UNIVERSITAT DE BARCELONA

Facultat de Matemàtiques
i Informàtica

SUMSETS AND MONOMIAL PROJECTIONS OF VERONESE VARIETIES

Autor: Sixte Oriol Llenas i Segura

Director: Dra. Rosa María Miró-Roig
Realitzat a: Dep. de matemàtiques i informàtica
Barcelona, 24 de gener de 2022

Contents

Acknowledgements

Firstly, I wish to express my sincere gratitude to my tutor, Mrs. Rosa María Miró-Roig, who guided me and gave me advice this whole time. Not only has she helped me understand the concepts that appear in this paper, but she has also supported and encouraged me to continue throughout this process.

I would also like to thank my family, who have always been by my side, and my friends, Víctor, Pol, José and Roger, who have accompanied me and made these last four years an unforgettable experience.

Abstract

The main purpose of this paper is to study the so-called *sumsets problem*. This problem is naturally seen from the point of view of Additive Combinatorics, yet we approach it using Algebraic Geometry. This work is divided into three chapters.

The first chapter is devoted to Commutative Algebra. We first define basic concepts, such as *graded modules* or *exact sequences*, which will be present throughout the whole article, and then we introduce the concept of the *Hilbert function* of a graded module. The most important result of the chapter is the fact that this function, for sufficiently large integers, is a polynomial, which we prove by means of the Hilbert-Serre theorem and also Hilbert's syzygy theorem. Knowing the coefficients of this polynomial is, in general, a very difficult problem.

In the second chapter, we link the previous one with Algebraic Geometry. We define the Hilbert function of a projective variety and we calculate it in some simple cases. Next, we study three invariants of projective varieties and introduce the Veronese varieties, which are key in this work. The monomial projections of these varieties will be fundamental to solving the sumsets problem.

Finally, in the last chapter, we show that the cardinality of the sumsets can be modeled by the Hilbert function of a suitable monomial projection of a Veronese variety, which proves that this cardinality asymptotically becomes a polynomial.

Notation: throughout this whole paper, if we do not say otherwise, any ring will be a commutative and unitary ring and we are going to work over an algebraically closed field k with characteristic equal to zero. These assumptions could be more general, but this would entail some technical details that are not among our interests.

2020 Mathematics Subject Classification. 11B13, 13A02, 13C05, 13D02, 14A25

Introduction

It is a well-known fact that the study of Mathematics covers a huge number of different areas, which, very roughly, are usually related to either quantity (number theory), structure (algebra), space (geometry) or change (analysis). Each of these fields has, in turn, an immense number of subdivisions. We could ingenuously think that all these different areas develop independently and that every field has its own results, its own ways of understanding and its own applications. This could not be further from the truth. When mathematicians dig deep into any mathematical area, it is common that questions from a completely non-related subject rise. Rather than having independent non-crossing paths, we constantly find ourselves in a labyrinth, where completely different ways turn out to have a stretch in common. One of the main problems we approach in this paper faithfully highlights this fact. In the third chapter, we are going to see how the cardinality of sumsets asymptotically behaves, which, seemingly, should be studied from the point of view of Additive Combinatorics. Nonetheless, the utilization of Commutative Algebra and Algebraic Geometry happens to be undeniably helpful, which uncovers a fascinating connection between these fields.

We start by giving the definition of graded ring and graded module. Generally speaking, these concepts try to generalise a property found in polynomials, namely, the property of being able to uniquely decompose into a sum of elements, each of which is associated to a grade. In other words, a graded ring or graded module decomposes into a direct sum and each component of such sum is called a *graded component*. Since these components are usually k-vector spaces, we can now ask the natural question of *how does the dimension of these graded components grow?* This is exactly what the Hilbert function measures. For each i, this function returns the dimension of the i-th graded component of the graded module. The big challenge in the first chapter of this article is, precisely, showing that this function becomes a polynomial for sufficiently big entries, thus defining the Hilbert polynomial of a graded module.

One of the ways to prove this fact relies on the famous Hilbert's syzygy theorem. In linear algebra, as we know, a linear relation between elements of a module is a linear equation that has these elements as a solution. More precisely, if M is a module over a ring R and $m_1, \dots, m_s \in M$, a relation between $m_1, \dots, m_s \in M$ is a sequence $(r_1, \dots, r_s)$, $r_i \in R$, such that $r_1 \cdot m_1 + \cdots + r_s \cdot m_s = 0$. The set of all relations between $m_1, \dots, m_s$ forms a module. Generally, one is interested to the case where M is graded and finitely generated and m_i is a generating set of M. In

this case, each $(r_1, \dots, r_s)$ is called a *syzygy* and the module they generate is called a *syzygy module of* M. Higher order syzygy modules are defined recursively. A first syzygy module of M is simply its syzygy module and a k-th syzygy module of M is a syzygy module of a $(k-1)$-th syzygy module. Hilbert's syzygy theorem asserts that, if k is a field and $R = k[x_1, \dots, x_n]$, then every n-th syzygy module of M is free.

In the second chapter, these results are linked to Algebraic Geometry by associating to any algebraic variety its *homogeneous coordinate ring*, namely, given an algebraic set $Y \subset \mathbb{P}^n$, its homogeneous coordinate ring is the ring $k[x_0, \dots, x_n]/I(Y)$, where $I(Y)$ is the homogeneous ideal of polynomials vanishing on Y. This ring is a graded module over $k[x_0, \dots, x_n]$ and hence allows us to consider the Hilbert function and Hilbert polynomial of the variety. The amount of information this polynomial encodes is vast. If $P_X(t) = a_n t^n + \cdots + a_1 t + a_0$ is the Hilbert polynomial of the variety, its *dimension* is n, its *degree* is $a_n n!$ and its *arithmetic genus* is $(-1)^n(a_0 - 1)$.

The chapter moves on by defining the rational normal curves and, more generally, the Veronese varieties, denoted by $V_{n,d}$ and defined as the image of

$$z = [z_0, \dots, z_n] \mapsto [\dots, m_i(z), \dots],$$

where $m_i(z)$ ranges over all monomials of degree d in $z_0, \dots, z_n$. These varieties can be described by a set of quadratic equations and they are also *arithmetically Cohen-Macaulay* (briefly, *ACM*), meaning the projective dimension of their homogeneous coordinate ring equals their codimension. The monomial projections of Veronese varieties are going to be of great relevance in the third chapter. Roughly speaking, a monomial projection of a Veronese variety is the closure of the image of the same parametrization, but deleting some monomials from it. Now, it is very natural that some questions arise from this procedure: how does the Hilbert polynomial change when deleting specific monomials? Does the degree decrease? Are they still ACM varieties? The last section of the second chapter is devoted to answering such questions.

Lastly, the third chapter utilizes everything from the previous lines in order to shed some light on the cardinality of sumsets. Let $A, B \subset \mathbb{Z}^n$. We define $A + B := \{a + b : a \in A, b \in B\}$ and $tA := A + \cdots + A$ for all $t \in \mathbb{Z}_{\geq 0}$. This set is called a *sumset*. Khovanskii, under mild hypothesis, proved in [11] that $|tA|$ becomes a polynomial $p_A(t) \in \mathbb{Q}[t]$ of degree at most n when t is sufficiently large, but there is not much known about this polynomial, nor the minimum value t_0 from which $|tA| = p_A(t)$. This chapter finds a suitable monomial projection of a Veronese variety for each set A, whose Hilbert function describes, precisely, the values $|tA|$.

Chapter 1

The Hilbert polynomial

This chapter starts by giving some of the fundamental notions needed to formally define the Hilbert polynomial of a graded R-module. Among other important concepts, it recalls the definition of an R-module, which is the main algebraic structure we will work on, and defines notions such as the *length* of an R-module, a *gradation* or an *exact sequence*. Next, we come to the definition of the Hilbert function and Hilbert polynomial of a graded module M. As we are going to see, the Hilbert function $H(M, n)$ measures the length of the n-th homogeneous piece of a graded module M. We will further see that this Hilbert function is of polynomial type, hence defining the Hilbert polynomial. This statement is proved by means of Hilbert-Serre theorem and Hilbert's syzygy theorem.

1.1 Basic concepts

Definition 1.1.1. Let R be a ring. An *R-module* M consists of an abelian group $(M, +)$ and an operation $\cdot : R \times M \to M$ such that for all $r, s \in R, x, y \in M$ it holds that

1. $r \cdot (x + y) = r \cdot x + r \cdot y$,
2. $(r + s) \cdot x = r \cdot x + s \cdot x$,
3. $(rs) \cdot x = r \cdot (s \cdot x)$,
4. $1 \cdot x = x$, where 1 is the multiplicative identity of R.

Example 1.1.2.

(a) If k is a field, k-vector spaces and k-modules are identical.

(b) Every ring can be thought of as a module over itself.

(c) If R is any ring, then R^n is an R-module with the usual definitions of addition and scalar multiplication, i.e., $(x_1, \ldots, x_n) + (x'_1, \ldots, x'_n) = (x_1 + x'_1, \ldots, x_n + x'_n)$ and $r \cdot (x_1, \ldots, x_n) = (r \cdot x_1, \ldots, r \cdot x_n)$.

(d) Every abelian group $(G, +)$ can be thought of as a $\mathbb{Z}$-module: for $n > 0, x \in G$, let

$$n \cdot x := \underbrace{x + \cdots + x}_{n \text{ times}}, \quad 0 \cdot x := 0, \quad (-n) \cdot x := -(n \cdot x).$$

Conversely, any $\mathbb{Z}$-module is also an abelian group. Therefore, $\mathbb{Z}$-modules and abelian groups can be thought of as the same object.

In some sense, an R-module has to be understood as the generalization of the notion of vector space over a field, wherein the corresponding scalars are now the elements of an arbitrary given ring. Thus, there are many concepts given in linear algebra that are completely analogous when considering modules, such as submodules, generating sets, sums of modules, quotients or homomorphisms. We are going to omit the formal definition of such concepts for the sake of brevity. However, the following three results are also very significant and we consider they are worth recalling.

Proposition 1.1.3 (Isomorphism theorems)**.**

(a) For any homomorphism $\varphi : M \to N$ of R-modules there is an isomorphism

$$M/\mathrm{Ker}(\varphi) \to \mathrm{Im}(\varphi), \quad [m] \mapsto \varphi(m).$$

(b) For R-modules $N' \subseteq N \subseteq M$ we have $(M/N')/(N/N') \cong M/N$.

(c) For two submodules N, N' of an R-module M we have $(N + N')/N' \cong N/(N \cap N')$.

Nonetheless, modules do not maintain, in general, the basic properties of vector spaces. For instance, not every R-module has a basis; and even if they do (they are then called *free* modules) its cardinality need not be unique. Take for example the group of integers modulo 3 and consider it to be a $\mathbb{Z}$-module, according to Example 1.1.2 (d). In this case, one cannot find even one element which satisfies the definition of a linearly independent set, since when an integer such as 3 or 6 multiplies an element of the group, the result is 0. This fact forces us to redefine the notion of *dimension*, hence introducing the *length* of a module.

Definition 1.1.4. Let M be a module over a ring R. Given a strict chain of submodules of M of the form

$$M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M,$$

we say that n is the *length of the chain*. The *length of* M, $l(M)$, is then defined to be the largest length of any of its chains. If it does not exist, we say that M has infinite length. A (finite) chain that has length $l(M)$ is called a *composition series for* M.

Example 1.1.5.

(a) If k is a field, the length of a k-module and its dimension as a k-vector space coincide.

(b) Let M be the module $\mathbb{R}[x]/(x^3 - x^2 + x - 1)$ over the ring $\mathbb{R}[x]$. We want to compute $l(M)$. The submodules of M correspond to the ideals of $\mathbb{R}[x]$ containing $(x^3 - x^2 + x - 1)$. Since $(x^3 - x^2 + x - 1) = (x - 1)(x^2 + 1)$, we obtain the maximal chain of ideals

$$(x^3 - x^2 + x - 1) \subset (x - 1) \subset \mathbb{R}[x]$$

or

$$(x^3 - x^2 + x - 1) \subset (x^2 + 1) \subset \mathbb{R}[x],$$

which corresponds to the chain of submodules

$$0 \subset \mathbb{R}[x]/(x - 1) \subset \mathbb{R}[x]/(x^3 - x^2 + x - 1)$$

or

$$0 \subset \mathbb{R}[x]/(x^2 + 1) \subset \mathbb{R}[x]/(x^3 - x^2 + x - 1).$$

This proves that $l(M) = 2$.

(c) The length of the cyclic group $\mathbb{Z}/n\mathbb{Z}$ (viewed as a $\mathbb{Z}$-module) is equal to the number of prime factors of n, with multiple prime factors counted multiple times. This can be proved by using the Chinese remainder theorem.

From now on, some of the results that are going to be used in proofs might be given for granted, yet can be found in any conventional algebra book or any notes on commutative algebra, such as [2, 6]. In the following proposition, for instance, we are using the fact that any chain $0 \subsetneq M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M$ of submodules of M can be refined to a composition series of M, as long as M has finite length. Also, if N is a non-trivial submodule of an R-module M, there is no submodule P of M with $N \subsetneq P \subsetneq M$ if and only if the module M/N has only trivial submodules.

Proposition 1.1.6. *Let M be an R-module such that $l(M) < \infty$ and N a submodule of M. We have*

$$l(N) + l(M/N) = l(M).$$

Proof. The chain $0 \subseteq N \subseteq M$ can be refined to a composition series for M

$$0 = N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_n = N \subsetneq M_0 \subsetneq \cdots \subsetneq M_m = M, \tag{1.1}$$

with $l(N) = n$ and $l(M) = n + m$. Setting $P_i := M_i/N$ for $i = 1, \ldots, m$ we obtain a chain of submodules

$$0 = P_0 \subsetneq \cdots \subsetneq P_m = M/N \tag{1.2}$$

in which $P_i/P_{i-1} \cong M_i/M_{i-1}$ (this follows from Proposition 1.1.3 (b)). These modules have no non-trivial submodules; otherwise, there would exist a submodule P of M such that $M_{i-1} \subsetneq P \subsetneq M_i$, yet this contradicts the maximality of (1). Therefore, (2) is a composition series for M/N of length m, so we get the desired result $l(N) + l(M/N) = n + m = l(M)$. □

Corollary 1.1.7. *Let M, N be R-modules. If $\varphi : M \to N$ is a homomorphism, $l(\operatorname{Ker}\varphi) + l(\operatorname{Im}\varphi) = l(M)$.*

Proof. This is just Proposition 1.1.6 applied to $M/\operatorname{Ker}(\varphi) \cong \operatorname{Im}(\varphi)$ from Proposition 1.1.3. □

Proposition 1.1.8. *Let M_1, M_2 be modules of finite length. We have*

$$l(M_1 \oplus M_2) = l(M_1) + l(M_2).$$

Proof. Consider the composition series $0 = X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_p = M_1$ and $0 = Y_0 \subsetneq Y_1 \subsetneq \cdots \subsetneq Y_q = M_2$. Then

$$0 = X_0 \oplus 0 \subsetneq X_1 \oplus 0 \subsetneq \cdots \subsetneq X_p \oplus 0 \subsetneq X_p \oplus Y_1 \subsetneq \cdots \subsetneq X_p \oplus Y_q = M_1 \oplus M_2$$

is a composition series for $M_1 \oplus M_2$ of length $p + q = l(M_1) + l(M_2)$. □

1.2 Graded rings and modules

Definition 1.2.1. Let R be a ring. We say R is a *graded* ring if the underlying additive group of R has a decomposition $R = \bigoplus_{i \in I} R_i$, known as *gradation*, where R_i is an abelian group for all i and $R_i R_j \subset R_{i+j}$ for all i, j. Usually, the index set I is the set of nonnegative integers or the set of integers.

A nonzero element $x \in R_i$ is said to be homogeneous of degree i and its degree is denoted by $\deg x$. By definition of direct sum, every nonzero element a of R can be uniquely written as a finite sum $a = \sum_i a_i$, where each a_i is homogeneous of degree i.

Example 1.2.2.

(a) Any ring R can receive a gradation by letting $R_0 = R$ and $R_i = 0$ for all $i \neq 0$. This is known as the trivial gradation of R.

(b) Given k a field, the polynomial ring $R = k[x_0, \ldots, x_n]$ is a graded ring, where each component R_i is the set of all homogeneous polynomials of degree i.

Proposition 1.2.3. *If $R = \bigoplus_i R_i$ is a graded ring, then R_0 is a subring of R, $1 \in R_0$ and R_n is an R_0-submodule for all n.*

Proof. We observe that $R_0 \cdot R_0 \subset R_0$, which means that R_0 is closed under multiplication. That forces R_0 to be a subring of R. Now, if we had $1 \notin R_0$, the equality $1 \cdot r = r$ would force r to have different degrees, which is nonsense. The last statement follows from the fact that $R_0 \cdot R_n \subset R_n$ for all n.

