CENTER FOR RESEARCH AND ADVANCED STUDIES
OF THE NATIONAL POLYTHECHNIC INSTITUTE

CAMPUS ZACATENCO

DEPARTMENT OF MATHEMATICS

Numerical Functions of Graded Ideals, Edge-Ideals of Digraphs and their Applications to Coding Theory

Dissertation submitted by

Carlos Eduardo Vivares Parra

to obtain the Degree of

DOCTOR OF SCIENCE

IN THE SPECIALITY OF

MATHEMATICS

Thesis Advisor: Dr. Rafael Heraclio Villarreal Rodríguez

Mexico City February, 2019

CENTRO DE INVESTIGACIÓN Y DE ESTUDIOS
AVANZADOS DEL INSTITUTO POLITÉCNICO NACIONAL

UNIDAD ZACATENCO

DEPARTAMENTO DE MATEMÁTICAS

Funciones Numéricas de Ideales Graduados, Ideales de Aristas de Digráficas y sus Aplicaciones a la Teoría de Códigos.

Tesis que presenta

Carlos Eduardo Vivares Parra

para obtener el grado de

DOCTOR EN CIENCIAS

EN LA ESPECIALIDAD DE

MATEMÁTICAS

Asesor de Tesis: Dr. Rafael Heraclio Villarreal Rodríguez

Ciudad de México Febrero, 2019

Contents

Abstract

In the first part we introduce the fundamental tools of commutative algebra and algebraic geometry needed for the study of the coding theory. Combining these tools with combinatorics we obtain formulas for the most important parameter of a code, the minimum distance.

Next we study monomial ideals, Gröbner bases and the footprint of an ideal, projective closures, vanishing ideals, and Hilbert functions. The role of Hilbert functions and vanishing ideals in affine and projective varieties is discussed here. The number of zeros that a homogeneous polynomial has in any given finite set of points in an affine or projective space is expressed in terms of vanishing ideals and the notion of degree. Also we study the families of projective and affine Reed–Muller-type codes and their connection to vanishing ideals and Hilbert functions.

In the chapter 4, we explore the r-th generalized minimum distance function (gmd function for short) and the corresponding generalized footprint function of a graded ideal in a polynomial ring over a field. If $\mathbb{X}$ is a set of projective points over a finite field and $I(\mathbb{X})$ is its vanishing ideal, we show that the gmd function and the Vasconcelos function of $I(\mathbb{X})$ are equal to the r-th generalized Hamming weight of the corresponding Reed-Muller-type code $C_{\mathbb{X}}(d)$. We show that the r-th generalized footprint function of $I(\mathbb{X})$ is a lower bound for the r-th generalized Hamming weight of $C_{\mathbb{X}}(d)$. As an application to coding theory we show an explicit formula and a combinatorial formula for the second generalized Hamming weight of an affine cartesian code.

In the chapter 5, we give an effective characterization of the Cohen–Macaulay vertex-weighted oriented trees and forests. For transitive weighted oriented graphs we show that Alexander duality holds. It is shown that edge ideals of weighted acyclic tournaments are Cohen–Macaulay and satisfy Alexander duality. For a monomial ideal with no embedded primes we classify the normality of its symbolic Rees algebra in terms of the normality of its primary components.

Finally in Chapter 6, we use polarization to study the behavior of the depth and regularity of a monomial ideal I, locally at a variable x_i, when we lower the degree of all the

highest powers of the variable x_i occurring in the minimal generating set of I, and examine the depth and regularity of powers of edge ideals of clutters using combinatorial optimization techniques. If I is the edge ideal of an unmixed clutter with the max-flow min-cut property, we show that the powers of I have non-increasing depth and non-decreasing regularity. As a consequence edge ideals of unmixed bipartite graphs have non-increasing depth. We are able to show that the symbolic powers of the ideal of covers of the clique clutter of a strongly perfect graph have non-increasing depth. A similar result holds for the ideal of covers of a uniform ideal clutter.

