$$\ker(\phi) = \{f \in M \mid \phi(f) = 0\},$$

and the *image* of ϕ , denoted $\text{im}(\phi)$, to be

$$\text{im}(\phi) = \{g \in N \mid \text{there exists } f \in M \text{ with } \phi(f) = g\}.$$

A *submodule* of the module M is a set $M' \subset M$ such that M' is a module with the same operation as in M . \triangle

A simple verification using the definition of a module proves the following proposition.

Proposition 4.1.2. Let $\phi : M \rightarrow N$ be an R -module homomorphism, where M, N are R -modules. Then $\ker(\phi)$ and $\text{im}(\phi)$ are submodules of M and N respectively.

Example 4.1.3. Let $R = k[x, y]$, and let M be the set of all solutions $(x_1, x_2, x_3) \in R^3$ of the linear equation

$$xX_1 + (y^3 - 5)X_2 + X_3 = 0.$$

Then M is a free R -module and it has a basis $b_1 = (0, 1, 5 - y^3)$ and $b_2 = (1, 0, -x)$. We prove this as follows. Let (f_1, f_2, f_3) be a solution of the equation. Then

$$f_3 = -xf_1 + (5 - y^3)f_2 = f_1b_1 + f_2b_2.$$

Therefore, $\{b_1, b_2\}$ is a generating set of M . Now suppose there exists $f, g \in R$ such that $fb_1 = gb_2$. Then we would have that $g = 0, f = 0$, so b_1 and b_2 are linearly independent over R , and therefore $\{b_1, b_2\}$ form a basis for the module M . \diamond

4.2 Syzygies

In the last section we saw that the kernel of a map between modules is itself a module. Algebraists harbor a special interest in kernels of maps and their generators. Our short introduction to the theory of resolutions given in the previous chapter suggests the fact that the sequence of kernels of homomorphisms starting with some module M in R^m plays an important role in computing Hilbert series. Another definition for the kernel module is the syzygy module.

Definition. Let $M \subset R^m$ be the module generated by the set $F = \{f_1, f_2, \dots, f_s\}$. The *syzygy module* of F , denoted by $\text{Syz}(F)$ (also denoted by $\text{Syz}(f_1, f_2, \dots, f_s)$) is the set

$$\text{Syz}(f_1, f_2, \dots, f_s) = \{(g_1, g_2, \dots, g_s) \in R^s \mid f_1g_1 + f_2g_2 + \dots + f_s g_s = 0\}.$$

An element of $\text{Syz}(F)$ is called a *syzygy*. \triangle

In other words, $\text{Syz}(f_1, f_2, \dots, f_s)$ is the kernel of the map $R^s \rightarrow M$ given by $e_i \mapsto f_i$. Syzygies are sometimes called *relations*, and so $\text{Syz}(F)$ is also called the *module of relations* of M .

We now introduce some notation regarding the generators of a module.

Definition. Let $M \subset R^m$ be the module generated by the set $F = \{f_1, f_2, \dots, f_s\}$. Suppose also that $f_i = (f_{i1}, f_{i2}, \dots, f_{im})^T$. Then we will let the matrix $\text{mat}(M)$ be as follows

$$\text{mat}(M) = \begin{pmatrix} f_{11} & f_{21} & \dots & f_{s1} \\ f_{12} & f_{22} & \dots & f_{s2} \\ \vdots & \vdots & \vdots & \vdots \\ f_{1m} & f_{2m} & \dots & f_{sm} \end{pmatrix}$$

and say that $mat(M)$ is the *generating matrix* of M . In fact $mat(M)$ is the image of the map $R^s \rightarrow R^m$ given by $e_i \mapsto f_i$. \triangle

In order to better understand this new concept we will further present an example. We will use Macaulay 2 to compute the syzygy module, since the algorithm described in [7] is tedious and is not pertinent to our interest in this paper.

Example 4.2.1. Let

$$m = \begin{pmatrix} x^3y & x & y \\ y^2 & y & y^3x \end{pmatrix}$$

be the generating matrix $mat(M)$ of the module $M \subset k[x, y]$. We will present here the Macaulay 2 sequence of commands that would produce the syzygy of the module generated by the matrix m . The lines that start with i represent the command-lines, and those starting with o represent the output:

```
i1 : R = QQ[x, y]
o1 = R
o1 : PolynomialRing
i2 : m = matrix{{x^3 * y, x, y}, {y^2, y, y^3 * x}}
o2 = | x3y x y |
      | y2 y xy3 |
o2 : Matrix R^2 < -- -R^3
i3 : syz m
o3 = {4} | -x2y2 + y - x2y + 1 |
      {1} | x4y3 - y2 x4y2 - y |
      {4} | -x3y + xy - x3 + x |
o3 : Matrix R^2 < -- -R^3.
```

This tells us that the the module of syzygies of m is the module generated by the columns of the above matrix $o3$, namely

$$b_1 = (-x^2y^2 + y, x^4y^3 - y^2, -x^3y + xy)^T \text{ and}$$

$$b_2 = (-x^2y + 1, x^4y^2 - y, -x^3 + x)^T.$$

Note that, for the matrices $o2$, and $o3$ obtained from the above commands, it is true that

$$o2 \ o3 = 0_{2 \times 2},$$

where $0_{2 \times 2}$ is the 2×2 zero matrix. Therefore, b_1 and b_2 are indeed syzygies for the module generated by m . \diamond

4.3 Freeness of modules generated by matrices in polynomial rings

In an attempt to better understand when a module is or is not free, we considered particular modules, such as those generated by polynomials in one variable, and those generated by r -tuples of polynomials in n variables. The work done in this section consists of my results.

Recall that a module is free if and only if it has a basis. That is, a module is free with a given generating set as a basis, if the only syzygy on the generating elements is the trivial one. In this case the syzygy module is 0. Notice that when the module M is generated by a single element, then M is free.

Theorem 4.3.1. *Let $R = k[x]$ and let*

$$I = \langle p_1, p_2, \dots, p_k \rangle \subseteq R$$

be an ideal in R . Then I is free, viewed as a module over R .