□

In a very similar way, it is possible to define a *graded R-module*, as long as R is a graded ring. In fact, whenever we speak of a graded module, the module is always assumed to be over a graded ring.

Definition 1.2.4. Let R be a graded ring and M and R-module. We say M is a *graded* R-module if the underlying additive group of M has a decomposition $M = \bigoplus_{i\in I} M_i$, known as *gradation*, where $R_i \cdot M_j \subset M_{i+j}$ for all i, j.

Again, a nonzero element $x \in M_i$ is said to be homogeneous of degree i and its degree is denoted by $\deg x$. One calls M_i the i-th homogeneous (or graded) component of M. By definition of a direct sum, every nonzero element a of R can be uniquely written as a finite sum $a = \sum_i a_i$, where each a_i is homogeneous of degree i.

Remark 1.2.5. If M is a graded R-module, M_n is an R_0-module for all n.

Example 1.2.6. Let R be any ring and let S be the graded ring $R[x]$. Consider the S-module $M := S[y]$. One way to grade $S[y]$ over S is the following one:

$$S[y] = \bigoplus_{k=0}^{\infty} M_k,$$

where $M_k := R[y]x^k$. It is easy to check that $S_p \cdot M_q = (Rx^p) \cdot (R[y]x^q) \subset R[y]x^{p+q} = M_{p+q}$. Another way to grade $S[y]$ over S is by saying

$$S[y] = \bigoplus_{k=0}^{\infty} M'_k$$

with $M'_k := \sum_{i+j=k} Rx^i y^j$, since

$$S_p \cdot M'_q = (Rx^p) \cdot \sum_{i+j=q} Rx^i y^j = \sum_{i+j=q} Rx^{i+p} y^j \subset \sum_{i+j=p+q} Rx^i y^j = M'_{p+q}.$$

Definition 1.2.7. Let M, N be graded R-modules.

(a) If $\varphi : M \to N$ is a homomorphism, we say φ is *homogeneous of degree r* if $\varphi(M_n) \subset N_{n+r}$ for all n. The set of homomorphisms of degree r is denoted by $Hom_R(M, N)_r$. Obviously, these sets induce the gradation

$$Hom_R(M, N) = \bigoplus_r Hom_R(M, N)_r.$$

(b) We say M, N are isomorphic if there is an isomorphism of degree 0 from M to N.

(c) A submodule N of M is a *graded submodule of M* if N is a graded R-module and $N \hookrightarrow M$ is homogeneous of degree 0.

(d) A quotient Q of M is a *graded quotient of M* if Q is a graded R-module and the natural projection $M \to Q$ is homogeneous of degree 0.

Definition 1.2.8. Let R be a graded ring an $I \subset R$ and ideal. I is said to be *homogeneous* if it can be generated by homogeneous elements.

Definition 1.2.9. For any graded R-module M and any $l \in \mathbb{Z}$, we define the twisted module $M(l)$ by $M(l)_d = M_{d+l}$.

Definition 1.2.10. Let R be a graded ring. If M is a graded R-module, the *annihilator* of M is defined as $\operatorname{Ann} M = \{r \in R : r \cdot m = 0 \text{ for all } m \in M\}$.

Proposition 1.2.11. *If M is a graded R-module,* $\operatorname{Ann} M$ *is a homogeneous ideal in R.*

Proof. First note $\operatorname{Ann} M \neq \emptyset$, since $0 \in \operatorname{Ann} M$. Now, we take r_1, r_2 such that $r_i \cdot m = 0$ for all $m \in M$ and $(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m = 0 + 0 = 0$. Finally, we take $r \in R$ and $s \in R$ such that $s \cdot m = 0$ for all $m \in M$. We want to see that $(rs) \cdot m = 0$ for all $m \in M$, but $(rs) \cdot m = r \cdot (s \cdot m) = r \cdot 0 = 0$. To see this ideal is homogeneous, we claim that

$$\operatorname{Ann} M = (r \in R : r \cdot m = 0 \text{ for all } m \in M, r \text{ homogeneous}).$$

The inclusion from right to left is clear. From left to right, we take $r \in R$ such that $r \cdot m = 0$ for all $m \in M$ and write $r = \sum_i r_i$, being r_i either 0 or homogeneous of degree i. We will have finished if we see $r_i \cdot m = 0$ for all i and $m \in M$. Now, for any $m \in M$ homogeneous of degree j,

$$0 = r \cdot m = \sum_i r_i \cdot m.$$

Each summand $r_i \cdot m$ is either zero or has degree $i + j$. By comparing degrees, $r_i \cdot m = 0$ for all i. This proves that $r_i \cdot m$ equals zero if m is homogeneous, but any $m \in M$ can be expressed as a sum of homogeneous components and the same idea works.

□

1.3 Exact sequences

Definition 1.3.1. An *exact sequence* of modules is a sequence of homomorphisms between modules

$$\cdots \xrightarrow{f_{-1}} M_{-1} \xrightarrow{f_0} M_0 \xrightarrow{f_1} M_1 \xrightarrow{f_2} \cdots$$

such that $\operatorname{Im}(f_i) = \operatorname{Ker}(f_{i+1})$. It is called a short exact sequence if it has the form

$$0 \to M_0 \xrightarrow{f} M_1 \xrightarrow{g} M_2 \to 0.$$

An immediate consequence of the definition of *exact sequence* is the following fact. If the exact sequence has the form

$$0 \to M_0 \xrightarrow{f_1} M_1 \xrightarrow{f_2} \cdots \xrightarrow{f_n} M_n \to 0,$$

then f_1 is a monomorphism and f_n is an epimorphism.

Proposition 1.3.2. *Let*

$$0 \to M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} \cdots \xrightarrow{\varphi_{n-1}} M_n \to 0$$

be an exact sequence of R-modules of finite length. Then $\sum_{i=1}^{n}(-1)^i l(M_i) = 0$.

Proof. By Corollary 1.1.7 we can express this sum as

$$\sum_{i=1}^{n-1}(-1)^i l(M_i) = \sum_{i=1}^{n-1}(-1)^i (l(\operatorname{Ker}\varphi_i) + l(\operatorname{Im}\ \varphi_i)),$$

which, with an index shift, can be expressed as

$$-\underbrace{l(\operatorname{Ker}\varphi_1)}_{0} + (-1)^{n-1}\underbrace{l(\operatorname{Im}\ \varphi_{n-1})}_{l(M_n)} + \sum_{i=2}^{n-1}(-1)^i (l(\operatorname{Ker}\varphi_i) - l(\operatorname{Im}\ \varphi_{i-1})).$$

However, $\operatorname{Ker}\varphi_i = \operatorname{Im}\varphi_{i-1}$, so this last sum vanishes and the result follows.

□

Proposition 1.3.3. *Let* M_i, $i \in \mathbb{Z}$, *be graded R-modules and let*

$$\cdots \xrightarrow{f_{-1}} M_{-1} \xrightarrow{f_0} M_0 \xrightarrow{f_1} M_1 \xrightarrow{f_2} \cdots$$

be an exact sequence of homomorphisms of degree 0. *Consider for all* i, n *the restriction* $f_{in} := f_i|_{(M_{i-1})_n}$. *Then, for all* n, *the sequence of* R_0*-modules*

$$\cdots \xrightarrow{f_{-1n}} (M_{-1})_n \xrightarrow{f_{0n}} (M_0)_n \xrightarrow{f_{1n}} (M_1)_n \xrightarrow{f_{2n}} \cdots$$

is an exact sequence.

Proof. The homomorphisms f_i are homogeneous of degree 0, so the sequence is well defined, since $\operatorname{Im}(f_{in}) = f_i(M_{i-1})_n \subset (M_i)_n$ for all i. Now, we need $\operatorname{Im}(f_{in}) = \operatorname{Ker}(f_{i+1n})$, but this is easy to check using $\operatorname{Im}(f_i) = \operatorname{Ker}(f_{i+1})$.

□

1.4 The Hilbert function and polynomial

The *Hilbert function* $H(M, *) : \mathbb{Z} \mapsto \mathbb{Z}$ is defined by $H(M, t) := l(M_t)$. Our next step is to see that this function is of polynomial type, meaning that there is $p_M(t) \in \mathbb{Q}[t]$ such that $H(M, t) = p_M(t)$ for $t \gg 0$.

Definition 1.4.1. A *numerical polynomial* is a polynomial $p(t) \in \mathbb{Q}[t]$ such that $p(t) \in \mathbb{Z}$ for all $t \gg 0$, $t \in \mathbb{Z}$.

Lemma 1.4.2. *If* $p(t) \in \mathbb{Q}[t]$ *is a numerical polynomial of degree* r, *then there are* $c_0, \ldots, c_r \in \mathbb{Z}$ *such that*

$$p(t) = c_0\binom{t}{r} + c_1\binom{t}{r-1} + \cdots + c_r.$$

In particular, $p(n) \in \mathbb{Z}$ *for all* $n \in \mathbb{Z}$. *In other words, if a rational polynomial gives integers from some value* $t \in \mathbb{Z}$, *then it gives integers for all integer values.*

Proof. We are going to use induction on the degree of p. If $\deg p = 0$, the result is obvious, because $p(n) = c_0 \in \mathbb{Z}$ cst. for all $n \gg 0$ means $p \equiv c_0$. Now, we suppose that any numerical polynomial $q(t) \in \mathbb{Q}[t]$ of degree $r-1$ can be written as

$$q(t) = c_0 \binom{t}{r-1} + c_1 \binom{t}{r-2} + \cdots + c_{r-1},$$

with $c_0, \ldots, c_{r-1} \in \mathbb{Z}$. Choose a numerical polynomial p of degree r. We have the following equalities:

$$\binom{t}{r} = \frac{t!}{r!\,(t-r)!} = \frac{1}{r!} t(t-1)\cdots(t-r+1) = \frac{t^r}{r!} + \ldots.$$

We claim that, for any r, the set $\{\binom{t}{i} : 0 \leq i \leq r\}$ is a $\mathbb{Q}$-basis of $\mathbb{Q}[t]_{\leq r}$. If we identify $\mathbb{Q}[t]_{\leq r}$ with $\mathbb{Q}^{r+1}$, this set becomes

$$\{(*, \ldots, 1/r!), (*, \ldots, 1/(r-1)!, 0), \ldots, (1, 0, \ldots, 0)\},$$

where $*$ means any value. This is clearly a $\mathbb{Q}$-basis. Therefore, p can be written as

$$p(t) = c_0 \binom{t}{r} + c_1 \binom{t}{r-1} + \cdots + c_r,$$

with $c_0, \ldots, c_r \in \mathbb{Q}$. For any polynomial q we shall now define the *difference polynomial* Δq by $\Delta q(t) := q(t+1) - q(t)$. Note that the degree of this expression decreases by one and also

$$\Delta \binom{t}{r} = \binom{t+1}{r} - \binom{t}{r} = \binom{t}{r-1}.$$

From this last expression we get

$$\Delta p(t) = p(t+1) - p(t) = c_0 \binom{t}{r-1} + c_1 \binom{t}{r-2} + \cdots + c_{r-1},$$

which is a polynomial of degree $r-1$ and, since $\Delta p(t) = p(t+1) - p(t) \in \mathbb{Z}$ for $t \gg 0$, it is also a numerical polynomial. Hence, by induction there is an expression such that

$$c_0 \binom{t}{r-1} + c_1 \binom{t}{r-2} + \cdots + c_{r-1} = a_0 \binom{t}{r-1} + a_1 \binom{t}{r-2} + \cdots + a_{r-1},$$

with $a_0, \ldots, a_{r-1} \in \mathbb{Z}$. But $\{\binom{t}{i} : 0 \leq i \leq r-1\}$ is a $\mathbb{Q}$-basis, so $a_i = c_i$ for all $0 \leq i \leq r-1$, which means that $c_i \in \mathbb{Z}$ for all $0 \leq i \leq r-1$. We are almost done. We still have to check that $c_r \in \mathbb{Z}$, but this follows from the fact that $p(t) \in \mathbb{Z}$ for $t \gg 0$.

□

Lemma 1.4.3. *Let $f : \mathbb{Z} \to \mathbb{Z}$ be a function. If there is a numerical polynomial $q(t)$ such that the difference function Δf is equal to $q(n)$ for all $n \gg 0$, then there is a numerical polynomial $p(t)$ such that $f(n) = p(n)$ for all $n \gg 0$.*

Proof. Suppose $q(t)$ has degree r. Using lemma 1.4.2, we can write

$$q(t) = c_0 \binom{t}{r} + \cdots + c_r$$

with $c_0, \ldots, c_r \in \mathbb{Z}$. We define $\widetilde{p}(t)$ as follows:

$$\widetilde{p}(t) = c_0 \binom{t}{r+1} + \cdots + c_r \binom{t}{1}.$$

We have $\Delta\widetilde{p} = q$, so $\Delta(f - \widetilde{p})(n) = \Delta f(n) - \Delta\widetilde{p}(n) = \Delta f(n) - q(n) = 0$ for $n \gg 0$, and this means that $(f - \widetilde{p})(n) = k$ cst. for all $n \gg 0$, so

$$f(n) = \widetilde{p}(n) + k$$

for all $n \gg 0$. Defining $p := \widetilde{p} + k$, we found a polynomial equal to f for large values of n, and p is a numerical polynomial, because $\mathrm{Im}(f) \subset \mathbb{Z}$. This is exactly what we needed and the proof is complete.

□

The next result is the analogue for graded modules of a well-known result for modules of finite type over a noetherian ring.

Proposition 1.4.4. *Let M be a graded module of finite type over a noetherian graded ring S. Then there exists an increasing sequence of submodules (that is, a graded filtration) $0 = M^0 \subset M^1 \subset \ldots \subset M^r = M$ such that for each i we have $M^i/M^{i-1} \cong (S/\mathfrak{p}_i)(l_i)$, where $\mathfrak{p}_i$ is a homogeneous prime ideal of S and $l_i \in \mathbb{Z}$.*

Proof. To prove the existence of this filtration, we consider the set $\mathfrak{A}$ of graded submodules of M that admit such a filtration. This set is nonempty, because $0 \in \mathfrak{A}$. Take any ordered chain of submodules $N^1 \subset N^2 \subset \ldots$, $N^i \in \mathfrak{A}$ for all i. M is a noetherian module, so this chain has to end and this implies that there exists $M' \in \mathfrak{A}$ maximal in $\mathfrak{A}$. Consider $M'' := M/M'$. If $M'' = 0$, then $M' = M$ and the statement is true. If not, we consider the set of ideals $\mathfrak{I} := \{I_m = \mathrm{Ann}(m) : m \in M'', m \text{ homogeneous}, m \neq 0\}$, where $\mathrm{Ann}(m) := \{s \in S : s \cdot m = 0\}$. If there was m such that $I_m = S$, m would satisfy $s \cdot m = 0$ for all $s \in S$, yet this forces m to be 0, hence $I_m \neq 0$ for all m. Besides, I_m is a homogeneous ideal. Now, since S is a noetherian ring, there is I_m maximal in $\mathfrak{I}$. We will now see that this ideal is a prime ideal.

To see so, let $a, b \in S$ such that $ab \in I_m$, but $b \notin I_m$. We want to see $a \in I_m$. In fact, it is sufficient to prove this when a, b are homogeneous, because S is graded and a, b can split into homogeneous components. Now consider the element $b \cdot m \in M''$. If $b \cdot m$ was 0, then $b \in I_m$ by definition, so $b \cdot m \neq 0$. We also have $I_m \subset I_{b\cdot m}$, since $s \cdot m = 0$ implies $s \cdot (b \cdot m) = 0$. By maximality of I_m, $I_m = I_{b\cdot m}$. However, $ab \in I_m$, so $(ab) \cdot m = a \cdot (b \cdot m) = 0$, and this means $a \in I_{b\cdot m} = I_m$, as wanted. Thus I_m is a homogeneous prime ideal of S. Call it $\mathfrak{p}$.