Resumen

En la primera parte introducimos las herramientas fundamentales del álgebra conmutativa y geometría algebraica necesarias para el estudio de la teoría de Códigos. Combinando estas herramientas con combinatoria obtenemos fórmulas para el parámetro más importante de un código, la mínima la distancia. A continuación estudiamos los ideales monomiales, las bases de Gröbner y la huella de un ideal, la clausura proyectiva, ideales de anulación, y funciones de Hilbert. El número de ceros que un polinomio homogéneo tiene en cualquier conjunto finito de puntos en un espacio afín o proyectivo se expresa en términos de ideales de anulación y la noción de grado. También estudiamos las familias de códigos proyectivos y afines de tipo Reed-Muller y su conexión. con los ideales de anulación y las funciones de Hilbert. En el capítulo 4, exploramos la r-ésima función de mínima distancia generalizada (función gmd para abreviar) y la correspondiente función de huella generalizada de un ideal graduado en un anillo polinomial sobre un campo. Si $\mathbb{X}$ es un conjunto puntos proyectivos sobre un campo finito, $I(\mathbb{X})$ su ideal de anulación, demostramos que la función gmd y la función de Vasconcelos de $I(\mathbb{X})$ son iguales al r-ésimo peso de Hamming generalizado del correspondiente código de tipo Reed-Muller $C_{\mathbb{X}}(d)$. Mostramos que la r-ésima función huella generalizada de $I(\mathbb{X})$ es un límite inferior para el r-ésimo peso de Hamming generalizado de $C_{\mathbb{X}}(d)$. Como una aplicación para la teoría de códigos mostramos una fórmula explícita y una fórmula combinatoria para el segundo peso generalizado de Hamming de un código cartesiano afín. En el capítulo 5, damos una caracterización efectiva de los árboles y bosques orientados con peso Cohen-Macaulay. Para los gráficos orientados con peso mostramos que la dualidad de Alexander se tiene. Finalmente en el Capítulo 6, usamos la polarización para estudiar el comportamiento de la profundidad y la regularidad de un ideal monomial I, localmente en una variable x_i, cuando bajamos el grado de todas las potencias más altas de la variable x_i que está en el conjunto mínimo generador de I, y examinamos la profundidad y la regularidad de las potencias ideales de aristas de hipergráficas utilizando técnicas combinatoria. Si un ideal de aristas de una hipergráfica no mezclada con la propiedad min-cut max-flow,

demostramos que las potencias de I tienen profundidad no creciente y regularidad no decreciente. Como consecuencia, los ideales de aristas de gráficas bipartitas no mezcladas tienen profundidad no decreciente.

Introduction

This thesis studies certain numerical functions coming from graded ideals (e.g., generalized minimum distance functions, regularity and depth) and certain algebraic properties of graded ideals and their symbolic and ordinary powers (e.g., Complete intersection, Cohen-Macaulay, normality, unmixed, non-increasing depth, non-decreasing regularity). We also study the irreducible decomposition of a monomial ideal and the algebraic properties of edge ideals of oriented graphs.

This work begins the study of the generalized minimum distance function—a general numerical function of a graded ideals—of which the r-th generalized Hamming weight of a Reed-Muller type code is the simplest, but also the typical case. This is naturally connected to coding theory and to algebraic geometry over finite fields, i.e., to projective varieties and vanishing ideals over finite fields.

The connection of the r-th generalized minimum distance function to coding theory comes from the observation that for vanishing ideals over finite fields and $r = 1$, this function is the minimum distance of the corresponding Reed-Muller type code. Coding theory is the study of error-correcting codes and their associated mathematics. An error-correcting code is used to encode information that will be transmitted through a noisy communication channel, in such a way that the original message can be recovered even though errors have occurred during the process. In a few words, the information to be sent turns into a binary string, then it is transmitted through a telephone, radio, satellite, etc., and when it reaches its destination the binary string may not have the same digits, because of human errors, electronic failures, weather, etc. An algorithm should be able to detect the errors and thus recover the original message. The determination of the minimum distance is essential to find good error-correcting codes [**HVLP98, BHHW98, MS77, TV13, Wal00**].