Proof. Since I is an ideal of R , and we know that $R = k[x]$ is a Principal Ideal Domain, we have that all ideals are generated by a single element. Therefore, I is free, for any polynomials $p_i \in R$. \square

A more complicated situation occurs if $M \subseteq R^n$ for some n . A similar result can be obtained in this case, and it is given by the following theorem

Theorem 4.3.2. *Let $R = k[x]$ and $M \subset R^t$ be a module. Then M is free.*

For a proof of 4.3.2, see [6, Theorem 3.7].

We now turn our attention to the more general case of a polynomial ring in p variables.

Theorem 4.3.3. *Let m be an $n \times n$ matrix with entries in R , where $R = k[x_1, x_2, \dots, x_p]$, such that the columns of m generate the module M . If $\det(m) \neq 0$ then M is free.*

Proof. Let

$$m = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}.$$

Let

$$v = (v_1, v_2, \dots, v_n)^T$$

be a syzygy on the columns of m . Then

$$m \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

We have that

$$\begin{aligned}
v_1 \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} &= \begin{vmatrix} v_1 a_{11} & a_{12} & \dots & a_{1n} \\ v_1 a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \dots \\ v_1 a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} \\
&= \begin{vmatrix} v_1 a_{11} + v_2 a_{12} + \dots + v_n a_{1n} & a_{12} & \dots & a_{1n} \\ v_1 a_{21} + v_2 a_{22} + \dots + v_n a_{2n} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ v_1 a_{n1} + v_2 a_{n2} + \dots + v_n a_{nn} & a_{n2} & \dots & a_{nn} \end{vmatrix} \\
&= \begin{vmatrix} 0 & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ 0 & a_{n2} & \dots & a_{nn} \end{vmatrix} = 0.
\end{aligned}$$

So we have obtained that

$$v_1 \det(m) = 0.$$

Since R is an integral domain, and $\det(m) \neq 0$, then it must be the case that $v_1 = 0$, so v_1 is the zero polynomial. From a similar argument it follows that $v_2 = 0, v_3 = 0, \dots, v_n = 0$. Therefore, there is no nontrivial syzygy on the columns of m , and so there is no nontrivial syzygy of the generators of M , thus M is free. \square

The case when the determinant of the generating matrix is 0 is more complicated.

We will only look at 2×2 matrices of polynomials in r variables, where $r \geq 2$, since we have already discussed freeness of modules in $k[x]$ (see Theorem 4.3.2).

Theorem 4.3.4. *Let*

$$m = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix},$$

where the a_{ij} 's are polynomials in $R = k[x_1, x_2, \dots, x_n]$, with $n \geq 2$ and $\det(m) = 0$. Then the module M generated by m is free.

Proof. Since $\det(m) = 0$ we will have that

$$a_{11}a_{22} = a_{12}a_{21}.$$

Since R is a unique factorization domain, the a_{ii} 's must factor uniquely as

$$a_{11} = f_1 f_2 \cdots f_m$$

$$a_{22} = g_1 g_2 \cdots g_r,$$

where the f_i 's and g_i 's are irreducible over R . Then, it follows that a_{12} , a_{21} are each a combination of products of the factors f_i and g_j . If no factors of a_{22} occur in a_{21} , then a_{11} must divide a_{12} . In this case we can deduce that $a_{21} \mid a_{22}$, and therefore one column of m is multiple of the other, implying that M is generated by a single element. In this case there is no syzygy on this generator, and so M is free.

Now suppose without loss of generality that

$$a_{21} = f_1 f_2 \cdots f_k g_1 g_2 g_{k_0},$$

and so

$$a_{12} = f_{k+1} \cdots f_m g_{k_0+1} \cdots g_r.$$

Then, let

$$f = f_1 f_2 \cdots f_k, \text{ and } f' = f_{k+1} \cdots f_m,$$

and let

$$g = g_1 g_2 g_{k_0}, \text{ and } g' = g_{k_0+1} \cdots g_r.$$

It follows that

$$m = \begin{pmatrix} f f' & g f' \\ f g' & g g' \end{pmatrix}.$$

Note that there exists a syzygy on the generators of M , namely $(-g, f)^T$. However this does not necessarily mean that M is not free.

Let $b_1 = f \begin{pmatrix} f' \\ g' \end{pmatrix}$ and $b_2 = g \begin{pmatrix} f' \\ g' \end{pmatrix}$ be the generators of M .

Let $d = \gcd(f, g)$. We will show that M is generated by

$$c = d \begin{pmatrix} f' \\ g' \end{pmatrix}.$$

Let N be the module generated by c . It is easy to see that $M \subseteq N$ since $d \mid f$, and $d \mid g$, implying that any element that can be written as a linear combination of b_1 and b_2 can be written as a multiple of c also. We need now prove that $N \subseteq M$. Let $p = c\alpha = d \begin{pmatrix} f' \\ g' \end{pmatrix} \alpha$, be an element of M . Since $d = \gcd(f, g)$, there exist polynomials β_1 and β_2 such that $d = \beta_1 f + \beta_2 g$. Then

$$\begin{aligned} p &= \alpha(\beta_1 f + \beta_2 g) \begin{pmatrix} f' \\ g' \end{pmatrix} \\ &= \alpha\beta_1 f \begin{pmatrix} f' \\ g' \end{pmatrix} + \alpha\beta_2 g \begin{pmatrix} f' \\ g' \end{pmatrix} \\ &= \alpha\beta_1 b_1 + \alpha\beta_2 b_2. \end{aligned}$$

Therefore, $N \subseteq M$ and since $M \subseteq N$, we obtain $M = N$. This proves that M is generated by only one element, thus M is free. \square

Corollary 4.3.5. *If m is a 2×2 matrix with entries polynomials in n -variables generating the module M , then M is free.*

Proof. The proof follows by putting together the results of Theorem 4.3.3 and Theorem 4.3.4. \square

Conjecture 4.3.6. *A $n \times n$ matrix m with $\det(m) = 0$ generates a free module M iff each column vector is a multiple of one fixed column vector, say v_1 , that is, if M is generated by only one element.*

4.4 Resolutions of Modules

As we have seen in the previous sections, given a module M generated by a set of elements $f_1, f_2 \dots f_m$, it is important to know what relations these generators satisfy, this is, to know $Syz(f_1, f_2, \dots, f_m)$. By knowing this we have more information about the module itself, such as if it is free or not, what its graded structure is, if any, and so on. In order to know about the module $S_1 = Syz(f_1, f_2 \dots f_m)$, we need to have some knowledge of the generators of S_1 and also of the syzygy module on the generators of S_1 , called the second syzygy module, and so on. In this way we need to consider the sequence of generators and syzygies, called a resolution of M .