Let m have degree l and let $N \subset M''$ be the module generated by m, that is, $S \cdot m$. Using Proposition 1.1.3 (a), the map

$$S/\mathfrak{p} \to S \cdot m = N, \quad [s] \mapsto s \cdot m$$

is an isomorphism of modules. If we want it to be an isomorphism of *graded* modules (that is, a homogeneous isomorphism of degree 0) we rather consider the twisted module $(S/\mathfrak{p})(-l)$. Thus, $N \cong (S/\mathfrak{p})(-l)$. Let $N' := \pi^{-1}(N) \subset M$, where $\pi : M \to M/M' = M''$ is the natural projection. Since $0 \in N$, $M' \subset \pi^{-1}(N) = N'$ and $N'/M' \cong N \cong (S/\mathfrak{p})(-l)$. So $N' \in \mathfrak{A}$ and also $M' \subsetneq N'$, which contradicts the maximality of M'. We conclude $M' = M$, which proves the existence of the filtration. □

Theorem 1.4.5 (Hilbert - Serre)**.** *Let M be a graded module of finite type over the polynomial ring $k[x_0, \dots, x_n]$, k a field. Then there exists a unique polynomial $p_M(t) \in \mathbb{Q}[t]$ such that $H(M,t) = p_M(t)$ for $t \gg 0$. Furthermore,* $\deg p_M = \dim \mathbb{V}(\operatorname{Ann} M)$*, where V denotes the zero set in $\mathbb{P}^n$ of a set of polynomials.*

Proof. Consider the short exact sequence $0 \to M' \to M \to M'' \to 0$. By Propositions 1.3.2 and 1.3.3, it holds that $H(M,t) = H(M',t) + H(M'',t)$ for all t, and also $\mathbb{V}(\operatorname{Ann} M) = \mathbb{V}(\operatorname{Ann} M') \cup \mathbb{V}(\operatorname{Ann} M'')$. This means that proving the statement for M', M'' is also proving it for M. Due to Proposition 1.4.4, there is a filtration of M with quotients of the form $(S/\mathfrak{p})(l)$, where $\mathfrak{p}$ is a homogeneous prime ideal and $l \in \mathbb{Z}$. This allows us to reduce to $M \cong (S/\mathfrak{p})(l)$, where the shift l is in fact a change of variables $z \mapsto z + l$. It is sufficient to consider the case $M = S/\mathfrak{p}$. Now, if $\mathfrak{p} = (x_0, \dots, x_n)$, $H(M,t) = 0$ for all $t > 0$, so $p_M = 0$ is the corresponding polynomial. Besides, $\deg p_M = \dim \mathbb{V}(\mathfrak{p})$, considering $\deg 0$ and $\dim \emptyset$ to be both -1.

We now study the case where $\mathfrak{p} \neq (x_0, \dots, x_n)$. We choose $x_i \notin \mathfrak{p}$ and we define $M'' := M/x_i \cdot M$. Consider the sequence $0 \to M(-1) \xrightarrow{x_i} M \to M'' \to 0$, which is an exact sequence. Then, $H(M'',t) = H(M,t) - H(M,t-1)$. On the other hand, $\mathbb{V}(\operatorname{Ann} M'') = \mathbb{V}(\mathfrak{p}) \cap \{x_i = 0\}$ and, by choice of x_i, $\mathbb{V}(\mathfrak{p}) \nsubseteq H$, where H is the hyperplane $x_i = 0$. Now, Projective Dimension Theorem tells us that $\dim \mathbb{V}(\operatorname{Ann} M'') = \dim \mathbb{V}(\mathfrak{p}) - 1$. Now we are going to use induction on $\dim \mathbb{V}(\operatorname{Ann} M)$. We may assume that $H(M'',t)$ is a polynomial function, which corresponds to a polynomial $p_{M''}$ of degree $= \dim \mathbb{V}(\operatorname{Ann} M'')$. From lemmas 1.4.2, 1.4.3, the statement follows.

□

We have seen that the Hilbert function is indeed a polynomial from a specific integer value t_0. Finding this t_0, as well as knowing other properties of this polynomial, such as its degree and leading coefficient, is in our interest. The next lines give an alternative way to reach such polynomial. We will give several previous results and then we prove the well-known *Hilbert's syzygy theorem*, which will also allow us to prove that the Hilbert function is of polynomial type.

Proposition 1.4.6. *A graded R-module admits a homogeneous generating set.*

Proof. This follows from the fact that any R-module has generators - the module itself is an example. Since the module is graded, take the union of the homogeneous components of each generator. This set still generates the module. □

Remark 1.4.7. If the module is finite, this procedure can be done with a finite generating set, thus obtaining a finite homogeneous generating set.

Proposition 1.4.8. *Let M be a graded R-module of finite type. There are always integers $r_1, \dots, r_n$ and an exhaustive homomorphism of degree 0 that has the form*

$$\bigoplus_i R(-r_i) \to M.$$

Proof. Consider $(x_1, \dots, x_s)$ a homogeneous generating set of M and $r_i := \deg x_i$. For each i we define the map $\varphi_i : R(-r_i) \to M$, $1 \mapsto x_i$. Here, $R(-r_i)$ has to be understood as an R-module, so $\varphi_i(r) = \varphi_i(r \cdot 1) = r \cdot \varphi(1) = r \cdot x_i$. These maps are clearly homomorphisms. Now, φ has degree 0, that is, $\varphi_i(R_{n-r_i}) \subset M_n$, beacuse if $\deg r = n - r_i$ then $\varphi_i(r) = r \cdot x_i$ has degree n. Let's now consider the sum of these homomorphisms. It is an exhaustive map, since any $m \in M$ can be written as $\sum_i a_i x_i$ and this is indeed the image of $(a_i)_i$, and it is also a homogeneous homomorphism of degree 0. This is exactly what we needed.

□

Corollary 1.4.9. *Let M be a free graded R-module of finite type. There are $r_1, \dots, r_n \in \mathbb{Z}$ such that $M \cong \bigoplus_i R(-r_i)$.*

Proof. It follows directly from Proposition 1.4.8 and the definition of basis. □

Lemma 1.4.10 (Nakayama's lemma)**.** *Let M be a graded R-module of finite type. If $M = R_+M$, where $R_+ := \bigoplus_{i>0} R_i$, then $M = 0$.*

Proof. Let $(x_1, \dots, x_l)$ be a homogeneous generating set of M. We can choose x_1 such that $\deg x_1 \leq \deg x_i$ for all i. It is clear that $x_1 \notin R_+M$, which contradicts the fact that $x_1 \in M$. □

1.5 Hilbert's syzygy theorem

The following lines are going to be devoted to the concept of *syzygy*, which will eventually lead us to the famous *Hilbert's syzygy theorem*. This theorem is one of the three fundamental theorems about polynomial rings over fields, first proved by David Hilbert in 1890, and it gives an alternative way to prove that the Hilbert function is of polynomial type.

We shall first try to understand what a syzygy is. In linear algebra, as we know, a linear relation between elements of a module is a linear equation that has these elements as a solution. More precisely, if M is a module over a ring R and $m_1, \dots, m_s \in M$, a relation between $m_1, \dots, m_s \in M$ is a sequence $(r_1, \dots, r_s)$, $r_i \in R$, such that $r_1 \cdot m_1 + \cdots + r_s \cdot m_s = 0$. The set of all relations between $m_1, \dots, m_s$ forms a module. Generally, one is interested to the case where M is graded and finitely generated and m_i is a generating set of M. In this case, each $(r_1, \dots, r_s)$ is called a *syzygy* and the module they generate is called a *syzygy module of M*.

Although the syzygy module depends on the chosen generating set, most of its properties are independent.

Higher order syzygy modules are defined recursively. A first syzygy module of M is simply its syzygy module and a k-th syzygy module of M is a syzygy module of a $(k-1)$-th syzygy module. Hilbert's syzygy theorem asserts that, if k is a field and $R = k[x_1, \dots, x_n]$, then every n-th syzygy module of M is free.

Example 1.5.1. Let $R = \mathbb{C}[x, y]$ and $M = R/\mathfrak{m}$, where $\mathfrak{m} = (x, y)$. A first syzygy module is $\mathfrak{m}$, but it is not free. The elements x, y are not independent, since they satisfy the non-trivial relation $(-y) \cdot x + x \cdot y = 0$. Therefore, we look at the syzygies of $\mathfrak{m}$ and we get a rank-one free module generated by the element $(-y, x) \in R^2$, as expected.

This procedure can be summarised with an exact sequence. Let M be a graded module of finite type over $R = k[x_0, \dots, x_d]$ and $e_{01}, \dots, e_{0m_0}$ a generating set of M with $n_{0j} := \deg e_{0j}$. We have just seen that the map

$$\varphi_0 : \bigoplus_{j=1}^{m_0} R(-n_{0j}) \to M, \quad (a_j)_j \mapsto \sum_j a_j \cdot e_{0j}$$

is a homogeneous epimorphism of degree 0. Now, the syzygy module is simply $\operatorname{Ker}(\varphi_0)$. Analogously, consider $e_{11}, \dots, e_{1m_1}$ a generating set of $\operatorname{Ker}(\varphi_0)$ with $n_{1j} := \deg e_{1j}$ and

$$\varphi_1 : \bigoplus_{j=1}^{m_1} R(-n_{1j}) \to \operatorname{Ker}(\varphi_0), \quad (a_j)_j \mapsto \sum_j a_j \cdot e_{1j}.$$

The second syzygy is $\operatorname{Ker}(\varphi_1)$. Recursively, the k-th syzygy is $\operatorname{Ker}(\varphi_{k-1})$. These maps are exhaustive, so $\operatorname{Im}(\varphi_i) = \operatorname{Ker}(\varphi_{i-1})$, which leads us to the exact sequence

$$\cdots \xrightarrow{\varphi_2} \bigoplus_{j=1}^{m_1} R(-n_{1j}) \xrightarrow{\varphi_1} \bigoplus_{j=1}^{m_0} R(-n_{0j}) \xrightarrow{\varphi_0} M \to 0.$$

Now, Hilbert's syzygy theorem is equivalent to verifying that the following sequence is exact:

$$0 \to \bigoplus_{j=1}^{m_{d+1}} R(-n_{d+1j}) \xrightarrow{\varphi_{d+1}} \cdots \xrightarrow{\varphi_2} \bigoplus_{j=1}^{m_1} R(-n_{1j}) \xrightarrow{\varphi_1} \bigoplus_{j=1}^{m_0} R(-n_{0j}) \xrightarrow{\varphi_0} M \to 0,$$

since the 0 at the left end means that φ_{d+1} maps $\bigoplus_{j=1}^{m_{d+1}} R(-n_{d+1j})$ isomorphically onto $\operatorname{Ker}(\varphi_d)$, that is, the $(d+1)$-th syzygy of M is free.

Theorem 1.5.2 (Hilbert's syzygy theorem)**.** *Let $V := k[x_0 \dots, x_d]$ be a ring of polynomials over a field k and M a graded V-module of finite type. If $m_i, n_{ij} \in \mathbb{Z}$ with $0 \le i \le d$ and $1 \le j \le m_i$ and*

$$0 \to K \to \bigoplus_{j=1}^{m_d} V(-n_{dj}) \to \cdots \to \bigoplus_{j=1}^{m_1} V(-n_{1j}) \to \bigoplus_{j=1}^{m_0} V(-n_{0j}) \to M \to 0$$

is an exact sequence of homomorphisms of degree 0, then there exist two values $m_{d+1}, n_{d+1j} \in \mathbb{Z}$ with $1 \le j \le m_{d+1}$ such that $K \cong \bigoplus_{1 \le j \le m_{d+1}} V(-n_{d+1\,j})$.

Proof. We are going to prove this statement using induction on the number $d+1$ of variables. If $d+1=0$, then $V=k$ and M is a finite k-vector space. Let $(e_1,\dots,e_m)$ be a homogeneous basis of M and $n_i=\deg e_i$. The homomorphism $f_i: V(-n_i)\to M$, defined by $f_i(1)=e_i$, is homogeneous of degree 0. Now, the following map is an isomorphism of graded V-modules:

$$\sum_{1\le j\le m} f_j : \bigoplus_{1\le i\le m} V(-n_i)\to M.$$

Suppose $d+1>0$. We define $N=\operatorname{Ker}(\bigoplus_{1\le j\le m_0} V(-n_{0j})\to M)$. The multiplication by x_d is injective in V, so it is also injective in N and K, because $N\subset\bigoplus_{1\le j\le m_0} V(-n_{0j})$ and $K\subset\bigoplus_{1\le j\le m_d} V(-n_{dj})$. Let's now consider the following commutative diagram, where rows and columns are both exact sequences of homomorphisms of degree 0:

$$\begin{array}{ccccccccccc}
 & & 0 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & K(-1) & \to & \bigoplus_{j=1}^{m_d} V(-n_{dj}-1) & \to\cdots\to & \bigoplus_{j=1}^{m_1} V(-n_{1j}-1) & \to & N(-1) & \to & 0\\
 & & \downarrow{\scriptstyle x_d} & & \downarrow{\scriptstyle x_d} & & \downarrow{\scriptstyle x_d} & & \downarrow{\scriptstyle x_d} & & \\
0 & \to & K & \to & \bigoplus_{j=1}^{m_d} V(-n_{dj}) & \to\cdots\to & \bigoplus_{j=1}^{m_1} V(-n_{1j}) & \to & N & \to & 0\\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & K/x_dK & \to & \bigoplus_{j=1}^{m_d} V'(-n_{dj}) & \to\cdots\to & \bigoplus_{j=1}^{m_1} V'(-n_{1j}) & \to & N/x_dN & \to & 0\\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & & 0 & &
\end{array}$$

where $V'=V/x_dV\cong k[x_0,\dots,x_{d-1}]$. A direct application of the snake lemma (see [6] for more details) shows that the last row is an exact sequence of graded V'-modules of homomorphisms of degree 0. By induction, there exist integer values m, l_i, $1\le i\le m$, such that $K/x_dK\cong\bigoplus_{1\le i\le m} V'(-l_i)$, and from this we are going to deduce an isomorphism $K\cong\bigoplus_{1\le i\le m} V(-l_i)$.

Consider $z_1,\dots,z_m$ homogeneous elements of K with $\deg z_i=l_i$, where the classes in K/x_dK form a basis of K/x_dK. If K' is the graded submodule of K formed by $z_1,\dots,z_m$, we get $K=K'+x_dK$. Using Lemma 1.4.10, we obtain $K=K'$.

Finally, we suppose that there is a relation between $z_1,\dots,z_m$ and we check that it is necessarily trivial. Let $a_1z_1+\cdots+a_mz_m=0$ be a homogeneous non-trivial relation of minimum degree. Since $[z_i]$ form a basis of K/x_dK, this relation becomes trivial when taking classes, which means that $a_i=b_ix_d$ and $x_d(b_1z_1+\cdots+b_mz_m)=0$. Now, x_d is not a divisor of zero in K, which leads to $b_1z_1+\cdots+b_mz_m=0$. However, the relation from before had minimum degree, so $b_i=0$ for all i and also $a_i=0$ for all i. So $(z_1,\dots,z_m)$ is a basis of K, which means that $K\cong\bigoplus_{1\le i\le m} V(-l_i)$. □

Corollary 1.5.3. *Let V be the polynomial ring $k[x_0,\dots,x_d]$ and M a graded V-module of finite type. There is a polynomial $p_M(n)\in\mathbb{Q}[n]$ such that $H(M,n)=p_M(n)$ for $n\gg 0$.*

Proof. We consider the exact sequence given by Theorem 1.5.2:

$$0 \to \bigoplus_{j=1}^{m_{d+1}} V(-n_{d+1j}) \to \cdots \to \bigoplus_{j=1}^{m_1} V(-n_{1j}) \to \bigoplus_{j=1}^{m_0} V(-n_{0j}) \to M \to 0.$$

By Proposition 1.3.3, this sequence can be reduced to the homogeneous components of its modules, hence obtaining an exact sequence of V_0-modules, that is, k-vector spaces:

$$0 \to \bigoplus_{j=1}^{m_{d+1}} V_{n-n_{d+1j}} \to \cdots \to \bigoplus_{j=1}^{m_1} V_{n-n_{1j}} \to \bigoplus_{j=1}^{m_0} V_{n-n_{0j}} \to M_n \to 0.$$

Hence, using Propositions 1.1.8 and 1.3.2, we get

$$H(M,n) = \dim M_n = \sum_{i,j} (-1)^i \dim(V_{n-n_ij}).$$

These V_i are nothing but the k-vector spaces formed by all polynomials of degree i. It is a well-known fact that $\dim V_i = \binom{i+d}{d} = i^d/d! + \cdots + 1 =: p_V(i)$, $i \geq 0$, which gives, for n big enough,

$$H(M,n) = \dim M_n = \sum_{i,j} (-1)^i p_V(n - n_{ij}).$$

□

Definition 1.5.4. A *finite free resolution* of a module M of length l is an exact sequence of the form

$$0 \to M_l \xrightarrow{f_l} M_{l-1} \xrightarrow{f_{l-1}} \cdots \xrightarrow{f_1} M_0 \xrightarrow{\epsilon} M \to 0,$$

where M_i is a free module for all i and $M_l \neq 0$. The homomorphisms f_i are called *boundary maps* and the map ϵ is called an *augmentation map*.