The motivation to study edge ideals of oriented graphs comes from the fact that initial ideals of vanishing ideals of projective spaces over finite fields are of this type [**Sor91**]. This can be then used to study the basic parameters of the corresponding evaluation code not only for projective space but also for nested carteasian codes [**CNL17**].

In what follows we introduce our main results and introduce some terminology and notation. In Chapter 1 we introduce primary decompositions of modules and ideals,

Hilbert series of graded modules, Cohen-Macaulay rings, and Artinian rings. The Hilbert theorem for graded modules is introduced here along with the algebraic invariants and properties of graded modules and ideals. In Chapter 2 we study monomial ideals, Gröbner bases and the footprint of an ideal, projective closures, vanishing ideals, and Hilbert functions. The role of Hilbert funtions and vanishing ideals in affine an projective varieties is discussed here. The number of zeros that a homogeneous polynomial has in any given finite set of points in an affine or projective space is expressed in terms of vanishing ideals and the notion of degree. The contents of Chapter 3 are as follows. We study the families of projective and affine Reed-Muller-type codes and their connection to vanishing ideals and Hilbert functions. Also, we show a finite version of Hilbert Nullstellensatz.

The contents of chapter 4 are as follows. Let $S = K[t_1, \ldots, t_s] = \oplus_{d=0}^{\infty} S_d$ be a polynomial ring over a field K with the standard grading and let $I \neq (0)$ be a graded ideal of S. In this thesis we extend the scope of **[MBPV17]** by considering generalized footprint and minimum distance functions. Let $\mathcal{F}_{d,r}$ be the set:

$$\mathcal{F}_{d,r} := \{\, \{f_1, \ldots, f_r\} \subset S_d \,|\, \overline{f}_1, \ldots, \overline{f}_r \text{ are linearly independent over } K, (I\colon (f_1, \ldots, f_r)) \neq I\},$$

where $\overline{f} = f + I$ is the class of f modulo I, and $(I\colon J) = \{h \in S | \, hJ \subset I\}$ is referred as a quotient ideal or a colon ideal.

We denote the *degree* of S/I by $\deg(S/I)$. The function $\delta_I\colon \mathbb{N}_+ \times \mathbb{N}_+ \to \mathbb{Z}$ given by

$$\delta_I(d,r) := \begin{cases} \deg(S/I) - \max\{\deg(S/(I,F)) | \, F \in \mathcal{F}_{d,r}\} & \text{if } \mathcal{F}_{d,r} \neq \emptyset, \\ \deg(S/I) & \text{if } \mathcal{F}_{d,r} = \emptyset. \end{cases}$$

is called the r-th *generalized minimum distance function* of I of degree d, or simply the r-th *gmd function* of I of degree d. To compute $\delta_I(d,r)$ is a difficult problem. For a certain family of ideals we will give lower bounds for $\delta_I(d,r)$ which are easier to compute.

Fix a monomial order $\prec$ on S. Let $\text{in}_\prec(I)$ be the initial ideal of I and let $\Delta_\prec(I)$ be the *footprint* of S/I consisting of all the *standard monomials* of S/I with respect to $\prec$. Given $d, r \geq 1$, let $\mathcal{M}_{\prec,d,r}$ be the set of all subsets M of $\Delta_\prec(I)_d = \Delta_\prec(I) \cap S_d$ with r distinct elements such that $(\text{in}_\prec(I)\colon (M)) \neq \text{in}_\prec(I)$. The *generalized footprint function* of I, denoted fp_I, is the function $\text{fp}_I\colon \mathbb{N}_+ \times \mathbb{N}_+ \to \mathbb{Z}$ given by

$$\text{fp}_I(d,r) := \begin{cases} \deg(S/I) - \max\{\deg(S/(\text{in}_\prec(I), M)) \,|\, M \in \mathcal{M}_{\prec,d,r}\} & \text{if } \mathcal{M}_{\prec,d,r} \neq \emptyset, \\ \deg(S/I) & \text{if } \mathcal{M}_{\prec,d,r} = \emptyset. \end{cases}$$