Definition. Let $F = \{f_1, f_2 \dots f_m\}$ be a set of polynomials in R^s . We denote by $Syz_i(F)$ the i th syzygy module of F , as it is described above. \triangle

Our goal is to show how resolutions play an important role in the theory of Hilbert series.

We will start by formally introducing the concept of an exact sequence.

Definition. Consider a sequence of R -modules and homomorphisms

$$\dots M_{i+1} \xrightarrow{f_{i+1}} M_i \xrightarrow{f_i} M_{i-1} \rightarrow \dots$$

We say that the sequence is *exact* at M_i if $im(f_{i+1}) = ker(f_i)$. The whole sequence is *exact* if it is exact at each M_i . \triangle

Some observations can be easily proven.

1. The sequence

$$M \xrightarrow{f} N \rightarrow 0$$

is exact iff f is surjective.

2. The sequence

$$0 \rightarrow M \xrightarrow{f} N$$

is exact iff f is injective.

3. The sequence

$$0 \rightarrow M \xrightarrow{f} N \rightarrow 0$$

is exact iff f is bijective.

Given a homomorphism $f: M \rightarrow N$ one can construct an exact sequence as follows in the next proposition

Proposition 4.4.1. *For any R -module homomorphism $f: M \rightarrow N$, we have an exact sequence*

$$0 \rightarrow \ker(f) \xrightarrow{f_1} M \xrightarrow{f} N \xrightarrow{f_0} \operatorname{coker}(f) \rightarrow 0,$$

where $\operatorname{coker}(f) \cong N/\operatorname{im}(f)$.

For a proof of the above see [7].

Definition. Let M be an R -module. A *presentation* for M is a generating set f_1, f_2, \dots, f_t for M , together with a set of generators for the syzygy module $\operatorname{Syz}(f_1, f_2, \dots, f_t)$. A presentation matrix A of M is the matrix obtained by writing the generators of $\operatorname{Syz}(f_1, f_2, \dots, f_t)$ as the columns of A . \triangle

Another way of seeing a presentation is by means of an exact sequence of the form

$$R^s \xrightarrow{g_1} R^t \xrightarrow{g_0} M \rightarrow 0,$$

where s is the cardinality of a set of generators for $\operatorname{Syz}(f_1, f_2, \dots, f_t)$, where g_0 is the generating matrix of M , and g_1 is given by the presentation matrix A of M .

Note that the presentation of M might not be unique.

In some of the sequences above, we had that the occurring modules were of the form R^m . We now define them formally as below.

Definition. Let M be an R -module. A *free resolution* of M is an exact sequence of the form

$$\dots \rightarrow F_2 \xrightarrow{f_2} F_1 \xrightarrow{f_1} F_0 \xrightarrow{f_0} M \rightarrow 0,$$

with $F_i \cong R_i^r$ for some $r \in \mathbb{N}$ for all i . The resolution is *finite* if there exists some integer l such that $F_l \neq 0$ and $F_i = 0$ for $i > l$. In this case the resolution is called of *length* l and it is written as

$$0 \rightarrow F_l \rightarrow F_{l-1} \rightarrow \dots \rightarrow F_2 \rightarrow F_1 \rightarrow F_0 \rightarrow M \rightarrow 0.$$

\triangle

Here is an example of a finite free resolution of an ideal in R .

Example 4.4.2. Let

$$I = \langle z^3 - yw^2, yz - xw, y^3 - x^2z, xz^2 - y^2w \rangle$$

be an ideal in $R = k[x, y, z, w]$.

We will form a free resolution of I . Using Macaulay 2, one can compute the generators of Syz_i , the i th syzygy module. The following are the results:

$$Syz_1 = \begin{pmatrix} 0 & -x & 0 & -y \\ xz & yw & y^2 & z^2 \\ -w & 0 & -z & 0 \\ -y & z & -x & w \end{pmatrix}$$

and

$$Syz_2 = \begin{pmatrix} -z \\ -y \\ w \\ x \end{pmatrix}.$$

Thus, since M has 4 generators and Syz_1 has also 4 generators, then

$$R^4 \rightarrow R^4 \rightarrow I \rightarrow 0$$

is a sequence contained in the free resolution of I . Now, since the second syzygy module is generated by one element, we conclude that a finite free resolution of I is

$$0 \rightarrow R \rightarrow R^4 \rightarrow R^4 \rightarrow I \rightarrow 0.$$

◇

The question that can be raised from the above is does there exist a finite resolution for any R -module? The answer is no, in general. However, for polynomial rings the answer is yes, as asserted by the following theorem, which is proved in [7, Theorem 2.1].

Theorem 4.4.3 (Hilbert Syzygy Theorem). *Let $R = k[x_1, x_2, \dots, x_n]$. Then every finitely generated R -module has a finite free resolution of length at most n .*

Notice that the theorem asserts the existence of such a resolution.

We will again not produce a proof of the Hilbert Syzygy Theorem since it involves technical details that are not relevant in our study.

4.5 Resolutions of Graded Modules

It turns out that more information about the structure of a module can be retrieved from its resolution if the module is graded. Recall from Chapter 2 that $R = k[x_1, x_2, \dots, x_n]$ is a graded algebra and can be written as

$$R = \bigoplus_{i=0}^{\infty} R_i,$$

where the R_i 's are k -vector spaces of homogeneous polynomials of degree i , and $R_i R_j \subset R_{i+j}$.