Let $R = k[x_0 \ldots, x_n]$ be a ring and $I \subset R$ a homogeneous ideal. One of our aims is to find a minimal free resolution for the quotient ring R/I[1], where, in this setting, minimal means that $\operatorname{Im} f_i \subset \mathfrak{m} M_{i-1}$. Precisely, the condition of exactness allows us to achieve this by finding a minimal resolution for I. Consider the short exact sequence

$$0 \to I \to R \to R/I \to 0.$$

By splicing this sequence with the finite free resolution defined before, we obtain the following sequence, which is also a finite free resolution:

$$0 \to M_l \xrightarrow{f_l} M_{l-1} \xrightarrow{f_{l-1}} \cdots \xrightarrow{f_1} M_0 \xrightarrow{\epsilon} R \to R/I \to 0.$$

[1]Technically, this set should be understood as a ring resulting from the quotient of a ring and an ideal, but many results seen so far revolve around modules. For the sake of coherence, any ring R will be thought of as a module over itself and any ideal as an R-submodule.

Now, Theorem 1.5.2 is going to be very useful when looking for such minimal free resolutions. This theorem, as we have seen, asserts that every finitely generated R-module has a finite free resolution of length at most $n+1$, which can be reached by computing syzygy modules.

Example 1.5.5 (Free resolutions of ideals)**.**

(a) Let $I = (x^2y, xy^2, yz^2)$ be a monomial ideal in $R = \mathbb{Q}[x, y, z]$. We want to find a free resolution of I. A way to start is by considering the exact sequence

$$R(-3)^3 \xrightarrow{\begin{pmatrix} x^2y & xy^2 & yz^2 \end{pmatrix}} I \to 0.$$

The next steps are very simple. We calculate the first syzygy module, $\mathrm{Ker}\begin{pmatrix} x^2y & xy^2 & yz^2 \end{pmatrix}$, and define f_1 such that $\mathrm{Ker}\begin{pmatrix} x^2y & xy^2 & yz^2 \end{pmatrix} = \mathrm{Im}(f_1)$, that is,

$$f_1 = \begin{pmatrix} -y & -z^2 & 0 \\ x & 0 & -z^2 \\ 0 & x^2 & xy \end{pmatrix}.$$

This allows us to extend the previous exact sequence to

$$R(-4) \oplus R(-5)^2 \xrightarrow{\begin{pmatrix} -y & -z^2 & 0 \\ x & 0 & -z^2 \\ 0 & x^2 & xy \end{pmatrix}} R(-3)^3 \xrightarrow{\begin{pmatrix} x^2y & xy^2 & yz^2 \end{pmatrix}} I \to 0.$$

Now, we proceed analogously. $\mathrm{Ker}(f_1)$ allows us to define

$$f_2 = \begin{pmatrix} z^2 \\ -y \\ x \end{pmatrix},$$

but this last map is injective, so we finally reach the free resolution that we sought:

$$0 \to R(-6) \xrightarrow{\begin{pmatrix} z^2 \\ -y \\ x \end{pmatrix}} R(-4) \oplus R(-5)^2 \xrightarrow{\begin{pmatrix} -y & -z^2 & 0 \\ x & 0 & -z^2 \\ 0 & x^2 & xy \end{pmatrix}} R(-3)^3 \xrightarrow{\begin{pmatrix} x^2y & xy^2 & yz^2 \end{pmatrix}} I \to 0.$$

Note that the length of this resolution is $2 \leq 3$, as guaranteed by Hilbert's syzygy theorem.

(b) There are various software packages that give an answer to such computations. A good example is *Macaulay2*, a software system devoted to supporting research in algebraic geometry and commutative algebra. In Appendix A (a) we redo the calculations of the previous part.

(c) Consider $I = (x^2, y^2, z^2, t^2)$ in $\mathbb{Q}[x, y, z, t]$. A free resolution of I is

$$0 \to R(-8) \xrightarrow{f_3} R(-6)^4 \xrightarrow{f_2} R(-4)^6 \xrightarrow{f_1} R(-2)^4 \xrightarrow{\epsilon} I \to 0,$$

where

$$f_3 = \begin{pmatrix} -t^2 \\ z^2 \\ -y^2 \\ x^2 \end{pmatrix}, \quad f_2 = \begin{pmatrix} z^2 & t^2 & 0 & 0 \\ -y^2 & 0 & t^2 & 0 \\ x^2 & 0 & 0 & t^2 \\ 0 & -y^2 & -z^2 & 0 \\ 0 & x^2 & 0 & -z^2 \\ 0 & 0 & x^2 & y^2 \end{pmatrix}, \quad f_1 = \begin{pmatrix} -y^2 & -z^2 & 0 & -t^2 & 0 & 0 \\ x^2 & 0 & -z^2 & 0 & -t^2 & 0 \\ 0 & x^2 & y^2 & 0 & 0 & -t^2 \\ 0 & 0 & 0 & x^2 & y^2 & z^2 \end{pmatrix}$$

and $\epsilon = \begin{pmatrix} x^2 & y^2 & z^2 & t^2 \end{pmatrix}$.

Chapter 2

Veronese varieties

In the previous chapter we have seen two ways to prove that the length of the homogeneous pieces of a graded module, for big entries, behaves like a polynomial. However, the approach we have used so far is mainly algebra. This section is going to combine the previous results with geometry, associating to each projective variety $Y \subset \mathbb{P}^n$ a polynomial $P_Y \in \mathbb{Q}[t]$ from which it is possible to rigorously and intuitively introduce some of the invariants of a projective variety (dimension, degree and arithmetic genus).

2.1 The Hilbert polynomial of a projective variety

Definition 2.1.1. Let $Y \subset \mathbb{P}^n$ be an algebraic set. Its *homogeneous coordinate ring* is the set

$$S(Y) := k[x_0, \dots, x_n]/I(Y),$$

where $I(Y)$ is the homogeneous ideal of polynomials vanishing on Y. $S(Y)$ has obviously a natural grading induced by

$$(k[x_0, \dots, x_n]/I(Y))_t := k[x_0, \dots, x_n]_t/(I(Y))_t,$$

where this last quotient is a quotient of k-vector spaces.

Definition 2.1.2. If $Y \subset \mathbb{P}^n$ is an algebraic set, we define the *Hilbert function of* Y, F_Y, to be the Hilbert function of its homogeneous coordinate ring $S(Y)$, i.e.,

$$F_Y(t) := \dim(k[x_0, \dots, x_n]/I(Y))_t.$$

Analogously, the *Hilbert polynomial of* Y, P_Y, is defined to be the Hilbert polynomial of $S(Y)$.

Remark 2.1.3. Due to Theorem 1.4.5, we know that the degree of such polynomial is the dimension of Y, since

$$\deg P_Y = \dim \mathbb{V}\left(\operatorname{Ann} \frac{k[x_0, \dots, x_n]}{I(Y)}\right) = \dim \mathbb{V}(I(Y)) = \dim Y.$$

Given the fact that an algebraic set $Y \subset \mathbb{P}^n$ is the intersection of a collection of hypersurfaces, one of the most basic problems we can pose in relation to Y is to describe the hypersurfaces that contain it. In particular, we want to know how many hypersurfaces of each degree contain Y; that is, for each value of t, to know the dimension of the vector space of homogeneous polynomials of degree t vanishing on Y. The Hilbert function of Y is meant to express this information. $F_Y(t) = \dim(k[x_0, \ldots, x_n]/I(Y))_t$ tells us the codimension, in the vector space of all homogeneous polynomials of degree t in $k[x_0, \ldots, x_n]$, of the subspace of those belonging to $I(Y)$, namely, those vanishing on Y.

Example 2.1.4 (Hilbert polynomial of a finite set of points)**.**

(a) To start with a simple case, suppose that Y consists of three nonlinear points $p_1, p_2, p_3 \in \mathbb{P}^2$. The value $F_Y(1)$ tells us exactly whether or not those three points are collinear. We have

$$F_Y(1) = \dim(k[x_0, x_1, x_2]/I(Y))_1 = 3 - \dim(I(Y))_1.$$

Now, $(I(Y))_1$ is the space of homogeneous linear polynomials vanishing at p_1, p_2, p_3. There is no such polynomial unless the three points are collinear, in which case the space is 1-dimensional, generated by the line on which they lie. Thus,

$$F_Y(1) = \begin{cases} 2 \text{ if the three points are collinear.} \\ \\ 3 \text{ otherwise.} \end{cases}$$

On the other hand, we claim that $F_Y(t) = 3$, $t \geq 2$, whatever the position of the points. It is not hard to prove. Consider the homomorphism of k-vector spaces

$$\varphi_t : (k[x_0, x_1, x_2])_t \to k^3,$$

given by evaluation at some fixed class representatives of p_1, p_2, p_3. The kernel of this map, which is the set we are interested in, does not depend on the chosen class representatives. Now, this map is surjective. To see that, take l_1, l_2, l_3 polynomials of degree 1 such that $\{l_i = 0\} \cap \{p_1, p_2, p_3\} = \{p_i\}$. Now,

$$\frac{l_2^{t-1} l_3}{l_2^{t-1} l_3(p_1)} \mapsto (1, 0, 0), \quad \frac{l_1^{t-1} l_3}{l_1^{t-1} l_3(p_2)} \mapsto (0, 1, 0), \quad \frac{l_1^{t-1} l_2}{l_1^{t-1} l_2(p_3)} \mapsto (0, 0, 1),$$

where $(l_i^{t-1} l_j)(p_k)$ actually means evaluation at the chosen class of p_k. Hence, using $\mathrm{Ker}(\varphi_t) = (I(Y))_t$, we have

$$F_Y(t) = \dim(k[x_0, x_1, x_2]_t / I(Y)_t) = \dim(k^3) = 3$$

for all $t \geq 2$. In short, we have seen that

(i) If $p_1, p_2, p_3 \in \mathbb{P}^2$ are collinear, $F_Y(t) = \begin{cases} 2 & \text{if} \quad t = 1 \\ \\ 3 & \text{if} \quad t \geq 2 \end{cases}$

(ii) If $p_1, p_2, p_3 \in \mathbb{P}^2$ are not collinear, $F_Y(t) = 3$, $t \geq 1$.

(b) Similarly, if $Y \subset \mathbb{P}^2$ consists of four points, there are two possible Hilbert functions.

(i) If the four points are collinear,

$$F_Y(t) = \begin{cases} 2 & \text{if} \quad t = 1 \\ 3 & \text{if} \quad t = 2 \\ 4 & \text{if} \quad t \geq 3 \end{cases}$$

(ii) If the points are not collinear, $F_Y(t) = \begin{cases} 3 & \text{if} \quad t = 1 \\ 4 & \text{if} \quad t \geq 2 \end{cases}$

More generally, we see that whenever $Y \subset \mathbb{P}^n$ is a finite set of points, the function $F_Y(t)$, for small values of t, give us information about the position of the points; $F_Y(1)$, for example, tells us the size of the linear subspace of $\mathbb{P}^n$ they span.

(c) The procedure used in (a) can be easily generalized. If $Y \subset \mathbb{P}^n$ consists of $p_1 \ldots, p_d$, then $F_Y(t) = d$ for all $t \geq d - 1$. To prove it, take the homomorphism

$$\varphi_t^d : (k[x_0, \ldots, x_n])_t \to k^d,$$

$t \geq d - 1$, defined as before. Again, this map is surjective. If $l_1, \ldots, l_d$ are homogeneous polynomials of degree 1 such that $\{l_i = 0\} \cap \{p_1, \ldots, p_d\} = \{p_i\}$, we have

$$\frac{l_2^{t-d+2} l_3 \ldots l_d}{l_2^{t-d+2} l_3 \ldots l_d(p_1)} \mapsto (1, \ldots, 0), \quad \ldots, \quad \frac{l_1^{t-d+2} l_2 \ldots l_{d-1}}{l_1^{t-d+2} l_2 \ldots l_{d-1}(p_d)} \mapsto (0, \ldots, 1).$$

This means that

$$F_Y(t) = \dim(k[x_0, \ldots, x_n]_t) - \dim(\operatorname{Ker} \varphi_t^d) = \dim(k^d) = d,$$

so $F_Y(t) = d$ for all $t \geq d - 1$.

Example 2.1.5 (Hilbert polynomial of an algebraic set)**.**

(a) To give an example involving a variety of positive dimension, suppose $Y \subset \mathbb{P}^n$ is the hypersurface $\mathbb{V}(f)$ for some $f \in k[x_0, \ldots, x_n] = R$ of degree d. The following sequence is exact and has degree 0:

$$0 \to R(-d) \xrightarrow{\times f} R \to R/(f) \to 0.$$

This shows that

$$\dim(R/(f))_t = \dim R_t - \dim R(-d)_t,$$

so

$$F_Y(t) = \binom{t+n}{n} - \binom{t-d+n}{n}.$$

(b) We can progressively generalize the example from above. Suppose $f_1, f_2 \in k[x_0, \ldots, x_n]$, where $d_i = \deg f_i$. Assuming $\gcf(f_1, f_2) = 1$, the following sequence is exact and has degree 0:

$$0 \to R(-d_1 - d_2) \xrightarrow{\begin{pmatrix} f_2 \\ -f_1 \end{pmatrix}} R(-d_1) \oplus R(-d_2) \xrightarrow{(f_1\ f_2)} R \to R/(f_1, f_2) \to 0.$$

So we can affirm that

$$F_Y(t) = \binom{t+n}{n} - \binom{t-d_1+n}{n} - \binom{t-d_2+n}{n} + \binom{t-d_1-d_2+n}{n}.$$

(c) When considering f_1, f_2, f_3, the resolution becomes

$$0 \to R(-d_1 - d_2 - d_3) \xrightarrow{\varphi_2} R(-d_1 - d_2) \oplus R(-d_1 - d_3) \oplus R(-d_2 - d_3) \xrightarrow{\varphi_1}$$
$$\xrightarrow{\varphi_1} R(-d_1) \oplus R(-d_2) \oplus R(-d_3) \xrightarrow{\epsilon} R \to R/(f_1, f_2, f_3) \to 0,$$

where

$$\varphi_2 = \begin{pmatrix} f_3 \\ -f_2 \\ f_1 \end{pmatrix}, \quad \varphi_1 = \begin{pmatrix} f_2 & f_3 & 0 \\ -f_1 & 0 & f_3 \\ 0 & -f_1 & -f_2 \end{pmatrix}, \quad \epsilon = \begin{pmatrix} f_1\ f_2\ f_3 \end{pmatrix}.$$

In this case, in order to make this configuration work, the condition

$$\dim R/(f_1, f_2, f_3) = n + 1 - 3$$

is required. The Hilbert polynomial is obtained exactly as before.