The definition of $\delta_I(d,r)$ was motivated by the notion of generalized Hamming weight of a linear code **[HKM77, Wei91]**. For convenience we recall this notion. Let $K=\mathbb{F}_q$ be a finite field and let C be a $[m,k]$ *linear code* of *length* m and *dimension* k, that is, C is a linear subspace of K^m with $k=\dim_K(C)$. Given a subcode D of C (that is, D is a linear subspace of C), the *support* of D, denoted $\chi(D)$, is the set of non-zero positions of D, that is,

$$\chi(D):=\{i\,|\,\exists\,(a_1,\ldots,a_m)\in D,\,a_i\neq 0\}.$$

The r-th *generalized Hamming weight* of C, denoted $\delta_r(C)$, is the size of the smallest support of an r-dimensional subcode. Generalized Hamming weights have received a lot of attention; see **[Car13, DG17, Gei08, SW03, Wei91, WY93]** and the references therein. The study of these weights is related to trellis coding, t–resilient functions, and was motivated by some applications from cryptography **[Wei91]**.

The minimum distance of projective Reed-Muller-type codes has been studied using Gröbner bases techniques; see **[Car13, Gei08, GT13, MBPV17]** and the references therein. In this work we extend these techniques to study the r-th generalized Hamming weights of projective Reed-Muller-type codes, a special type of linear codes that generalizes affine Reed-Muller-type codes **[LSPV12]**. These projective codes are constructed as follows.

Let $K=\mathbb{F}_q$ be a finite field with q elements, let $\mathbb{P}^{s-1}$ be a projective space over K, and let $\mathbb{X}$ be a subset of $\mathbb{P}^{s-1}$. The *vanishing ideal* of $\mathbb{X}$, denoted $I(\mathbb{X})$, is the ideal of S generated by the homogeneous polynomials that vanish at all points of $\mathbb{X}$. The Hilbert function of $S/I(\mathbb{X})$ is denoted by $H_{\mathbb{X}}(d)$. We can write $\mathbb{X}=\{[P_1],\ldots,[P_m]\}\subset\mathbb{P}^{s-1}$ with $m=|\mathbb{X}|$. Here we assume that the first non-zero entry of each $[P_i]$ is 1. In the special case that $\mathbb{X}$ has the form $[X\times\{1\}]$ for some $X\subset\mathbb{F}_q^{s-1}$, we assume that the s-th entry of each $[P_i]$ is 1.

Fix a degree $d\geq 1$. There is a K-linear map given by

$$\mathrm{ev}_d\colon S_d\to K^m,\quad f\mapsto(f(P_1),\ldots,f(P_m))\,.$$

The image of S_d under ev_d, denoted by $C_{\mathbb{X}}(d)$, is called a *projective Reed-Muller-type code* of degree d on $\mathbb{X}$ **[DRTR01, GSRTR02]**. The *parameters* of the linear code $C_{\mathbb{X}}(d)$ are:

(a) *length*: $|\mathbb{X}|$,
(b) *dimension*: $\dim_K C_{\mathbb{X}}(d)$,
(c) r-th *generalized Hamming weight*: $\delta_{\mathbb{X}}(d,r):=\delta_r(C_{\mathbb{X}}(d))$.