We need to define formally what a graded module is. The definition of a graded module is very similar to the definition of graded algebras given in Chapter 2.

Definition. A *graded module* over a graded algebra R is a module M and a family of vector spaces M_t , with $t \in \mathbb{Z}$ that satisfy the following properties

1. $M = \bigoplus_{t \in \mathbb{Z}} M_t$
2. $R_s M_t \subset M_{s+t}$ for all $s \geq 0$ and $t \in \mathbb{Z}$.

The elements of M_t are called *homogeneous of degree t* . △

The most familiar examples of graded modules are homogeneous ideals I and their quotient rings R/I . Also, the free modules R^m are graded modules, since by defining $(R^m)_t = (R_t)^m$ we obtain a grading, that is, the elements of $(R^m)_t$ are the m -tuples whose entries are homogeneous elements of degree t .

In order to compute the Hilbert function of a module, as we will see later in this section, we will need to know a free resolution of M . One condition that needs to take place in order for the computation to be possible is to have the homomorphisms between the free modules carry elements in the domain to elements of the same degree in the codomain. These homomorphisms will be called of degree 0. We will give a formal definition of graded homomorphisms later in the section. Now, in order to get from any free resolution to one where all the homomorphisms are of degree 0, one needs to perform a shifting in the grading of the free modules occurring in the resolution. This means that if a monomial in R is of degree t , then by applying a shifting by d , denoted by $R(d)$, the same monomial in $R(d)$ would be of degree $t + d$. Below we formalize all these new ideas and concepts.

Proposition 4.5.1. *Let M be a graded R -module, and let d be an integer. Let $M(d)$ be the direct sum*

$$M(d) = \bigoplus_{t \in \mathbb{Z}} M(d)_t,$$

where $M(d)_t = M_{d+t}$. Then $M(d)$ is also a graded R -module.

Proof. Since M is a graded module, then $M = \bigoplus_{r \in \mathbb{Z}} M_r$, with each M_r an additive subgroup and such that $R_s M_r \subset M_{r+s}$. We then have that M_{d+t} is an element of $\{M_r \mid r \in \mathbb{Z}\}$, and so M_{d+t} is an additive subgroup of $M(d)$. Also $R_s M_{d+t} \subset M_{s+d+t}$ since M is a graded module. This ends the proof, so we can conclude that $M(d)$ is a graded module. □

The graded module $(R^m)(d)$ has the same standard basis as R^m , but since $R(d)_{-d} = R_0$, the standard basis of $R^m(d)$ is homogeneous of degree $-d$. The module $R(d)$ is called *shifted* or *twisted*, and d is called the *shifting* or the *twist*.

Proposition 4.5.2. *Given integers d_1, d_2, \dots, d_m , then*

$$M = R(d_1) \oplus R(d_2) \oplus \dots \oplus R(d_m)$$

is a graded, free module, where the basis elements are homogeneous of degree $-d_i$ for $1 \leq i \leq m$.

Proof. Since each $R(d_i)$ is nothing else but the module R where the degrees have been shifted by the constant d_i , it follows that $R(d_i)$ is isomorphic to R , for any i , so $R(d_1) \oplus R(d_2) \oplus \cdots \oplus R(d_m)$ is isomorphic to R^m , and therefore it is free.

Now let $M_t = R(d_1)_t \oplus R(d_2)_t \oplus \cdots \oplus R(d_m)_t$. We will show that M_t defines a graded structure on M . Since as we have seen above $R(d_i)$ is a graded module, for each i we have that

$$R(d_i) = \bigoplus_{r \in \mathbb{Z}} R(d_i)_r.$$

Therefore,

$$\begin{aligned} M &= (\bigoplus_{r \in \mathbb{Z}} R(d_1)_r) \oplus (\bigoplus_{r \in \mathbb{Z}} R(d_2)_r) \oplus \cdots \oplus (\bigoplus_{r \in \mathbb{Z}} R(d_m)_r) \\ &= \bigoplus_{t \in \mathbb{Z}} (R(d_1)_t \oplus R(d_2)_t \oplus \cdots \oplus R(d_m)_t) \\ &= \bigoplus_{t \in \mathbb{Z}} M_t. \end{aligned}$$

Now

$$\begin{aligned} R_s M_t &= R_s(R(d_1)_t \oplus R(d_2)_t \oplus \cdots \oplus R(d_m)_t) \\ &= R_s R(d_1)_t \oplus R_s R(d_2)_t \oplus \cdots \oplus R_s R(d_m)_t \\ &\subset R(d_1)_{t+s} \oplus R(d_2)_{t+s} \oplus \cdots \oplus R(d_m)_{t+s} \\ &= M_{t+s}. \end{aligned}$$

This concludes the proof of the proposition. \square

Other important concepts that we need to define are *graded homomorphism* and *degree of a homomorphism*. Here are the formal definitions.

Definition. Let M and N be graded modules over R . A homomorphism

$$\phi : M \rightarrow N$$

is said to be a *graded homomorphism of degree d* if

$$\phi(M_t) \subset N_{t+d}$$

for all $t \in \mathbb{Z}$. \triangle

Theorem 4.5.3. *Let*

$$M = \langle f_1, f_2, \dots, f_m \rangle$$

be a graded R -module and suppose the polynomials f_i are homogeneous of degree d_i . Then the following homomorphism is graded of degree 0

$$\phi : R(-d_1) \oplus R(-d_2) \oplus \cdots \oplus R(-d_m) \rightarrow M,$$

where $\phi(e_i) = f_i$, with the e_i 's being the standard basis elements of R^m , but $\deg(e_i) = d_i$. Also ϕ is a surjective function.