(d) This can be generalized for a finite number of functions $f_1, \ldots, f_r \in k[x_0, \ldots, x_n]$, where $\deg f_i = d_i$. However, just as happened in (c), we need to suppose

$$\dim R/(f_1, \ldots, f_r) = n + 1 - r.$$

This condition is usually referred to as *complete intersection*. More specifically, if $Y \subset \mathbb{P}^n$ is a projective variety of codimension r, then the number of generators of $I(Y)$ is at least r and we say that Y is a *complete intersection* if this number of generators of $I(Y)$ equals r. From an algebraic point of view, Y is a complete intersection if and only if $I(Y) = (f_1, \ldots, f_r)$, where $(f_1, \ldots, f_r)$ is a regular sequence. Now, the minimal free R-resolution of $I(Y)$ is given by

$$0 \to \overbrace{R\left(\sum_{j=1}^{r} -d_j\right)}^{F_r} \xrightarrow{\varphi^r_{r-1}} \overbrace{\bigoplus_{1 \le i_1 < \cdots < i_{r-1} \le r} R\left(\sum_{j=1}^{r-1} -d_{i_j}\right)}^{F_{r-1}} \xrightarrow{\varphi^r_{r-2}} \cdots \xrightarrow{\varphi^r_k}$$

$$\underbrace{\bigoplus_{1 \le i_1 < \cdots < i_k \le r} R\left(\sum_{j=1}^{k} -d_{i_j}\right)}_{F_k} \xrightarrow{\varphi^r_{k-1}} \cdots \xrightarrow{\varphi^r_1} \underbrace{\bigoplus_{1 \le i \le r} R(-d_i)}_{F_1} \xrightarrow{\epsilon^r} \underbrace{R}_{F_0} \to R/(f_1, \ldots, f_r) \to 0,$$

where the matrices φ^r_k can be given recursively by

$$\varphi^1_0 = \begin{pmatrix} f_1 \end{pmatrix}$$

and, for all k, r such that $0 \leq k < r$, $r > 1$,

$$\varphi_k^r = \left(\begin{array}{c|c} \varphi_k^{r-1} & f_r \cdot Id \\ \hline 0 & -\varphi_{k-1}^{r-1} \end{array}\right).$$

This resolution is called the *Koszul resolution*. A convention we used is the fact that φ_0^r means ϵ^r for all r. Also, if $k = 0$,

$$\left(\begin{array}{c|c} \varphi_k^{r-1} & f_r \cdot Id \\ \hline 0 & -\varphi_{k-1}^{r-1} \end{array}\right)$$

means

$$\left(\varphi_k^{r-1} \;\middle|\; f_r \cdot Id\right)$$

and if $k = r - 1$,

$$\left(\begin{array}{c|c} \varphi_k^{r-1} & f_r \cdot Id \\ \hline 0 & -\varphi_{k-1}^{r-1} \end{array}\right)$$

means

$$\left(\begin{array}{c} f_r \cdot Id \\ \hline -\varphi_{k-1}^{r-1} \end{array}\right).$$

There are several features one might want to check, the first one being the fact that the number of rows of φ_k^r is the rank of F_k and the number of columns of φ_k^r is the rank of F_{k+1}. Clearly, the rank of F_k is $\binom{r}{k}$. The first cases are very clear (Example 2.1.5 (a), 2.1.5 (b), 2.1.5 (c) might help). Now, suppose the number of rows of φ_i^{r-1} is $\binom{r-1}{i}$ for all $0 \leq i < r-1$. Using induction on r, for any $0 \leq k < r$ we rapidly get that the number of rows of φ_k^r is

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

as expected[1]. An analogous argument shows that the number of columns of φ_k^r is the rank of F_{k+1}, so the sequence is well defined. We may as well use induction on r to see the sequence is exact. The first cases are easy. Now, suppose $\operatorname{Im} \varphi_{i+1}^{r-1} = \operatorname{Ker} \varphi_i^{r-1}$ for all $0 \leq i < r-2$. For any $0 \leq k < r-1$, we have:

$$\varphi_k^r \cdot \varphi_{k+1}^r = \left(\begin{array}{c|c} \varphi_k^{r-1} & f_r \cdot Id \\ \hline 0 & -\varphi_{k-1}^{r-1} \end{array}\right) \cdot \left(\begin{array}{c|c} \varphi_{k+1}^{r-1} & f_r \cdot Id \\ \hline 0 & -\varphi_k^{r-1} \end{array}\right) =$$

$$= \left(\begin{array}{c|c} \varphi_k^{r-1} \cdot \varphi_{k+1}^{r-1} & f_r \cdot \varphi_k^{r-1} - f_r \cdot \varphi_k^{r-1} \\ \hline 0 & \varphi_{k-1}^{r-1} \cdot \varphi_k^{r-1} \end{array}\right) = 0.$$

This shows that $\operatorname{Im}(\varphi_{k+1}^r) \subset \operatorname{Ker}(\varphi_k^r)$ for all k, r. To see the converse, suppose there is a column vector g such that

$$0 = \varphi_k^r \cdot g = \left(\begin{array}{c|c} \varphi_k^{r-1} & f_r \cdot Id \\ \hline 0 & -\varphi_{k-1}^{r-1} \end{array}\right) \cdot \left(\begin{array}{c} \vdots \\ \hline g_{i_1 \ldots i_{k+1}} \\ \hline \vdots \end{array}\right)_{1 \leq i_1 < \cdots < i_{k+1} \leq r}.$$

[1] Of course, any $\binom{i}{j}$ with $j < 0$ or $j > i$ is considered to be 0, so that both cases $k = 0$ and $k = r - 1$ are also taken into consideration.

We can split g as follows:

$$\left.\begin{pmatrix} \vdots \\ g_{i_1\dots i_{k+1}} \\ \vdots \end{pmatrix}\right\} \begin{matrix} g' \\ g'' \end{matrix}$$

where $g' = (g_{i_1\dots i_{k+1}})_{1\leq i_1<\dots<i_{k+1}<r}$ and $g'' = (g_{i_1\dots i_{k+1}})_{1\leq i_1<\dots<i_{k+1}=r}$. We have that $g'' \in \operatorname{Ker}\varphi_{k-1}^{r-1} = \operatorname{Im}\varphi_k^{r-1}$, so $g'' = \varphi_k^{r-1}\cdot z''$. Also,

$$\varphi_k^{r-1}\cdot g' + f_r\cdot g'' = \varphi_k^{r-1}\cdot(g' + f_r\cdot z'') = 0,$$

which means that $g' + f_r\cdot z'' \in \operatorname{Ker}\varphi_k^{r-1} = \operatorname{Im}\varphi_{k+1}^{r-1}$, so $g' + f_r\cdot z'' = \varphi_{k+1}^{r-1}\cdot z'$. With this in mind,

$$\begin{pmatrix} \vdots \\ g_{i_1\dots i_{k+1}} \\ \vdots \end{pmatrix} = \left(\begin{array}{c|c} \varphi_{k+1}^{r-1} & f_r\cdot Id \\ \hline 0 & -\varphi_k^{r-1} \end{array}\right)\cdot\begin{pmatrix} z' \\ \hline -z'' \end{pmatrix},$$

so $g \in \operatorname{Im}\varphi_{k+1}^{r}$, as desired. The last detail we may want to look at is whether or not the exact sequence has degree 0. To see it, suppose that each component of the column vector

$$g = \begin{pmatrix} \vdots \\ g_{i_1\dots i_{k+1}} \\ \vdots \end{pmatrix}_{1\leq i_1<\dots<i_{k+1}\leq r}$$

has degree $t - \sum_{j=1}^{k+1} d_{i_j}$. We would like each component of the vector

$$\varphi_k^r\cdot g = \begin{pmatrix} \vdots \\ g^*_{i_1\dots i_k} \\ \vdots \end{pmatrix}_{1\leq i_1<\dots<i_k\leq r}$$

to have degree $t - \sum_{j=1}^{k} d_{i_j}$. It is also an inductive argument. The first cases, just as before, can be checked out in Example 2.1.5 (a), 2.1.5 (b), 2.1.5 (c). Now, suppose that for all $0 \leq i < r-1$ the map φ_i^{r-1} has degree 0. With the same notation as before,

$$\varphi_k^r\cdot g = \left(\begin{array}{c|c} \varphi_k^{r-1} & f_r\cdot Id \\ \hline 0 & -\varphi_{k-1}^{r-1} \end{array}\right)\cdot\begin{pmatrix} \vdots \\ g_{i_1\dots i_{k+1}} \\ \vdots \end{pmatrix} = \begin{pmatrix} \varphi_k^{r-1}\cdot g' + f_r\cdot g'' \\ \hline -\varphi_{k-1}^{r-1}\cdot g'' \end{pmatrix}.$$

By induction, each component of $\varphi_k^{r-1}\cdot g'$ has degree $t - \sum_{j=1}^{k} d_{i_j}$, each component of $f_r\cdot g''$ has degree $t - \sum_{j=1}^{k} d_{i_j} - r + r = t - \sum_{j=1}^{k} d_{i_j}$ and each component of $-\varphi_{k-1}^{r-1}\cdot g''$ has degree $(t-r) - \sum_{j=1}^{k-1} d_{i_j} = t - \sum_{j=1}^{k} d_{i_j}$, which exactly what we needed. We can give some more examples:

$$\varphi_3^4 = \begin{pmatrix} f_4 \\ -f_3 \\ f_2 \\ -f_1 \end{pmatrix}, \quad \varphi_2^4 = \begin{pmatrix} f_3 & f_4 & 0 & 0 \\ -f_2 & 0 & f_4 & 0 \\ f_1 & 0 & 0 & f_4 \\ 0 & -f_2 & -f_3 & 0 \\ 0 & f_1 & 0 & -f_3 \\ 0 & 0 & f_1 & f_2 \end{pmatrix}, \quad \varphi_1^4 = \begin{pmatrix} f_2 & f_3 & 0 & f_4 & 0 & 0 \\ -f_1 & 0 & f_3 & 0 & f_4 & 0 \\ 0 & -f_1 & -f_2 & 0 & 0 & f_4 \\ 0 & 0 & 0 & -f_1 & -f_2 & -f_3 \end{pmatrix}, \quad \varphi_0^4 = \begin{pmatrix} f_1 & f_2 & f_3 & f_4 \end{pmatrix}$$

and

$$\varphi_4^5 = \begin{pmatrix} f_5 \\ -f_4 \\ f_3 \\ -f_2 \\ f_1 \end{pmatrix}, \quad \varphi_3^5 = \begin{pmatrix} f_4 & f_5 & 0 & 0 & 0 \\ -f_3 & 0 & f_5 & 0 & 0 \\ f_2 & 0 & 0 & f_5 & 0 \\ -f_1 & 0 & 0 & 0 & f_5 \\ 0 & -f_3 & -f_4 & 0 & 0 \\ 0 & f_2 & 0 & -f_4 & 0 \\ 0 & -f_1 & 0 & 0 & -f_4 \\ 0 & 0 & f_2 & f_3 & 0 \\ 0 & 0 & -f_1 & 0 & f_3 \\ 0 & 0 & 0 & -f_1 & -f_2 \end{pmatrix}, \quad \varphi_2^5 = \begin{pmatrix} f_3 & f_4 & 0 & 0 & f_5 & 0 & 0 & 0 & 0 & 0 \\ -f_2 & 0 & f_4 & 0 & 0 & f_5 & 0 & 0 & 0 & 0 \\ f_1 & 0 & 0 & f_4 & 0 & 0 & f_5 & 0 & 0 & 0 \\ 0 & -f_2 & -f_3 & 0 & 0 & 0 & 0 & f_5 & 0 & 0 \\ 0 & f_1 & 0 & -f_3 & 0 & 0 & 0 & 0 & f_5 & 0 \\ 0 & 0 & f_1 & f_2 & 0 & 0 & 0 & 0 & 0 & f_5 \\ 0 & 0 & 0 & 0 & -f_2 & -f_3 & 0 & -f_4 & 0 & 0 \\ 0 & 0 & 0 & 0 & f_1 & 0 & -f_3 & 0 & -f_4 & 0 \\ 0 & 0 & 0 & 0 & 0 & f_1 & f_2 & 0 & 0 & -f_4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & f_1 & f_2 & f_3 \end{pmatrix},$$

$$\varphi_1^5 = \begin{pmatrix} f_2 & f_3 & 0 & f_4 & 0 & 0 & f_5 & 0 & 0 & 0 \\ -f_1 & 0 & f_3 & 0 & f_4 & 0 & 0 & f_5 & 0 & 0 \\ 0 & -f_1 & -f_2 & 0 & 0 & f_4 & 0 & 0 & f_5 & 0 \\ 0 & 0 & 0 & -f_1 & -f_2 & -f_3 & 0 & 0 & 0 & f_5 \\ 0 & 0 & 0 & 0 & 0 & 0 & -f_1 & -f_2 & -f_3 & -f_4 \end{pmatrix}, \quad \varphi_0^5 = \begin{pmatrix} f_1 & f_2 & f_3 & f_4 & f_5 \end{pmatrix}.$$

We can also write down the Hilbert function of the variety $\mathbb{V}(f_1, \ldots, f_r)$:

$$F_Y(t) = \binom{t+n}{n} + \sum_{k=1}^{r} (-1)^k \sum_{1 \leq i_1 < \cdots < i_k \leq r} \binom{t - \sum_{j=1}^{r} d_{i_j} + n}{n}.$$

2.2 Geometric invariants of a projective variety

Our next goal consists of gaining some understanding about three of the geometric invariants of a projective variety $X \subset \mathbb{P}^n$, namely, its *dimension*, its *degree* and its *arithmetic genus*. These three features can be found in the Hilbert polynomial $P_X(t) = a_n t^n + \cdots + a_1 t + a_0$ and are, respectively, n, $a_n n!$ and $(-1)^n(a_0 - 1)$. Now, we are already familiar with the dimension of a variety. In order to formally define degree, we shall first take a look at the following concepts:

Definition 2.2.1. Let V, W be irreducible projective varieties. A *rational map* $\varphi : V \to W$ is an equivalence class of pairs (φ_U, U), where φ_U is a morphism of varieties from an open set $\emptyset \neq U \subset V$ to W and two such pairs (φ_U, U), $(\varphi'_{U'}, U')$ are considered equivalent if φ_U and $\varphi'_{U'}$ coincide on the intersection $U \cap U'$.

The proof that ensures this defines an equivalence relation relies on the following lemma:

Lemma 2.2.2. *If two morphisms of smooth varieties are equal on some non-empty open set, then they are equal.*

A rational map is usually represented by a dashed arrow, as follows:

$$\varphi : V \dashrightarrow W.$$

Example 2.2.3. Projecting from a point p is one of the clearest examples of rational map. We start with a hyperplane $\mathbb{P}^{n-1} \subset \mathbb{P}^n$ and a point $p \in \mathbb{P}^n$ not lying on

$\mathbb{P}^{n-1}$; if we like, we can take coordinates on $\mathbb{P}^n$ so that $\mathbb{P}^{n-1}$ is given by $x_n = 0$ and the point p is actually $[0, \ldots, 0, 1]$. We can then define a map

$$\pi_p : \mathbb{P}^n \setminus \{p\} \to \mathbb{P}^{n-1}$$

by

$$\pi_p : q \mapsto \overline{qp} \cap \mathbb{P}^{n-1},$$

that is, sending a point q to the point of intersection of the line $\overline{qp}$ with the hyperplane $x_n = 0$. π_p is called *projection from the point p to the hyperplane* $\mathbb{P}^{n-1}$ and it is clearly a rational map. In terms of coordinates used earlier, this is merely

$$\pi_p : [x_0, \ldots, x_n] \mapsto [x_0, \ldots, x_{n-1}].$$

Nonetheless, among the ways in which rational maps fail to behave like ordinary maps, the composition of rational maps is not always defined. Take

$$f : X \dashrightarrow Y, \quad g : Y \dashrightarrow Z.$$

It might happen that the image of f lies outside any open subset of Y on which g is defined, making it impossible to consider a composition, even as a rational map. One circumstance in which this will not happen, though, is if the map f is *dominant*, meaning that the closure of the image of f is Y. It is clear from the definitions that given a pair of rational maps f, g with f dominant, the composition $g \circ f$ is a well-defined rational map.

Definition 2.2.4. A rational map $f : X \dashrightarrow Y$ is *birational* if there exists a rational map $g : Y \dashrightarrow X$ such that $f \circ g$ and $g \circ f$ are both defined and equal to the identity.

With this in mind, we are ready to define the degree of a projective variety $X \subset \mathbb{P}^n$. It may be defined in ways mostly analogous to the notion of dimension. As we know, we defined dimension by saying that $\dim \mathbb{P}^n = n$. We then said that a projective variety $X \subset \mathbb{P}^n$ admits a surjective map to some projective space $\mathbb{P}^k$ and we simply defined $\dim X$ to be k. To define degree, we may again start with a case where we have some intuition of what degree should be: if $X \subset \mathbb{P}^{k+1}$ is a hypersurface, given as the set where a homogeneous irreducible polynomial F vanishes, then the degree of X should be the degree of the polynomial F.

Definition 2.2.5. Let $X \subset \mathbb{P}^n$ be an irreducible k-dimensional variety. Its degree can be described in the following two ways:

(i) Unless X is already a hypersurface, the projection map $\pi_p : X \to \mathbb{P}^{n-1}$ from a general point $p \in \mathbb{P}^n$ is birational onto its image. Thus, we can project successively from general points until we get a hypersurface in $\mathbb{P}^{k+1}$. We may define the degree of X to be the degree of this hypersurface.

(ii) The degree of X can also be defined as the maximum number of points of intersection of X with a linear subspace L such that $\dim X + \dim L = n$.

Definition 2.2.6. A *rational normal curve* is the image of a map of the form

$$v_d : \mathbb{P}^1 \to \mathbb{P}^d$$

given by

$$[z_0, z_1] \mapsto [z_0^d, z_0^{d-1}z_1, \ldots, z_1^d].$$

Proposition 2.2.7. *The image of v_d is the set where the polynomials $F_{ij}(x) = x_i x_j - x_{i-1}x_{j+1}$ vanish for all $1 \leq i \leq j \leq d-1$.*

Proof. One inclusion is clear, since

$$F_{ij}(z_0^d, z_0^{d-1}z_1, \ldots, z_1^d) = z_0^{d-i}z_1^i z_0^{d-j}z_1^j - z_0^{d-i+1}z_1^{i-1}z_0^{d-j-1}z_1^{j+1} = 0.$$

For the converse, consider a point $[x_0, \ldots, x_d] \in \mathbb{P}^d$ such that $x_i x_j - x_{i-1}x_{j+1} = 0$ for all $1 \leq i \leq j \leq d-1$. Take $x_0 = 0$. If $i = 1$, we have $x_1 x_j = 0$ for all $1 \leq j \leq d-1$, which means in particular that $x_1 = 0$; on the other hand, $i = 2$ implies $x_2 x_j = 0$ for all $2 \leq j \leq d-1$, which means $x_2 = 0$, and so forth. This procedure ends when $i = d-1$ and forces $[x_0, \ldots, x_d]$ to be exactly $[0, \ldots, 1]$, which is indeed an element of the image.