If $\mathbb{X}$ is a finite set of projective points over a finite field and $I(\mathbb{X})$ is its vanishing ideal, we show that $\delta_{I(\mathbb{X})}(d,r)$ is the r-th generalized Hamming weight $\delta_{\mathbb{X}}(d,r)$ of the corresponding Reed-Muller-type code $C_{\mathbb{X}}(d)$ (Theorem 4.18). We introduce the *Vasconcelos* function $\vartheta_I(d,r)$ of a graded ideal I (Definition 4.17) and show that this function is also equal to $\delta_{\mathbb{X}}(d,r)$ (Theorem 4.18). These abstract algebraic formulations gives us a new tool

to study generalized Hamming weights in a systematic manner. One of our results shows that the r-th generalized footprint function of $I(\mathbb{X})$ is a lower bound for $\delta_{\mathbb{X}}(d,r)$ (Theorem 4.23). As is seen in this Chapter, in certain cases the generalized footprint function gives the exact value of $\delta_{\mathbb{X}}(d,r)$.

We give two applications to coding theory. The first is the following explicit formula for the second generalized Hamming weight of an affine cartesian code.

Theorem 4.32 Let A_i, $i = 1,\ldots,s-1$, be subsets of $\mathbb{F}_q$ and let $\mathbb{X} \subset \mathbb{P}^{s-1}$ be the projective set $\mathbb{X} = [A_1 \times \cdots \times A_{s-1} \times \{1\}]$. If $d_i = |A_i|$ for $i = 1,\ldots,s-1$ and $2 \leq d_1 \leq \cdots \leq d_{s-1}$, then

$$\delta_{\mathbb{X}}(d,2) = \begin{cases} (d_{k+1} - \ell + 1)\, d_{k+2} \cdots d_{s-1} - d_{k+3} \cdots d_{s-1} & \text{if } k < s-3, \\ (d_{k+1} - \ell + 1)\, d_{k+2} \cdots d_{s-1} - 1 & \text{if } k = s-3, \\ d_{s-1} - \ell + 1 & \text{if } k = s-2, \end{cases}$$

where $0 \leq k \leq s-2$ and ℓ are integers, $d = \sum_{i=1}^{k} (d_i - 1) + \ell$, and $1 \leq \ell \leq d_{k+1} - 1$.

Using this result one can recover the case when $\mathbb{X}$ is a projective torus in $\mathbb{P}^{s-1}$ [**SCSV18**, Theorem 17]. The second application of this Chapter gives a combinatorial formula for the second generalized Hamming weight of an affine cartesian code, which is quite different from the corresponding formula of [**BD17**, Theorem 5.4].

Theorem 4.33 Let $\mathcal{P}_d$ be the set of all pairs (a,b), a, b in $\mathbb{N}^s$, $a = (a_i)$, $b = (b_i)$, such that $a \neq b$, $d = \sum_i a_i = \sum_i b_i$, $1 \leq a_i, b_i \leq d_i - 1$ for $i = 1,\ldots,n$, $n := s-1$, $a_i \neq 0$ and $b_j \neq 0$ for some $1 \leq i, j \leq n$. If $\mathbb{X} = [A_1 \times \cdots \times A_n \times \{1\}]$, with $A_i \subset \mathbb{F}_q$, $d_i = |A_i|$, and $2 \leq d_1 \leq \cdots \leq d_n$, then

$$\mathrm{fp}_{I(\mathbb{X})}(d,2) = \delta_{\mathbb{X}}(d,2) = \min\{P(a,b) |\, (a,b) \in \mathcal{P}_d\} \quad \text{for } \ d \leq \textstyle\sum_{i=1}^{n}(d_i - 1),$$

where $P(a,b) = \prod_{i=1}^{n}(d_i - a_i) + \prod_{i=1}^{n}(d_i - b_i) - \prod_{i=1}^{n} \min\{d_i - a_i, d_i - b_i\}$.