Proof. From proposition 4.5.2 we have that the degree of e_i is d_i in the module $R(-d_1) \oplus R(-d_2) \oplus \dots \oplus R(-d_m)$. Let

$$\begin{aligned} N_t &= R(-d_1)_t \oplus R(-d_2)_t \oplus \dots \oplus R(-d_m)_t \\ &= R_{t-d_1} \oplus R_{t-d_2} \oplus \dots \oplus R_{t-d_m}. \end{aligned}$$

Let $g = (g_1, g_2, \dots, g_m) \in N_t$, meaning that each g_i has degree $t - d_i$. Then

$$g = g_1 e_1 + g_2 e_2 + \dots + g_m e_m,$$

and

$$\phi(g) = g_1 f_1 + g_2 f_2 + \dots + g_m f_m \in M.$$

Since $\deg(g_i f_i) = \deg(g_i) + \deg(f_i) = t - d_i + d_i = t$ then

$$\phi(g) \in M_t = M_{t+0}.$$

This concludes the proof that ϕ is graded of degree 0. Moreover, since for any $h \in M$, there exist h_1, h_2, \dots, h_m such that

$$h = h_1 f_1 + \dots + h_m f_m,$$

then there exists

$$h' = h_1 e_1 + \dots + h_m e_m \in R(-d_1) \oplus R(-d_2) \oplus \dots \oplus R(-d_m).$$

Therefore ϕ is onto, and this completes the proof of the proposition. \square

Similarly, more general graded homomorphisms can be proven to exist. For example

Theorem 4.5.4. *i) Let A be an $m \times p$ matrix with all the entries homogeneous polynomials of degree d in R . Then*

$$\phi: R^p \rightarrow R^m,$$

defined by

$$\phi(f) = Af$$

for all $f \in R^p$, is a graded homomorphism of degree d .

ii) Let A be a matrix such that each column i has entries homogeneous polynomials of degree d_i . Then

$$\phi: R(-d_1) \oplus R(-d_2) \oplus \dots \oplus R(-d_p) \rightarrow R^m,$$

defined by

$$\phi(f) = Af$$

for all $f \in R(-d_1) \oplus R(-d_2) \oplus \cdots \oplus R(-d_p)$, is a graded homomorphism of degree 0. Note that the d_i 's can vary from column to column.

iii) Let A be a matrix such that the element a_{ij} for each i, j is a homogeneous polynomial of degree $d_j - c_i$ in R . Then

$$\phi: R(-d_1) \oplus R(-d_2) \oplus \cdots \oplus R(-d_p) \rightarrow R(-c_1) \oplus R(-c_2) \oplus \cdots \oplus R(-c_m),$$

defined by

$$\phi(f) = Af$$

for all $f \in R(-d_1) \oplus R(-d_2) \oplus \cdots \oplus R(-d_p) \rightarrow R(-c_1)$ is a graded homomorphism of degree 0.

We will not include the details of the proofs in here, but the ideas used are the same as in the Theorem 4.5.3. Notice that the theorem asserts what shiftings we should perform in order to obtain the 0-degree homomorphisms that we need for computational reasons.

We call the matrix A from Theorem 4.5.4 a graded matrix. We have by now acquired most of the necessary information to go back to the Hilbert series. We are now in the position of understanding a new means of computing Hilbert functions. But before that, we introduce a new definition which we will discuss in detail in an example.

Definition. If M is a graded R -module, then a *graded resolution* of M is a resolution of the form

$$\cdots \rightarrow F_2 \xrightarrow{\phi_2} F_1 \xrightarrow{\phi_1} F_0 \xrightarrow{\phi_0} M \rightarrow 0,$$

where the F_i 's are twisted free graded modules of the form $R(-d_1) \oplus \cdots \oplus R(-d_p)$, and the homomorphisms between them are graded of degree 0. In this case the ϕ_i 's are given by the graded matrices described in the Theorem 4.5.4. \triangle

Example 4.5.5. We will now form a graded resolution of the ideal from example 4.4.2. Recall that

$$I = \langle z^3 - yw^2, yz - xw, y^3 - x^2z, xz^2 - y^2w \rangle,$$

so I is a homogeneous ideal of $R = k[x, y, z, w]$.

Then by Theorem 4.5.3 we have that there exists a graded homomorphism of degree 0 of the form

$$R(-3) \oplus R(-2) \oplus R(-3)^2 \rightarrow M.$$

Here, the shifting in degrees are the respective degrees of the generators. Now, recall that the first syzygy matrix was

$$A = \begin{pmatrix} 0 & -x & 0 & -y \\ xz & yw & y^2 & z^2 \\ -w & 0 & -z & 0 \\ -y & z & -x & w \end{pmatrix}.$$

We want to use Theorem 4.5.4 in order to find a graded module F_1 such that there exists a homomorphism

$$F_1 \rightarrow R(-3) \oplus R(-2) \oplus R(-3)^2.$$

So we need take $c_1 = c_3 = c_4 = 3$, and $c_2 = 2$. Now suppose A is the graded matrix that defines the wanted homomorphism. Then, with a little bit of computation we obtain $d_1 = d_2 = d_3 = d_4 = -4$, so the following is a homomorphism degree 0

$$R(-4)^4 \xrightarrow{A} R(-3) \oplus R(-2) \oplus R(-3)^2.$$

Now, again the second syzygy module is defined by

$$B = \begin{pmatrix} -z \\ -y \\ w \\ x \end{pmatrix}.$$

We want to make B the graded matrix that defines a graded homomorphism of degree 0 of the form

$$R(a_1) \oplus \cdots \oplus R(a_k) \xrightarrow{B} R(-4)^4.$$

Since B has only one column then $k = 1$. In this case, applying Theorem 4.5.3 we have that $c_1 = c_2 = c_3 = c_4 = 4$. Also, the column of B is homogeneous of degree 1. So $d_i - c_i = 1$, implying $d_i = 5$, and so,

$$R(-5) \rightarrow R(-4)^4,$$

is the wanted graded homomorphism. By putting everything together we obtain the following graded resolution of M .

$$0 \rightarrow R(-5) \rightarrow R(-4)^4 \rightarrow R(-3) \oplus R(-2) \oplus R(-3)^2 \rightarrow M \rightarrow 0.$$

We can now compare it to the classical resolution computed in the Example 4.4.2, given by

$$0 \rightarrow R \rightarrow R^4 \rightarrow R^4 \rightarrow M \rightarrow 0.$$

We must notice that the graded resolution provides us with a better insight in the structure of M than the classical one. The resolution tells us now what are the degrees of the polynomials occurring in the syzygies modules and also, it tells us how many generators these syzygy modules have. We will see later how easy it will be to compute Hilbert functions knowing a graded free resolution of a module. \diamond

One more helpful fact we know about graded resolutions is described in the the Graded Hilbert Syzygy Theorem that we cite from [7] below.