We can suppose $x_0 \neq 0$. In this case, $[x_0, \ldots, x_d] = [x_0^d, x_0^{d-1}x_1 \ldots, x_0^{d-1}x_d]$. Now, take the term $x_0^{d-1}x_k$ for some $2 \leq k \leq d$. Using the fact that $x_0 x_j = x_1 x_{j-1}$ for all $2 \leq j \leq d$, it holds that

$$x_0^{d-1}x_k = x_0^{d-2}x_1 x_{k-1} = x_0^{d-3}x_1^2 x_{k-2} = \cdots = x_0^{d-k-1}x_1^k x_0 = x_0^{d-k}x_1^k,$$

which completes the proof. □

Example 2.2.8. If $d = 2$, we get the plane conic curve $x_0x_2 - x_1^2 = 0$. If $d = 3$, the curve receives the name of *twisted cubic* and it is given by the equations

$$x_0x_2 - x_1^2 = 0, \quad x_0x_3 - x_1x_2 = 0, \quad x_1x_2 - x_2^2 = 0.$$

Example 2.2.9 (Hilbert polynomial of the rational normal curve)**.**

(a) As a first approach, we shall first find the Hilbert polynomial of the twisted cubic. Consider the image of the map

$$[z_0, z_1] \mapsto [z_0^3, z_0^2z_1, z_0z_1^2, z_1^3].$$

As we have seen, this variety is described by the equations

$$x_0x_2 - x_1^2 = 0, \quad x_0x_3 - x_1x_2 = 0, \quad x_1x_3 - x_2^2 = 0.$$

We define $I := (x_0x_2 - x_1^2, x_0x_3 - x_1x_2, x_1x_3 - x_2^2)$. By definition, the Hilbert function of the variety is

$$F_Y(t) = \dim(k[x_0, x_1, x_2, x_3]/I(V(I)))_t,$$

but I is a radical ideal, since it is actually the kernel of the map

$$\varphi : k[x_0, x_1, x_2, x_3] \to k[x_0, x_1]$$

given by

$$p(x_0, x_1, x_2, x_3) \mapsto p(x_0^3, x_0^2x_1, x_0x_1^2, x_1^3).$$

Clearly, $k[x_0, x_1, x_2, x_3]/I \cong \mathrm{Im}(\varphi) \subset k[x_0, x_1]$, which is an integral domain. I is therefore prime and hence radical. We already know that $\deg P_Y = \dim \mathrm{Im}(v_3) = 1$. As we can see in Appendix A (b), we can use *Macaulay2* to find the whole polynomial, which turns out to be $3t + 1$.

(b) We are now going to find a general answer. Let Y be $\mathrm{Im}(v_d)$; we want the Hilbert polynomial of Y. For all t consider the homomorphism of k-vector spaces

$$\varphi_t : k[x_0, \dots, x_d]_t \to k[x_0, x_1]_{dt},$$

defined by $p(x_0, \dots, x_d) \mapsto p(x_0^d, x_0^{d-1}x_1, \dots, x_1^d)$. The kernel of this map is, precisely, the set of polynomials of degree t that vanish on the rational normal curve, that is, $\mathrm{Ker}(\varphi_t) = I(Y)_t$. Also, this map is clearly exhaustive. Hence

$$k[x_0, \dots, x_d]_t / I(Y)_t = S(Y)_t \cong k[x_0, x_1]_{dt},$$

and this implies

$$F_Y(t) = \dim(k[x_0, x_1])_{dt} = \binom{dt+1}{1} = dt + 1.$$

Note that, in this case, the Hilbert polynomial and Hilbert function are identical.

The following concept is the natural generalization of the rational normal curves.

2.3 Veronese varieties

Definition 2.3.1. For any n and d we define the *Veronese map* of degree d

$$v_{n,d} : \mathbb{P}^n \to \mathbb{P}^{N_{n,d}-1}$$

by sending

$$z = [z_0, \dots, z_n] \mapsto [\dots, m_i(z), \dots],$$

where $m_i(z)$ ranges over all monomials of degree d in $z_0, \dots, z_n$ and $N_{n,d}$ is simply the binomial coefficient $\binom{n+d}{d}$.

The image of the Veronese map is an algebraic variety of dimension n, often called a *Veronese variety*. We will denote it by $V_{n,d}$. Now, let each monomial of degree d $m_i(z) = z_0^{i_0} \dots z_n^{i_n}$ correspond to the variable $x_{i_0 \dots i_n}$ in $\mathbb{P}^{N_{n,d}-1}$. We have the following characterization:

Proposition 2.3.2. *The Veronese varieties are exactly the set where the polynomials*

$$F_{IJKL} = x_{i_0 \dots i_n} x_{j_0 \dots j_n} - x_{k_0 \dots k_n} x_{l_0 \dots l_n}$$

vanish, where $I = (i_h)_h$, $J = (j_h)_h$, $K = (k_h)_h$, $L = (l_h)_h$ *are multi-indices such that* $i_h + j_h = k_h + l_h$ *for all* h.

Proof. Similarly to the rational normal curves, one inclusion is obvious, because

$$F_{IJKL}(\dots, m_i(z), \dots) = z_0^{i_0} \dots z_n^{i_n} z_0^{j_0} \dots z_n^{j_n} - z_0^{k_0} \dots z_n^{k_n} z_0^{l_0} \dots z_n^{l_n} = 0.$$

To prove the converse, we shall take an element $[\dots, x_{i_0 \dots i_n}, \dots] \in \mathbb{P}^{N_{n,d}-1}$ verifying the equations from above. The first observation we can make is the fact that these equations are incompatible with the condition $x_{d\dots 0} = \dots = x_{0\dots d} = 0$, so we can suppose there is a term $x_{0\dots d\dots 0} \neq 0$. For simplicity purposes suppose it is the first one, i.e., $x_{d\dots 0} \neq 0$. Now, consider the product

$$x_{d\dots 0}^{d-1} x_{i_0 \dots i_n} = x_{d\dots 0}^{d-2} x_{d-1,10\dots 0} x_{i_0+1, i_1-1 \dots i_n} = \dots = x_{d\dots 0}^{d-i_1-1} x_{d-1,10\dots 0}^{i_1} x_{i_0+i_1, 0\dots i_n}.$$

We can iterate this procedure with the rest of i_h, thus obtaining

$$x_{d\dots 0}^{d-i_1-\dots-i_n-1} x_{d-1,10\dots 0}^{i_1} \dots x_{d-1,0\dots 1}^{i_n} x_{i_0+\dots+i_n, 0\dots 0} =$$

$$= x_{d\dots 0}^{i_0-1} x_{d-1,10\dots 0}^{i_1} \dots x_{d-1,0\dots 1}^{i_n} x_{d0\dots 0} = x_{d\dots 0}^{i_0} x_{d-1,10\dots 0}^{i_1} \dots x_{d-1,0\dots 1}^{i_n}.$$

Therefore,

$$[\dots, x_{i_0 \dots i_n}, \dots] = [\dots, x_{d\dots 0}^{i_0} x_{d-1,10\dots 0}^{i_1} \dots x_{d-1,0\dots 1}^{i_n}, \dots],$$

which is the image of $[x_{d\dots 0}, x_{d-1,10\dots 0}, \dots, x_{d-1,0\dots 1}]$. □

Example 2.3.3 (Hilbert polynomial of the Veronese map)**.** It suffices to generalize Example 2.2.9 (b). Let Y be $\mathrm{Im}(v_{n,d})$. For all t we consider the homomorphism of k-vector spaces

$$\varphi_t : k[x_0, \dots, x_{N_{n,d}-1}]_t \to k[x_0, \dots, x_n]_{dt},$$

defined by $p(x_0, \dots, x_{N_{n,d}-1}) \mapsto p(\dots, m_i(x), \dots)$ (the notation is the same as in Definition 2.3.1). Just like before, we have $\mathrm{Ker}(\varphi_t) = I(Y)_t$. Also, this map is clearly exhaustive. Hence

$$k[x_0, \dots, x_{N_{n,d}-1}]_t / I(Y)_t = S(Y)_t \cong k[x_0, \dots, x_n]_{dt}$$

and this forces

$$F_Y(t) = \dim(k[x_0, \dots, x_n]_{dt}) = \binom{dt+n}{n} = \frac{d^n}{n!} t^n + \dots.$$

Again, the Hilbert polynomial and the Hilbert function coincide. It is also clear that the degree of $V_{n,d}$ is d^n and its arithmetic genus is 0.

One natural problem we may pose in regard to Hilbert functions and Hilbert polynomials is to give explicit estimates for how large t has to be to ensure that $P_Y(t) = F_Y(t)$. This is a very difficult problem. It is already a major theorem that a minimum t_0 exists, and very little is known about its actual value, even in simple cases. For example, Castelnuovo showed that taking $t_0 = d - 2$ is sufficient for irreducible curves $C \subset \mathbb{P}^3$ with Hilbert polynomial $p(t) = dt + c$, but we are still miles away from understanding the general question.

2.4 Arithmetically Cohen-Macaulay varieties

Definition 2.4.1. Let M be a graded R-module. M is said to be of finite projective dimension if there is a free R-resolution of M that has the form

$$0 \to M_l \xrightarrow{f_l} M_{l-1} \xrightarrow{f_{l-1}} \cdots \xrightarrow{f_1} M_0 \to M \to 0.$$

The minimum of the length l of such free resolution is called the projective dimension of M and it is denoted by $\mathrm{pd}(M)$.

Definition 2.4.2. A variety $X \subset \mathbb{P}^n$ is said to be *arithmetically Cohen-Macaulay* (briefly, *ACM*) if $\mathrm{pd}(R/I(X)) = \operatorname{codim} X$.

Hence, if $X \subset \mathbb{P}^n$ is an ACM projective variety of codimension l, a graded minimal free R-resolution of $I(X)$ is of the form:

$$0 \to F_l \xrightarrow{f_l} F_{l-1} \xrightarrow{f_{l-1}} \cdots \xrightarrow{f_2} F_1 \xrightarrow{f_1} I(X) \to 0,$$

where $F_i = \bigoplus_{j\in\mathbb{Z}} R(-i-j)^{\beta_{ij}}$ for all $1 \leq i \leq l$. The integers $\beta_{ij}(X)$ are called the *graded Betti numbers of* X and are usually represented in a table.

Proposition 2.4.3. *All Veronese varieties $V_{n,d}$ are arithmetically Cohen-Macaulay.*

Proof. See [7] for further details. □

We shall use *Macaulay2* and check this is true for small values of n, d:

Example 2.4.4. Consider the twisted cubic, $X = V_{1,3}$. As we can see in Appendix A (c), the minimal resolution of $M = R/I(X)$ has length 2 and $\operatorname{codim} X = 3 - 1 = 2$, as expected.

Example 2.4.5. Consider now the Veronese variety $X = V_{2,3}$. According to Appendix A (d), $\mathrm{pd}(R/I(X)) = 7$, which equals $\operatorname{codim} X = 9 - 2 = 7$.

Complete intersections are one of the simplest examples of ACM varieties, since both the length of the Koszul resolution and the codimension equal r. It is not true, though, that any ACM variety is a complete intersection.

Example 2.4.6. Consider the twisted cubic curve $C \subset \mathbb{P}^3$, with $I(C) = (x_0x_2 - x_1^2, x_0x_3 - x_1x_2, x_1x_3 - x_2^2)$. Its minimal free resolution is the following:

$$0 \to R(-3)^2 \xrightarrow{f_2} R(-2)^3 \xrightarrow{f_1} I(C) \to 0,$$

where

$$f_2 = \begin{pmatrix} -x_1 & x_0 \\ x_2 & -x_1 \\ -x_3 & x_2 \end{pmatrix}, \quad f_1 = \begin{pmatrix} x_0x_2 - x_1^2 & x_0x_3 - x_1x_2 & x_1x_3 - x_2^2 \end{pmatrix}.$$

So the twisted cubic is ACM, yet it is not a complete intersection.

Example 2.4.7. The smooth rational quartic curve $C \subset \mathbb{P}^3$, given by

$$I(C) = (x_0x_3 - x_1x_2, x_0x_2^2 - x_1^2x_3, x_1x_3^2 - x_2^3, x_2x_0^2 - x_1^3),$$

is an example of non-ACM variety. $I(C)$ has the following minimal free resolution:

$$0 \to R(-5) \xrightarrow{f_3} R(-4)^4 \xrightarrow{f_2} R(-3)^3 \oplus R(-2) \xrightarrow{f_1} I(C) \to 0,$$

where

$$f_2 = \begin{pmatrix} -x_0 \\ -x_1 \\ x_2 \\ -x_3 \end{pmatrix}, \quad f_3 = \begin{pmatrix} -x_2^2 & x_1x_3 & -x_0x_2 & -x_1^2 \\ 0 & 0 & x_3 & x_2 \\ x_1 & -x_0 & 0 & 0 \\ x_3 & -x_2 & -x_1 & -x_0 \end{pmatrix}$$

and

$$f_1 = \begin{pmatrix} x_0x_3 - x_1x_2 & x_0x_2^2 - x_1^2x_3 & x_1x_3^2 - x_2^3 & x_2x_0^2 - x_1^3 \end{pmatrix}.$$

2.5 Monomial projections of Veronese varieties

Another type of projective varieties we are going to focus on is constructed by taking the Veronese variety $v_{n,d}$ and projecting it from a given set of points. Similarly to Example 2.2.3, the projection we want to work with simply consists of

$$\pi : [x_1, \ldots, x_{N_{n,d}}] \mapsto [x_{i_1}, \ldots, x_{i_r}].$$

Of course, when removing terms from the image, there is a risk that we get an undefined map, so the domain has to be $\mathbb{P}^{N_{n,d}-1}$ minus a set of points; π is therefore a rational map, not a morphism between varieties. Consider now all possible monomials of degree d in $n+1$ variables, namely, $m_1, \ldots, m_{N_{n,d}}$, and a subset of these: $m_{i_1}, \ldots, m_{i_r}$ for some $1 \leq i_j \leq N_{n,d}$. We want to study the closure of the image of the map $\psi = \pi \circ v_{n,d}$, which sends $x = [x_0, \ldots, x_n] \in \mathbb{P}^n$ to $[m_{i_1}(x), \ldots, m_{i_r}(x)] \in \mathbb{P}^{r-1}$. The following commutative diagram summarises this whole idea:

$$\begin{array}{ccccc} \mathbb{P}^n & \xrightarrow{v_{n,d}} & \mathbb{P}^{N_{n,d}-1} & \xhookleftarrow{i} & V_{n,d} \\ & \searrow^{\psi} & \downarrow \pi & & \downarrow \\ & & \mathbb{P}^{r-1} & \xhookleftarrow{i} & Y_{n,d} \end{array}$$

If the set of parameters of a projection is obtained by deleting one or two or three monomials, then we call this a simple or double or triple projection of $v_{n,d}$, respectively. We want to find out which Hilbert polynomial has the resulting variety and whether or not it is ACM. This last question is called *Gröbner problem* and it is still today an open problem.

Notation: The monomials that are removed will be noted as superscripts.

Example 2.5.1 (Hilbert polynomial of simple projections of $v_{n,d}$)**.**

(a) Consider the twisted cubic, defined by the image of

$$v_{1,3} : [z_0, z_1] \mapsto [z_0^3, z_0^2 z_1, z_0 z_1^2, z_1^3].$$

Remove, according to the previous remarks, the first term, i.e.,

$$v_{1,3}^{3,0} : [z_0, z_1] \mapsto [z_0^2 z_1, z_0 z_1^2, z_1^3].$$

Using *Macaulay2*, we can obtain the ideal of polynomials $I \subset k[x, y, z]$ vanishing on the image, which will eventually lead us to the Hilbert polynomial of the projection. These computations are written in Appendix A (e) and show that the Hilbert polynomial of $\mathrm{Im}(v_{1,3}^{3,0})$ is $2t + 1$. We now proceed analogously. The following correspondence maps each projection to its Hilbert polynomial:

- $v_{1,3}^{3,0} \mapsto 2t + 1$
- $v_{1,3}^{2,1} \mapsto 3t$
- $v_{1,3}^{1,2} \mapsto 3t$
- $v_{1,3}^{0,3} \mapsto 2t + 1$

As we can observe, there seems to be some symmetry when removing monomials from the Veronese map, that is, the behaviour of the polynomials obtained is not completely random. This is partly due to the fact that $v_{1,3}^{3,0}$ and $v_{1,3}^{0,3}$ can be simplified; note that

$$[z_0^2 z_1, z_0 z_1^2, z_1^3] = [z_0^2, z_0 z_1, z_1^2]$$

and also

$$[z_0^3, z_0^2 z_1, z_0 z_1^2] = [z_0^2, z_0 z_1, z_1^2].$$

So both $v_{1,3}^{3,0}$ and $v_{1,3}^{0,3}$ coincide with $v_{1,2}$. This explains why both maps produce the polynomial $2t + 1$, according to Example 2.2.9 (b). On the other hand, a mere change of variables shows that the image of $v_{1,3}^{2,1}$ and $v_{1,3}^{1,2}$ is identical and thus give the same Hilbert polynomial. Now, consider the following diagram:

$$z_0^3 \text{ —— } z_0^2 z_1 \text{ —— } z_0 z_1^2 \text{ —— } z_1^3$$

Removing any vertex produces the polynomial $2t + 1$ and removing a term from the inside produces the polynomial $3t$. We shall see that sorting the terms in an analogous way, even in higher dimensions, give precious information about which Hilbert polynomials appear.