Let $\psi(d)$ be the formula for $\delta_{\mathbb{X}}(d,2)$ given in Theorem 4.32. Then

$$\psi(d) = \min\{P(a,b) |\, (a,b) \in \mathcal{P}_d\}$$

for $d \leq \sum_{i=1}^{n}(d_i - 1)$. This equality is interesting in its own right.

We also prove a related inequality which is of independent interest:

Proposition 4.28 Let $d \geq 1$ and $1 \leq e_1 \leq \cdots \leq e_m$ be integers. Suppose $1 \leq a_i \leq e_i$ and $1 \leq b_i \leq e_i$, for $i = 1,\ldots,m$, are integers such that $d = \sum_i a_i = \sum_i b_i$ and $a \neq b$. Then

$$\pi(a,b) \geq \left(\sum_{i=1}^{m} a_i - \sum_{i=k+1}^{m} e_i - (k-2) \right) e_{k+1} \cdots e_m - e_{k+2} \cdots e_m$$

for $k = 1,\ldots,m-1$, where $\pi(a,b) = \prod_i a_i + \prod_i b_i - \prod_i \min(a_i, b_i)$.

There is a nice combinatorial expression for the r-th generalized Hamming weight of an affine cartesian code [**BD17**, Theorem 5.4]. Using this result we give an explicit formula to compute the r-th generalized Hamming weight for a family of cartesian codes (Theorem 4.34).

For additional information we refer to [**BH98, CLO07, Eis13**] (for the theory of Gröbner bases, commutative algebra, and Hilbert functions), and [**MS77, TV13**] (for the theory of error-correcting codes and linear codes).

Let us describe the contents of Chapter 5. Consider a polynomial ring over a field K, $R = K[x_1, \ldots, x_n]$. Let $I \subset R$ be a monomial ideal. The *Rees algebra* of I is

$$R[It] := R \oplus It \oplus \cdots \oplus I^k t^k \oplus \cdots \subset R[t],$$

where t is a new variable, and the *symbolic Rees algebra* of I is

$$R_s(I) := R \oplus I^{(1)} t \oplus \cdots \oplus I^{(k)} t^k \oplus \cdots \subset R[t],$$

where $I^{(k)}$ is the k-th symbolic power of I (see Definitions 1.62 and 6.27).

One of the early works on symbolic powers of monomial ideal is [**MBRV11**]. Symbolic powers of ideals and edge ideals of graphs where studied in [**Bah04**]. A method to compute symbolic powers of radical ideals in characteristic zero is given in [**Sim96**].

In Section 5.1 we recall the notion of irreducible decomposition of a monomial ideal and prove that the exponents of the variables that occur in the minimal generating set of a monomial ideal I are exactly the exponents of the variables that occur in the minimal generators of the irreducible components of I (Lemma 5.3). This result indicates that the well known Alexander duality for squarefree monomial ideals could also hold for other families of monomial ideals.

We give algorithms to compute the symbolic powers of monomial ideals using *Macaulay*2 [**GSa**] (Lemma 5.5, Remarks 5.6 and 5.14). For a monomial ideal with no embedded primes we classify the normality of its symbolic Rees algebra in terms of the normality of its primary components (Proposition 5.19).

The normality of a monomial ideal is well understood from the computational point of view. If I is minimally generated by $x^{v_1}, \ldots, x^{v_r}$ and A is the matrix with column vectors $v_1^{\mathrm{t}}, \ldots, v_r^{\mathrm{t}}$, then I is normal if and only if the system $xA \geq \mathbf{1}; x \geq 0$ has the integer rounding property [**DV10**, Corollary 2.5]. The normality of I can be determined using the program *Normaliz* [**BIR**$^+$]. For the normality of monomial ideals of dimension 2 see [**CQ10, GSVV13**] and the references therein.