Theorem 4.5.6. *Graded Hilbert Syzygy Theorem* Let $R = k[x_1, x_2, \dots, x_n]$. Then every finitely generated graded R -module has a finite graded resolution of length at most n .

4.6 Computing Hilbert Functions

In this section we will show how to compute the Hilbert function of a graded module knowing the shifts. We will end up by proving that the Hilbert and Serre Theorem that we encountered in Chapter 2 holds for modules over polynomial rings, not only for ideals. The theorems presented in this section are cited from [7]. We added the proofs.

Both in a finitely generated graded module and graded algebra, the homogenous elements have a vector space structure. Therefore, we can adopt the same definition of a Hilbert function for modules as for graded algebras. Namely,

$$\mathcal{H}(M, t) = \dim_k M_t.$$

A standard result in algebraic combinatorics that gives the number of monomials of degree d in a polynomial ring in n -variables is presented in the following theorem.

Theorem 4.6.1. *For $R = k[x_1, x_2, \dots, x_n]$ we have that*

$$\mathcal{H}(R, t) = \binom{n+t-1}{n-1}.$$

Proof. We will represent the monomial $x_1^{a_1} x_2^{a_2} \dots x_n^{a_n}$ as the n -tuple (a_1, a_2, \dots, a_n) . We will allocate t imaginary slots that will be filled eventually with the integer unit 1, and $n-1$ slots that will be filled with a delimiter, say $|$, that will mark the end of a sequence of 1's. We will represent the n -tuple (a_1, a_2, \dots, a_n) , as a_1 units in a row, followed by a vertical bar, followed by a_2 units in a row, followed by a vertical bar, and so on, until the last a_n units. Notice that the number of monomials of degree t in R is exactly the number of possible combinations in which one can place the $n-1$ bars in the $n+t-1$ slots. The later number is $\binom{n+t-1}{n-1}$, which concludes the proof. \square

Proposition 4.6.2. *If M is a finitely generated graded R -module and $M(d)$ is the twist defined in Proposition 4.5.1, then*

$$\mathcal{H}(M(d), t) = \mathcal{H}(M, t+d).$$

Proof. By the definition,

$$M(d) = \bigoplus_{t \in \mathbb{Z}} M(d)_t,$$

where $M(d)_t = M_{d+t}$. So,

$$\dim_k M(d)_t = \dim_k M_{d+t}$$

and therefore, it follows that

$$\mathcal{H}(M(d), t) = \mathcal{H}(M, t+d).$$

\square

Using Proposition 4.6.2 together with Theorem 4.6.1, we obtain the next corollary.

Corollary 4.6.3. *For $R = k[x_1, x_2, \dots, x_n]$, we have*

$$\mathcal{H}(R(d), t) = \binom{t + d + n - 1}{n - 1}.$$

Proposition 4.6.4. *If M and N are finitely generated graded modules, then*

$$\mathcal{H}(M \oplus N, t) = \mathcal{H}(M, t) + \mathcal{H}(N, t).$$

Proof. The grading on $M \oplus N$ is given by the gradings of M and the grading of N , namely

$$(M \oplus N)_t = M_t \oplus N_t.$$

Since M and N are finitely generated, so are M_t and N_t . Notice that M_t and N_t are vector spaces over k . Like in direct products of vector spaces, we have that the any element $(f, g) \in M_t \oplus N_t$ can be obtained as a linear combination of elements of the forms $(f_i, 0)$ and $(0, g_j)$, where $1 \leq i \leq \dim_k M_t$ and $1 \leq j \leq \dim_k N_t$. Therefore,

$$\dim_k(M \oplus N)_t = \dim_k M_t + \dim_k N_t.$$

This concludes the proof. □

Proposition 4.6.4 provides an easy way of computing the Hilbert function of modules that look like $M = N \oplus N \oplus \dots \oplus N$, where there are p copies of N . This is

$$\mathcal{H}(N \oplus N \oplus \dots \oplus N, t) = p\mathcal{H}(N, t).$$

This implies that

$$\mathcal{H}(R^p, t) = p\mathcal{H}(R, t).$$

We are now able to prove the result that will enable us to compute the Hilbert functions of different graded modules. It is an important classical result regarding graded resolutions, which we include next.

Theorem 4.6.5. *Let $R = k[x_1, x_2, \dots, x_n]$, and let M be a graded R -module. For any graded resolution of M of the form*

$$0 \rightarrow F_m \rightarrow F_{m-1} \rightarrow \dots \rightarrow F_0 \rightarrow M \rightarrow 0$$

we have

$$\mathcal{H}(M, s) = \sum_{j=0}^m (-1)^j \mathcal{H}(F_j, s).$$

Proof. Since in a graded resolution the homomorphisms are of degree 0 (meaning that polynomials of a certain degree go to polynomials of the same degree by applying the homomorphism), then we can restrict the sequence above to

$$0 \rightarrow (F_m)_s \xrightarrow{f_m} (F_{m-1})_s \xrightarrow{f_{m-1}} \cdots \rightarrow (F_0)_s \xrightarrow{f_0} M_s \rightarrow 0$$