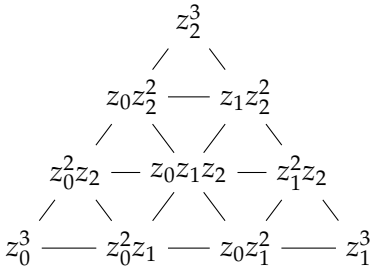
(b) Consider a more complicated case, say

$$v_{2,3} : [z_0, z_1, z_2] \mapsto [z_0^3, z_0^2 z_1, z_0 z_1^2, z_1^3, z_0^2 z_2, z_0 z_1 z_2, z_1^2 z_2, z_0 z_2^2, z_1 z_2^2, z_2^3].$$

In this case, the Hilbert polynomial of each projection is given by the following correspondence:

- $v_{2,3}^{3,0,0} \mapsto 4t^2+4t+1$
- $v_{2,3}^{2,1,0} \mapsto \frac{9}{2}t^2+\frac{9}{2}t$
- $v_{2,3}^{1,2,0} \mapsto \frac{9}{2}t^2+\frac{9}{2}t$
- $v_{2,3}^{0,3,0} \mapsto 4t^2+4t+1$
- $v_{2,3}^{2,0,1} \mapsto \frac{9}{2}t^2+\frac{9}{2}t$
- $v_{2,3}^{1,1,1} \mapsto \frac{9}{2}t^2+\frac{9}{2}t+1$
- $v_{2,3}^{0,2,1} \mapsto \frac{9}{2}t^2+\frac{9}{2}t$
- $v_{2,3}^{1,0,2} \mapsto \frac{9}{2}t^2+\frac{9}{2}t$
- $v_{2,3}^{0,1,2} \mapsto \frac{9}{2}t^2+\frac{9}{2}t$
- $v_{2,3}^{0,0,3} \mapsto 4t^2+4t+1$

Here, the diagram sorting out all monomials $z_0^{i_0}z_1^{i_1}z_2^{i_2}$ of degree 3 is:

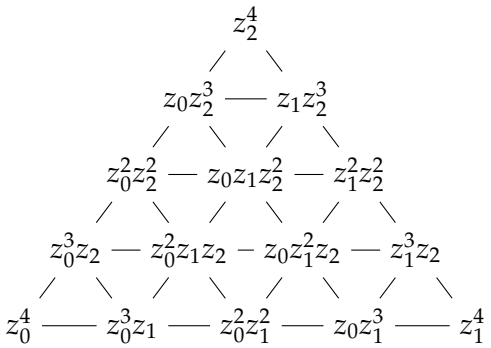


And again, one observes that any vertex of the triangle gives the polynomial $4t^2+4t+1$, any monomial from the sides gives the polynomial $\frac{9}{2}t^2+\frac{9}{2}t$ and the element from the inside gives $\frac{9}{2}t^2+\frac{9}{2}t+1$. If we were in three dimensions, we would be coping with a tetrahedron and an analogous phenomenon would happen.

(c) Consider the map $v_{2,4}$. The Hilbert polynomial of each projection is

- $v_{2,4}^{4,0,0} \mapsto \frac{15}{2}t^2+\frac{11}{2}t+1$
- $v_{2,4}^{3,1,0} \mapsto 8t^2+6t$
- $v_{2,4}^{2,2,0} \mapsto 8t^2+6t$
- $v_{2,4}^{1,3,0} \mapsto 8t^2+6t$
- $v_{2,4}^{0,4,0} \mapsto \frac{15}{2}t^2+\frac{11}{2}t+1$
- $v_{2,4}^{3,0,1} \mapsto 8t^2+6t$
- $v_{2,4}^{2,1,1} \mapsto 8t^2+6t+1$
- $v_{2,4}^{1,2,1} \mapsto 8t^2+6t+1$
- $v_{2,4}^{0,3,1} \mapsto 8t^2+6t$
- $v_{2,4}^{2,0,2} \mapsto 8t^2+6t$
- $v_{2,4}^{1,1,2} \mapsto 8t^2+6t+1$
- $v_{2,4}^{0,2,2} \mapsto 8t^2+6t$
- $v_{2,4}^{1,0,3} \mapsto 8t^2+6t$
- $v_{2,4}^{0,1,3} \mapsto 8t^2+6t$
- $v_{2,4}^{0,0,4} \mapsto \frac{15}{2}t^2+\frac{11}{2}t+1$

and the diagram is, in this case,



The same remarks as in the previous part happen again.

In the first case we discussed, $v_{1,3}^{3,0}$, we might have observed that the Hilbert polynomial obtained depended on whether or not the point p from which we projected belonged to $V_{1,3}$. When $p \in V_{1,3}$, $2t+1$ is obtained; whereas when $p \notin V_{1,3}$, $3t$ appears. It can be easily checked that this happens in more complex examples, being relevant the multiplicity of the point from which we project.

Of course, we can remove more than one monomial, which leads to a huge variety of cases. In the following example we write some of them and the Hilbert polynomial they are correlated to. The superscripts indicate which monomials are deleted.

Example 2.5.2 (Hilbert polynomial of other projections of $v_{n,d}$)**.**

- $v_{1,3}^{(3,0),(2,1)} \mapsto t+1$
- $v_{1,3}^{(2,1),(1,2)} \mapsto t+1$
- $v_{2,3}^{(3,0,0),(2,1,0),(1,2,0),(0,3,0)} \mapsto 2t^2+3t+1$
- $v_{2,3}^{(2,1,0),(1,2,0),(0,2,1)} \mapsto \frac{9}{2}t^2+\frac{3}{2}t+1$
- $v_{2,4}^{(1,0,3),(2,1,1),(1,1,2),(0,4,0)} \mapsto \frac{15}{2}t^2+\frac{11}{2}t-1$
- $v_{3,2}^{(1,0,1,0),(0,1,0,1)} \mapsto \frac{4}{3}t^3+4t^2+\frac{5}{3}t+1$
- $v_{3,2}^{(2,0,0,0),(1,0,1,0),(0,1,0,1)} \mapsto t^3+3t^2+2t+1$

As we said before, another important issue we may want to look at is whether or not the monomial projection obtained is ACM. With the help of Macaulay2 we can see what happens with some of the cases we have discussed so far. The computations of the first case are written in Appendix A (f); the others are obtained analogously. As we have seen, though, some monomial projections coincide with other Veronese varieties and due to Proposition 2.4.3 they are automatically ACM.

Example 2.5.3 (Gröbner problem)**.**

- $v_{1,3}^{3,0}$: codim $= 2-1 = 1$, pd $= 1$. ACM: yes.
- $v_{1,3}^{2,1}$: codim $= 2-1 = 1$, pd $= 1$. ACM: yes.
- $v_{1,3}^{1,2}$: codim $= 2-1 = 1$, pd $= 1$. ACM: yes.
- $v_{1,3}^{0,3}$: codim $= 2-1 = 1$, pd $= 1$. ACM: yes.
- $v_{2,3}^{3,0,0}$: codim $= 8-2 = 6$, pd $= 6$. ACM: yes.
- $v_{2,3}^{2,1,0}$: codim $= 8-2 = 6$, pd $= 7$. ACM: no.
- $v_{2,3}^{1,2,0}$: codim $= 8-2 = 6$, pd $= 7$. ACM: no.

- $v_{2,3}^{0,3,0}$: codim = $8-2=6$, pd = 6. ACM: yes.
- $v_{2,3}^{2,0,1}$: codim = $8-2=6$, pd = 7. ACM: no.
- $v_{2,3}^{1,1,1}$: codim = $8-2=6$, pd = 8. ACM: no.
- $v_{2,3}^{0,2,1}$: codim = $8-2=6$, pd = 7. ACM: no.
- $v_{2,3}^{1,0,2}$: codim = $8-2=6$, pd = 7. ACM: no.
- $v_{2,3}^{0,1,2}$: codim = $8-2=6$, pd = 7. ACM: no.
- $v_{2,3}^{0,0,3}$: codim = $8-2=6$, pd = 6. ACM: yes.
- $v_{1,3}^{(3,0),(2,1)}$ codim = $1-1=0$, pd = 0. ACM: yes.
- $v_{1,3}^{(2,1),(1,2)}$: codim = 7, pd = 7. ACM: yes.
- $v_{2,3}^{(3,0,0),(2,1,0),(1,2,0),(0,3,0)}$: codim = $1-1=0$, pd = 0. ACM: yes.
- $v_{2,3}^{(2,1,0),(1,2,0),(0,2,1)}$: codim = $6-2=4$, pd = 4. ACM: yes.
- $v_{2,4}^{(1,0,3),(2,1,1),(1,1,2),(0,4,0)}$: codim = $10-2=8$, pd = 10. ACM: no.
- $v_{3,2}^{(1,0,1,0),(0,1,0,1)}$: codim = $7-3=4$, pd = 5. ACM: no.
- $v_{3,2}^{(2,0,0,0),(1,0,1,0),(0,1,0,1)}$: codim = $6-3=3$, pd = 4. ACM: no.

There were first some efforts of Renschuch to solve Gröbner's problem in [16, 17], but the first important result is due to Schenzel, who showed in [18] exactly which simple projection of $v_{n,d}$ is ACM. A basic tool one has to work with is the fact that the homogeneous coordinate ring of a simple projection of $V_{n,d}$ is isomorphic to the semigroup ring over k of an affine semigroup in $\mathbb{Z}_{\geq 0}^{n+1}$ generated by $N_{n,d}-1$ elements of the set

$$J = \{(\alpha_0, \ldots, \alpha_n) \in \mathbb{Z}_{\geq 0}^{n+1} : \alpha_0 + \cdots + \alpha_n = d\}.$$

We denote by a the element of J deleted by the projection and set

$$e_i = (0, \ldots, d, \ldots, 0) \in \mathbb{Z}_{\geq 0}^{n+1},$$

where d stands at the i-th place, $i = 1, \ldots, n+1$, and

$$e_{ij} = (0, \ldots, d-1, \ldots, 1, \ldots, 0) \in \mathbb{Z}_{\geq 0}^{n+1},$$

where $d-1$ stands at the i-th place and 1 at the j-th place, $i, j = 1, \ldots, n+1$ with $i \neq j$.

Proposition 2.5.4. *A simple projection of $v_{n,d}$ is ACM if and only if*

(1) $a = e_i$ for some i, or

(2) $a = e_{ij}$ *for some* i, j *with* $n = 1$ *or* $(n, d) = (2, 2)$.

Schenzel's method, though, could not be applied to the classification of double projections of Veronese varieties. This was achieved by N. V. Trung [20], who used the theory of affine semigroup rings. With the same notation as before, consider a, b, $a \neq b$, to be the elements deleted from J. Again, the homogeneous coordinate ring of a double projection of $V_{n,d}$ is isomorphic to the semigroup ring over k of an affine semigroup in $\mathbb{Z}_{\geq 0}^{n+1}$ generated by $N_{n,d} - 2$ elements of J. By a suitable permutation we always have one of the following situations:

(1) $a = e_1$, b arbitrary.

(2) $a = e_{12}, b \neq e_1, \ldots, e_{n+1}$.

(3) $a, b \neq e_i, e_{ij}$ for all $i, j = 1, \ldots, n+1$ with $i \neq j$.

We denote $f_1 = (d-2, 2, \ldots, 0)$, $f_2 = (d-3, 3, \ldots, 0)$, $f_3 = (d-2, 1, \ldots, 0)$.

Proposition 2.5.5. *For each case we listed before, a double projection of* $v_{n,d}$ *is ACM if and only if the following conditions hold:*

(1) $b = e_2, e_{12}$,
$b = f_1$ *with* $n = 1$ *or* $(n, d) = (2, 3)$,
$b = e_{21}$ *with* $n = 1$ *or* $(n, d) = (2, 3)$,
b_{23} *with* $(n, d) = (2, 2)$.

(2) $b = f_1, f_2, e_{21}$ *with* $n = 1$,
$b = e_{21}$, *with* $(n, d) = (2, 3), (2, 4)$,
$b = e_{13}$ *with* $(n, d) = (2, 2), (3, 2)$.

(3) Impossible for $v_{n,d}$ *to be ACM.*

Finally, one could ask what happens further with multiple projections of Veronese varieties. The classification of triple projections is far more complicated that the ones we have just seen, yet can be found in [10].

Chapter 3

Effective results on sumsets

One of the main goals of this paper is to approach a problem that concerns sums of finite integer sets, also known as *sumsets problem*. This is an issue which can be seen from the point of view of additive combinatorics, yet is rough and simple computations do not give efficient answers. Throughout this chapter we are going to shed some light to this problem using algebraic geometry.

3.1 Basic concepts and examples

Definition 3.1.1. Let $A, B \subset \mathbb{Z}^n$. We define $A + B := \{a + b : a \in A, b \in B\}$ and $tA := \underbrace{A + \cdots + A}_{t \text{ times}}$ for all $t \in \mathbb{Z}_{\geq 0}$. This set is called a *sumset*. As usual, $0A$ is defined to be $\{0\}$.

Definition 3.1.2. Let $A \subset \mathbb{Z}^n$ any finite set. We define the numerical function

$$\begin{aligned} \varphi_A : \mathbb{Z}_{\geq 0} &\to \mathbb{Z}_{\geq 1} \\ t &\mapsto |tA|. \end{aligned}$$

Our interest is now focused on the behaviour of this function as t grows, which is a longstanding problem in additive combinatorics. Khovanskii proved in [11] that $\varphi_A(t)$ becomes a polynomial $p_A(t) \in \mathbb{Q}[t]$ of degree at most n when t is sufficiently large, but there is not much known about this polynomial, nor the minimum value t_0 from which $\varphi_A(t) = p_A(t)$. This value, by the way, is called *phase transition* or *regularity index*.

In this chapter we will identify φ_A with the Hilbert polynomial of a suitable monomial projection $Y_{n,d}$ of a Veronese variety $V_{n,d}$ so that we get upper bounds for the phase transition as well as for identifying certain coefficients of $p_A(t)$. Notwithstanding, we can first compute some examples and, given A, get an idea of how φ_A behaves. The following program receives an input $A \subset \mathbb{Z}^n$ and gives the values of $|tA|$.

```
#include <stdio.h>
#include <stdlib.h>
#include <math.h>

void initialize(int, int, int ***, int ***, int ***, FILE *);
int sumset(int, int, int, int **, int **, int **);

int main(void){

    int i, j, a, b, n, t;
    int **A, **B, **sum;
    FILE *input;

    // Input file
    input=fopen("Input_file", "r");
    if(input==NULL){
        printf("File error.\n");
        exit(1);
    }

    // We initialize data
    fscanf(input, "%d %d", &a, &n);
    initialize(a, n, &A, &B, &sum, input);

    b=a;
    printf("%4s%8s\n", "t", "Phi(t)");
    printf(" ---------\n");
    printf("%4d%8d\n", 1, a);

    // We start computing tA inductively
    // A[][] will keep A and B[][] will keep (t-1)A
    for(t=2; t<=10; ++t){

        // sum <-- A+B, where B is in fact (t-1)A
        b=sumset(a,b,n,A,B,sum);
        printf("%4d%8d\n", t, b);

        for(i=0; i<500; ++i) for(j=0; j<n; ++j) B[i][j]=sum[i][j];

    }

    for(i=0; i<a; ++i) free(A[i]);
    for(i=0; i<500; ++i){
        free(B[i]);
```

```
        free(sum[i]);
    }
    free(A);
    free(B);
    free(sum);

    return 0;
}

void initialize(int a, int n, int ***A, int ***B, int ***sum, FILE *input){

    int i, j;

    *A=(int **)malloc(a*sizeof(int *));
    if(*A==NULL){
        printf("Memory error.\n");
        exit(1);
    }
    for(i=0; i<a; ++i){
        (*A)[i]=(int *)malloc(n*sizeof(int));
        if((*A)[i]==NULL){
            printf("Memory error.\n");
            exit(1);
        }
    }

    *B=(int **)malloc(500*sizeof(int *));
    if(*B==NULL){
        printf("Memory error.\n");
        exit(1);
    }
    for(i=0; i<500; ++i){
        (*B)[i]=(int *)malloc(n*sizeof(int));
        if((*B)[i]==NULL){
            printf("Memory error.\n");
            exit(1);
        }
    }

    *sum=(int **)malloc(500*sizeof(int *));
    if(*sum==NULL){
        printf("Memory error.\n");
        exit(1);
    }
```

```
    for(i=0; i<500; ++i){
        (*sum)[i]=(int *)malloc(n*sizeof(int));
        if((*sum)[i]==NULL){
            printf("Memory error.\n");
            exit(1);
        }
    }

    // We scan A
    for(i=0; i<a; ++i) for(j=0; j<n; ++j){
        fscanf(input, "%d", &(*A)[i][j]);
        (*B)[i][j]=(*A)[i][j];
    }

}

// We compute |A+B|
int sumset(int a, int b, int n, int **A, int **B, int **sum){

    int i, j, k, r, s, cont=0;

    for(i=0; i<a; ++i) for(j=0; j<b; ++j){
        for(k=0; k<n; ++k) sum[cont][k]=A[i][k]+B[j][k];
        for(r=0; r<cont; ++r){
            for(s=0; s<n; ++s) if(sum[r][s]!=sum[cont][s]) break;
            if(s==n) break;
        }
        if(r==cont) ++cont;
    }

    return cont;
}
```

Example 3.1.3 (Computation of sumsets)**.**

(a) Consider the input

```
5 1

1
2
3
4
5
```

(which means $A = \{1, 2, 3, 4, 5\}$). We get

```
 t  Phi(t)
---------
 1       5
 2       9
 3      13
 4      17
 5      21
 6      25
 7      29
 8      33
 9      37
10      41
```

According to what we wrote before, the values obtained are the images of a polynomial $p_A \in \mathbb{Q}[t]$ if t is big enough. In this case, $p_A(t) = 4t + 1$. t_0 turns out to be 0, namely, φ_A and p_A coincide for all $t \geq 0$.