Recall now that the modules $(F_j)_s$ are vector spaces over k . Also recall that, if U and V are vector spaces over some field k and there is a homomorphism ϕ between them, namely

$$\phi : U \rightarrow V,$$

then

$$\dim U = \dim \ker(\phi) + \dim \operatorname{im}(\phi).$$

When we write $\dim X$ we mean $\dim_k X$. Therefore, for any $1 \leq i \leq m$, we have that

$$\dim F_i = \dim \ker(f_i) + \dim \operatorname{im}(f_i).$$

Since the sequence is exact at every F_i and at M we have that $\ker(f_i) = \operatorname{im}(f_{i+1})$. Since the homomorphisms are of degree 0, then an element of a certain degree is carried to an element of the same degree. We prove that $\ker(f_i)$ is a graded modules, and by a similar argument $\operatorname{im}(f_{i+1})$ is graded as well. We need to show that there exists a grading on $\ker(f_i)$. Suppose $g = g_0 + g_1 + \cdots + g_r \in \ker(f_i)$, where the g_j 's are homogeneous of distinct degrees d_j . We need to show that $g_j \in \ker(f_i)$ for every j . We have that

$$0 = f_i(g_0 + g_1 + \cdots + g_r) = \sum_{j=0}^r f_i(g_j),$$

since f_i is a homomorphism. Now, using the fact that f_i is a degree 0 map, we have that the $f_i(g_j)$'s are homogeneous of distinct degrees d_j , where $1 \leq j \leq r$. This implies that $f_i(g_j) = 0$ for every j , which concludes that $g_j \in \ker(f_i)$. Therefore, there exists a grading on $\ker(f_i)$, namely

$$\ker(f_i) = \bigoplus_{s \in \mathbb{Z}} (\ker(f_i) \cap M_s).$$

Thus, for the sequence 4.6 we obtain the following sequence of equalities

$$\begin{aligned} \dim M &= \dim \operatorname{im}(f_0) \\ &= \dim (F_0)_s - \dim \ker(f_0) \\ &= \dim (F_0)_s - \dim (F_1)_s + \dim \ker(f_1) \\ &\vdots \\ &= \sum_{i=1}^{i=m} (-1)^i \dim (F_i)_s. \end{aligned}$$

Therefore,

$$\mathcal{H}(M, s) = \sum_{i=1}^{i=m} (-1)^i \mathcal{H}(F_i, s),$$

and so we have proven the theorem. \square

Corollary 4.6.6. *Let $R = k[x_1, x_2, \dots, x_n]$, and let M be a graded R -module. For any graded resolution of M of the form*

$$0 \rightarrow F_m \rightarrow F_{m-1} \rightarrow \cdots \rightarrow F_0 \rightarrow M \rightarrow 0$$

we have

$$\mathcal{F}(M, t) = \sum_{j=0}^m (-1)^j \mathcal{F}(F_j, t).$$

Proof. The proof follows easily by summing over all the t 's in Theorem 4.6.5. \square

Theorem 4.6.7. *Let R be as above, and let M be an R -module, such that*

$$M = R(-d_1)^{c_1} \oplus \cdots \oplus R(-d_m)^{c_m},$$

where $d_i \in \mathbb{Z}$ and $c_i \in \mathbb{N}$, for $1 \leq i \leq m$. Then the Hilbert series of M is given by

$$\mathcal{F}(M, t) = \frac{c_1 t^{d_1} + \cdots + c_m t^{d_m}}{(1-t)^n}.$$

Proof. Recall that one of our first results were that

$$\mathcal{F}(R, t) = \frac{1}{(1-t)^n}.$$

and also

$$\mathcal{F}(R, t) = \sum_{i=0}^{\infty} \binom{n+i-1}{n-1} t^i.$$

Also, we have that

$$\begin{aligned}
\mathcal{F}(R(-d), t) &= \sum_{i=0}^{\infty} \binom{n+i-d-1}{n-1} t^i \\
&= \sum_{j=-d}^{\infty} \binom{n+j-1}{n-1} t^{j+d} \\
&= \sum_{j=-d}^{-1} \binom{n+j-1}{n-1} t^{j+d} + \sum_{j=0}^{\infty} \binom{n+j-1}{n-1} t^{j+d} \\
&= \sum_{j=0}^{\infty} \binom{n+j-1}{n-1} t^{j+d} \\
&= t^d \sum_{j=0}^{\infty} \binom{n+j-1}{n-1} t^j \\
&= t^d \mathcal{F}(R, t) \\
&= t^d \frac{1}{(1-t)^{n+1}}.
\end{aligned}$$

Then by applying the theorems above we have that

$$\mathcal{F}(R(-d_1)^{c_1} \oplus \cdots \oplus R(-d_m)^{c_m}, t) = \sum_{i=0}^{i=m} \frac{c_i t^i}{(1-t)^n},$$

which concludes the proof. \square

Example 4.6.8. Let $I \subset k[x, y, z, w]$ be

$$I = \langle xz - y^2, xw - yz, yw - z^2 \rangle.$$

We will compute a graded resolution of I and using the results so far we compute the Hilbert functions.

Using Macaulay 2 we obtain

$$Syz_1 = \begin{pmatrix} w & z \\ -z & -y \\ y & x \end{pmatrix}$$

and

$$Syz_2 = 0.$$

Using Theorem 4.5.3 we have a homomorphism of the form

$$R(-2)^3 \rightarrow I,$$

since I is generated by 3 elements and each degree of the generators is 2. We will now use Syz_1 to define the homomorphism between

$$R(-d_1) \oplus R(-d_2) \rightarrow R(-2)^3.$$

Theorem 4.5.4 asserts how we can find d_1 and d_2 . Since all the polynomials of Syz_1 are of degree 1, we have that $d_1 = d_2 = 2 + 1 = 3$, where the 2 comes from the fact that all the shifts in $R(-2)^3$ are 2. Therefore, we obtain the following graded resolution for I

$$0 \rightarrow R(-3)^2 \rightarrow R(-2)^3 \rightarrow I \rightarrow 0.$$

By Theorem 4.6.5 we have that

$$\begin{aligned} \mathcal{H}(I, t) &= \mathcal{H}(R(-2)^3, t) - \mathcal{H}(R(-3)^2, t) \\ &= 3\mathcal{H}(R(-2), t) - 2\mathcal{H}(R(-3), t) \\ &= 3 \binom{t-1-2+4}{3} - 2 \binom{t-1-3+4}{3} \\ &= 3 \binom{t+1}{3} - 2 \binom{t}{3}. \end{aligned}$$

Remember that algebraists usually compute the Hilbert series of R/I instead of the Hilbert series of I . The same is true for the Hilbert function. So, once we know $\mathcal{H}(I, t)$ in the example above, we can compute $\mathcal{H}(R/I, t)$ as below

$$\mathcal{H}(R/I, t) = \binom{t+3}{3} - 3 \binom{t+1}{3} + 2 \binom{t}{3}.$$

Moreover, using the theorems above, the Hilbert series of I is

$$\begin{aligned} \mathcal{F}(I, t) &= \mathcal{F}(R(-2)^3, t) - \mathcal{F}(R(-3)^2, t) \\ &= \frac{3t^2 - 2t^3}{(1-t)^4}, \end{aligned}$$

and the Hilbert series of R/I is

$$\mathcal{F}(R/I, t) = \frac{1 - 3t^2 + 2t^3}{(1-t)^4}.$$

◇

We will end this project by proving the theorem that motivated all this work. Here is its statement.

Theorem 4.6.9 (Hilbert & Serre). *Let $R = k[x_1, \dots, x_n]$ The Hilbert series of any finitely generated graded R -module M can be written in the form*

$$\mathcal{F}(M, t) = \frac{p(t)}{(1-t)^n},$$

where p is a polynomial with coefficients in \mathbb{Z} .

Proof. By Hilbert Syzygy Theorem we know that for any graded R -module M there exists a free graded resolution of M of the form

$$0 \rightarrow F_m \rightarrow F_{m-1} \cdots \rightarrow F_0 \rightarrow M \rightarrow 0.$$

Also, we know by Corollary 4.6.6 that

$$\mathcal{F}(M, t) = \sum_{i=0}^{i=m} (-1)^i \mathcal{F}(F_i, t).$$

Since each F_i is free it means that each F_i is of the form

$$F_i = R(-d_{i1})^{\alpha_1} \oplus R(-d_{i2})^{\alpha_2} \oplus \dots \oplus R(-d_{ip_i})^{\alpha_{p_i}}.$$

Now, by using the Theorem 4.6.7 we obtain that indeed

$$\mathcal{F}(M, t) = \frac{p(t)}{(1-t)^n},$$

where the polynomial $p(t)$ has integer coefficients. □

5

Open questions

Recall that the Hilbert & Serre theorem states the fact that the Hilbert series of an ideal I , or more generally of a graded module, is always equal to a rational function of the form

$$\frac{p(t)}{(1-t)^n},$$

where n is the number of variables of the polynomial ring that contains I . One of the questions on which I was working in the beginning, was on characterizing the I 's for which the roots of $p(t)$ are integer values, or for which $p(t)$ is divisible by $t - a$. Unfortunately, I was not familiar enough with the vast theory of dimensionality of which I only got some flavor later in the year, so I had to give up pursuing this directions. Now that I know more about modules and graded resolutions, I feel there might be something in this direction that would make a good approach to the initial problem. So the above questions remain open and I think they would make a good subject for a senior project.

Another place where I reached a dead end in my research was in finding a nice formula for the $p(t)$ of an ideal in 3 variables. I have already discussed the difficulty of finding a way of representing the ideal, which led to the difficulty in computing its Hilbert series.

In Chapter 4, I was trying to find an elementary proof for showing that any module in one variable that sits inside a free module is itself free. We know that this is true by Hilbert's Syzygy theorem, but a direct proof involves the "structure theorem for the finitely generated modules over a p.i.d", which is not elementary. Now I have started to doubt that an elementary proof can be produced. The reason for this is that, given a generating matrix m for a module M , even if we find conditions for m to have only null syzygies, we cannot deduce that M is free. We need to find a minimal generating set for M , and such that it only has the trivial syzygy.

For example, take

$$m = \begin{pmatrix} x^4 & x^9 & x^3 \\ x^7 & x^2 & 1 \end{pmatrix}.$$

Then we can deduce that there exists a syzygy module for the columns of m , namely

$$Syz_1 = \begin{pmatrix} x + x^3 \\ 1 + x^2 + x^4 \\ -x^{10} - x^8 - x^6 - x^4 - x^2 \end{pmatrix}.$$

This says that the module might be not free. Using Macaulay 2, we computed the minimal generating set for the modules generated by the columns of m . This is expressed by the columns of the below matrix

$$m_1 = \begin{pmatrix} x^3 & 0 \\ 1 & x^3 - x \end{pmatrix}.$$

If we now compute the syzygies on this generating set, we obtain that there are no non-trivial syzygies, so the module generated by m is free.

So, it seems that we need a way to compute minimal generating sets, and I am not totally sure but I think this way must involve computing Groebner Bases. So, an elementary proof might not be possible.

One last theorem I have been trying to prove is the Conjecture 4.3.6. I have been verifying it with Macaulay 2 for many examples. I could not achieve any progress, so it remains open for other daring students.

References

- [1] M.F. Atiyah, I.G. MacDonal, *Introduction to Commutative Algebra*, Addison-Wesley Publishing Company, University of Oxford, 1969.
- [2] David Cox, John Little, Donal O'Shea, *Ideals, Varieties and Algorithms*, Springer, 1997.
- [3] David Dummit, Richard Foote, *Abstract Algebra*, 2nd Edition, Prentice Hall, N.J., 1999.
- [4] Takayuki Hibi, *Algebraic Combinatorics on Convex Polytopes*, Carlsaw Publication, 1992.
- [5] Heather Ann Hulett, *Maximum Betti Numbers for a given Hilbert function*, PhD Thesis, U of Illinois, 1993.
- [6] Nathan Jacobson, *Basic Algebra I*, W.H.Freeman and Company, San Francisco, 1974.
- [7] Donal O'Shea, John Little, *Using Algebraic Geometry*, Springer, 1998.
- [8] Jaren Smith, *Hilbert Sequences of Monomial Ideals - Senior Project*, Bard College, 2002.
- [9] Mike Stillman, Dave Bayer, *Computations of Hilbert functions*, J. Symbolic Computations (1992) **14**, 31-50