(b) If the program receives the input

```
4 2

0 0
2 0
2 2
0 1
```

(which means $A = \{(0, 0), (2, 0), \dots\}$), we get

```
 t  Phi(t)
---------
 1       4
 2      10
 3      19
 4      31
 5      46
 6      64
 7      85
 8     109
 9     136
10     166
```

These values correspond to the image of $\frac{3}{2}t^2 + \frac{3}{2}t + 1$ for all $t \geq 0$. Now, we can slightly change the input data of this example so that we realise that small changes in the set A can turn into huge changes in the final polynomial.

(c) If the program receives the input

```
4 2

0 0
2 0
2 1
0 1
```

we get

```
 t  Phi(t)
---------
 1       4
 2       9
 3      16
 4      25
 5      36
 6      49
 7      64
 8      81
 9     100
10     121
```

and the polynomial, in this case, is $t^2 + 2t + 1$. t_0 is also 0.

(d) If the program receives the input

```
4 2

0 0
3 0
2 2
0 1
```

we get the values

```
 t  Phi(t)
---------
 1       4
 2      10
 3      20
 4      35
 5      56
 6      84
```

```
 7     120
 8     164
 9     216
10     276
```

which correspond to the image of the polynomial $4t^2 - 16t + 36$. In this case, t_0 is 5.

(e) The input

```
6 6

8 8 8 2 6 9
4 0 3 4 7 3
8 1 5 0 8 2
0 3 4 1 9 5
4 2 8 9 4 8
1 8 1 1 4 3
```

generates the values

```
t  Phi(t)
---------
1       6
2      21
3      56
4     126
5     252
6     462
```

and these correspond to the image of the polynomial $\frac{1}{120}t^5 + \frac{1}{8}t^4 + \frac{17}{24}t^3 + \frac{15}{8}t^2 + \frac{137}{60}t + 1$. t_0 is 0.

3.2 Sumsets and projections of Veronese varieties

The goal of this section is to establish a connection between the cardinality of sumsets and geometry. If we do not say otherwise, A will be a finite subset of $\mathbb{Z}^n$. The idea here is to find a suitable monomial projection $Y_{n,d}$ of a Veronese variety $V_{n,d}$ whose Hilbert function models φ_A. We will therefore conclude that φ_A is asymptotically a polynomial $p_A(t) \in \mathbb{Q}[t]$ of degree $\dim Y_{n,d}$.

Definition 3.2.1. We set $d_A = \max\{\sum_{i=1}^n a_i : a = (a_i)_i \in A\}$ and we define

$$\Omega_{n,d_A} = \{x_0^{d_A - a_1 - \cdots - a_n} x_1^{a_1} \cdots x_n^{a_n} : a = (a_1, \ldots, a_n) \in A\} = \{m_1, \ldots, m_{|A|}\},$$

a set of monomials of degree d_A in $k[x_0, \ldots, x_n]$. Y_{n,d_A} will be the closure of the image of the parametrization

$$\begin{aligned} \mathbb{P}^n &\to \mathbb{P}^{|A|-1} \\ [x_0, \ldots, x_n] &\mapsto [m_1, \ldots, m_{|A|}], \end{aligned}$$

which, as we know, is a monomial projection of the Veronese variety V_{n,d_A}.

Remark 3.2.2. Consider the translation $\tau_A : \mathbb{Z}^n \to \mathbb{Z}^n$, defined by $x = (x_1, \ldots, x_n) \mapsto x^* = (x_1 - \delta_1, \ldots, x_n - \delta_n)$, where $\delta_i = \min\{a_i : a = (a_1, \ldots, a_n) \in A\}$. This translation verifies $\tau_A(A) \subset \mathbb{Z}^n_{\geq 0}$ and also $\mathrm{GCD}(m \in \Omega_{n,d_{\tau_A(A)}}) = 1$; it is, in fact, the only translation verifying these two conditions. Since the cardinality of a sumset is invariant under translations, we can assume w.l.o.g. that $A \subset \mathbb{Z}^n_{\geq 0}$ and $\mathrm{GCD}(m \in \Omega_{n,d_A}) = 1$.

With this in mind, we now take the new variables $\omega_1, \ldots, \omega_{|A|}$. The map

$$\rho : k[\omega_1, \ldots, \omega_{|A|}] \to k[m_1, \ldots, m_{|A|}],$$

defined by

$$p(\omega_1, \ldots, \omega_{|A|}) \mapsto p(m_1, \ldots, m_{|A|}),$$

is a surjective morphism whose kernel is precisely the ideal $I(Y_{n,d_A})$. So we get that

$$k[\omega_1, \ldots, \omega_{|A|}]/I(Y_{n,d_A}) \cong k[m_1, \ldots, m_{|A|}],$$

and this leads to

$$F_{Y_{n,d_A}}(t) = \dim k[\omega_1, \ldots, \omega_{|A|}]_t / I(Y_{n,d_A})_t = \dim k[m_1, \ldots, m_{|A|}]_{td_A}.$$

We can now devote some time to think about what $\dim k[m_1, \ldots, m_{|A|}]_{td_A}$ is equal to. When $t = 1$, we get the k-vector space $k[m_1, \ldots, m_{|A|}]_{d_A}$. This is clearly spanned by the set

$$\{m_i : 1 \leq i \leq |A|\} = \{x_0^{d_A - a_1 - \cdots - a_n} x_1^{a_1} \cdots x_n^{a_n} : a = (a_1, \ldots, a_n) \in A\},$$

so the dimension has to be $|A|$. When $t = 2$, the k-vector space is now spanned by

$$\{m_i m_j : 1 \leq i, j \leq |A|\} = \{x_0^{2d_A - \sum(a_i + b_i)} x_1^{a_1 + b_1} \cdots x_n^{a_n + b_n} : a, b \in A\},$$

so the dimension is simply the resulting number of monomials when deleting the repeated ones, namely, $|2A|$. This applies for the rest of the cases. In the end, we get that the Hilbert function of Y_{n,d_A} models the values $|tA|$, as desired, and this immediately means that $|tA|$ behaves asymptotically as a polynomial of degree at most n.

Since Y_{n,d_A} is a monomial projection of the n-dimensional Veronese variety V_{n,d_A}, its dimension is bounded by n and its degree by d_A^n. However, both the dimension and the degree of the variety Y_{n,d_A} could decrease (check [5] for some examples), so from now onward we are going to restrict our attention to finite subsets $A \subset \mathbb{Z}^n_{\geq 0}$ associated with n-dimensional monomial projections Y_{n,d_A} of V_{n,d_A}. Assuming this hypothesis we can find the Hilbert polynomial associated to A in two specific cases:

Proposition 3.2.3. *Let $A \subset \mathbb{Z}^n_{\geq 0}$ be a finite set associated by n-dimensional projective variety Y_{n,d_A} of degree d.*

(a) If $|A| = n+1$, then

$$\varphi_A(t) = \binom{t+n}{n} \text{ for all } t \geq 0.$$

(b) If $|A| = n+2$, then

$$\varphi_A(t) = \begin{cases} \binom{t+n+1}{n+1} & \text{if } 0 \leq t < d \\ \binom{t+n+1}{n+1} - \binom{t-d+n+1}{n+1} & \text{if } t \geq d \end{cases}$$

In particular, $t_0 \leq d$.

Proof.

(a) As we know, A induces a rational map $\mathbb{P}^n \dashrightarrow \mathbb{P}^n$, and the closure of its image, Y_{n,d_A}, is a subvariety of $\mathbb{P}^n$ of dimension n. This means that $Y_{n,d_A} = \mathbb{P}^n$ and

$$\varphi_A(t) = \binom{t+n}{n}$$

for all $t \geq 0$.

(b) In this case, A defines a rational map $\mathbb{P}^n \dashrightarrow \mathbb{P}^{n+1}$ and the closure of its image, Y_{n,d_A}, is a hypersurface of degree d of $\mathbb{P}^{n+1}$. The exact sequence

$$0 \to S(-d) \to S \to S/I(Y_{n,d_A}) \to 0,$$

where $S = k[w_0, \ldots, w_{n+1}]$, proves the claim.

□

Determining the function $\varphi_A(t)$, the coefficients of the polynomial $p_A(t)$ and the phase transition t_0 for arbitrary finite subsets $A \subset \mathbb{Z}^n$ with more than $n+2$ elements is out of reach.

Appendix A

Scripts of Macaulay2

(a) Example 1.5.5 (b).

```
i1 : R=QQ[x..z]
o1 = R
o1 : PolynomialRing

i2 : I = ideal (x^2*y, x*y*z^3, y*z^2, x*y^2)
o2 = ideal (x^2y, xyz^3, yz^2, xy^2)
o2 : Ideal of R

i3 : C = res I
o3 = R^1  <-- R^3  <-- R^3  <-- R^1  <-- 0
     0        1        2        3        4
o3 : ChainComplex

i4 : C_2
o4 = R^3
o4 : R-module, free, degrees {4..5,5}

i5 : C.dd_2
     {3} | -y -z^2    0 |
o5 = {3} |  x    0 -z^2 |
     {3} |  0  x^2   xy |
o5 : Matrix R^3  <--- R^3
```

(b) Example 2.2.9 (a).

```
i1 : R=QQ[x,y,z,t]
o1 = R
o1 : PolynomialRing

i2 : I = ideal (x*z-y^2,x*t-y*z,y*t-z^2)
```

```
o2 = ideal (-y^2+xz,-yz+xt,-z^2+yt)
o2 : Ideal of R

i3 : M = module R/I
o3 = cokernel (-y^2+xz  -yz+xt  -z^2+yt)
o3 : R-module, quotient of R

i4 : hilbertPolynomial(M, Projective=>false)
o4 = 3i+1
o4 : Q[i]
```

(c) Example 2.4.4.

```
i1 : R = QQ[x,y,z,t];

i2 : S = QQ[s,t];

i3 : F = map(S,R,{s^3,s^2*t, s*t^2, t^3})
o3 = map (S,R,{s^3,s^2t, st^2, t^3})
o3 : RingMap S <-- R

i4 : I = ker F
o4 = ideal(z^2-yt,yz-xt,y^2-xz)
o4 : Ideal of R

i5 : M = module R/I
o5 = cokernel(z^2-yt,yz-xt,y^2-xz)
o5 : R-module, quotient of R

i7 : C = res M
o7 = R^1  <-- R^3  <-- R^2  <-- 0
     0        1        2        3
o7 : ChainComplex
```

(d) Example 2.4.5.

```
i1 : R = QQ[x_0..x_9];

i2 : S = QQ[y_0..y_2];

i3 : F = map(S,R,{y_0^3,y_1^3,y_2^3,y_0^2*y_1,y_0^2*y_2,y_0*y_1^2,
     y_0*y_2^2,y_1^2*y_2,y_1*y_2^2,y_0*y_1*y_2})
o3 = map (S,R,{y_0^3,y_1^3,y_2^3,y_0^2y_1,y_0^2y_2,y_0y_1^2,
     y_0y_2^2,y_1^2y_2,y_1y_2^2,y_0y_1y_2})
o3 : RingMap S <-- R
```

```
i4 : I = ker F
o4 = ideal( ... )
o4 : Ideal of R

i5 : M = module R/I
o5 = cokernel( ... )
o5 : R-module, quotient of R

i7 : C = res M
o7 = R^1<-R^27<-R^105<-R^189<-R^189<-R^105<-R^27<-R^1<-0
     0    1     2      3      4      5      6     7    8
o7 : ChainComplex
```

(e) Example 2.5.1 (a).

```
i1 : R = QQ[x..z];

i2 : S = QQ[s,t];

i3 : F = map(S,R,{s^2*t, s*t^2, t^3})
o3 = map (S,R,{s^2t, st^2, t^3})
o3 : RingMap S <-- R

i4 : I = ker F
o4 = ideal(y^2-xz)
o4 : Ideal of R

i5 : M = module R/I
o5 = cokernel(y^2-xz)
o5 : R-module, quotient of R

i6 : hilbertPolynomial(M,Projective=>false)
o6 = 2i+1
o6 : Q[i]
```

(f) Example 2.5.3 (a).

```
i1 : R = QQ[x..z];

i2 : S = QQ[s,t];

i3 : res ker map(S,R,{s^2*t, s*t^2, t^3})
o3 = R^1 <-- R^1 <-- 0
```

```
      0      1      2
o3 : ChainComplex
```

Bibliography

[1] E. Arrondo, *Introduction to projective varieties* (2017).

[2] S. Bosch, *Algebraic geometry and commutative algebra*, Graduate Texts in Mathematics, Springer, (2013).

[3] W. Bruns and J. Herzog, *Cohen-Macaulay rings*, Cambridge studies in advanced mathematics, vol. 39, (1993).

[4] E. Clader, *Hilbert polynomials and the degree of a projective variety*.

[5] L. Colarte, J. Elias and R. M. Miró-Roig, *Sumsets and Veronese varieties*.

[6] A. Gathmann, *Commutative algebra*, Class Notes TU Kaiserslautern (2013).

[7] W. Gröbner, *Über Veronesische Varietäten und deren Projektionen*, (1990). Arch. Math., 16 (1965), 257-264.

[8] J. Harris, *Algebraic Geometry: a first course*, Graduate Texts in Mathematics, vol. 133, Springer, (1992).

[9] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, vol. 52, Springer, (1977).

[10] L. T. Hoa of Hanoi, *Classification of the Triple Projections of Veronese Varieties*, Math. Nachr. 128 (1980) 185-197.

[11] A. G. Khovanskii, *Newton polyhedron, Hilbert polynomial, and sums of finite sets*. Funct. Anal. Its Appl. 26 (1992), 276-281.

[12] R. M. Miró Roig, *Determinantal ideals* (2009).

[13] R. M. Miró Roig, *Lectures on the representation type of a projective variety*, Lectures at the Vietnam Institute for Advanced Study in Mathematics (Hanoi), (2014).

[14] C. McAuley, *On the minimal free resolution of a monomial ideal*, (2012).

[15] C. Peskine, *Introduction algébrique à la géometrie projective*, (1990).

[16] B. Renschuch, *Zur Klassifizierung Veronesescher Projektionsideale*, Math. Nachr., 67 (1975), 35-40.

[17] B. Renschuch, *Beitrage zur konstruktiven Theorie der Polynomideale* VII, VIII, XIV, Wiss. Zeit. Pad. Hochsch. "Karl Liebnecht" Potsdam, 19 (1975), 101-106, and 21 (1977), 159- 173.

[18] P. Schenzel, *On Veronesean embedding and projections of Veronesean varieties*, Arch. Math. 80 (1978), 391-397.

[19] J. Sidman and P. Vermeire, *Equations defining secant varieties: geometry and computation*, (2011).

[20] N. V. Trung, *Classification of the double projections of Veronese varieties*, J. Math. Kyoto Univ. 22-4 (1983), 567-581.

[21] N. V. Trung, *On projections of one-dimensional Veronese varieties*, Math. Nachr. 118 (1984), 47-67.

[22] R. Wiegand, *What is... a syzygy?*, Notices of the AMS, vol. 53, n. 4., (2006), 456-457.