To compute the generators of the symbolic Rees algebra of a monomial ideal one can use the algorithm in the proof of [**HHT07**, Theorem 1.1]. If the primary components of a monomial ideal are normal, we present a procedure that computes the generators of its symbolic Rees algebra using Hilbert bases and *Normaliz* [**BIR**$^+$] (Proposition 5.21, Example 5.23), and give necessary and sufficient conditions for the equality between its ordinary and symbolic powers (Corollary 5.30).

In Section 5.2 we study edge ideals of weighted oriented graphs. A *directed graph* or *digraph* $\mathcal{D}$ consists of a finite set $V(\mathcal{D})$ of vertices, together with a prescribed collection $E(\mathcal{D})$ of ordered pairs of distinct points called *edges* or *arrows*. An *oriented graph* is a digraph having no oriented cycles of length two. In other words an oriented graph $\mathcal{D}$ is a simple graph G together with an orientation of its edges. We call G the *underlying graph* of $\mathcal{D}$. If a digraph $\mathcal{D}$ is endowed with a function $d\colon V(\mathcal{D}) \to \mathbb{N}_+$, where $\mathbb{N}_+ := \{1, 2, \ldots\}$, we call $\mathcal{D}$ a *vertex-weighted digraph*.

Edge ideals of edge-weighted graphs were introduced and studied by Paulsen and Sather-Wagstaff [**PSW13**]. In this work we consider edge ideals of graphs which are oriented and have weights on the vertices. In what follows by a weighted oriented graph we shall always mean a vertex-weighted oriented graph.

Let $\mathcal{D}$ be a vertex-weighted digraph with vertex set $V(\mathcal{D}) = \{x_1, \ldots, x_n\}$. The weight $d(x_i)$ of x_i is denoted simply by d_i. The *edge ideal* of $\mathcal{D}$, denoted $I(\mathcal{D})$, is the ideal of R given by

$$I(\mathcal{D}) := (x_i x_j^{d_j} \mid (x_i, x_j) \in E(\mathcal{D})).$$

If a vertex x_i of $\mathcal{D}$ is a *source* (that is, has only arrows leaving x_i) we shall always assume $d_i = 1$ because in this case the definition of $I(\mathcal{D})$ does not depend on the weight of x_i. In the special case when $d_i = 1$ for all i, we recover the edge ideal of the graph G which has been extensively studied in the literature [**DHS13, FHM13, GV11, HM10, HH11, MV12, SVV94, VT13, Vil90, Vil15**]. A vertex-weighted digraph $\mathcal{D}$ is called *Cohen–Macaulay* (over the field K) if $R/I(\mathcal{D})$ is a Cohen–Macaulay ring.

It turns out that edge ideals of weighted acyclic tournaments are Cohen–Macaulay and satisfy Alexander duality (Corollaries 5.42 and 5.44). For transitive weighted oriented graphs it is shown that Alexander duality holds (Theorem 5.43). Edge ideals of weighted digraphs arose in the theory of Reed-Muller codes as initial ideals of vanishing ideals of projective spaces over finite fields [**CNL17, MV12, MBPV17**].

A major result of Pitones, Reyes and Toledo [**PRT17**] shows an explicit combinatorial expression for the irredundant decomposition of $I(\mathcal{D})$ as a finite intersection of irreducible

monomial ideals (Theorem 5.33). We will use their result to prove the following explicit combinatorial classification of all Cohen–Macaulay weighted oriented forests.

Theorem 5.49 *Let $\mathcal{D}$ be a weighted oriented forest without isolated vertices and let G be its underlying forest. The following conditions are equivalent:*

(a) *$\mathcal{D}$ is Cohen–Macaulay.*
(b) *$I(\mathcal{D})$ is unmixed, that is, all its associated primes have the same height.*
(c) *G has a perfect matching $\{x_1, y_1\}, \ldots, \{x_r, y_r\}$ so that $\deg_G(y_i) = 1$ for all $i = 1, \ldots, r$ and $d(x_i) = d_i = 1$ if $(x_i, y_i) \in E(\mathcal{D})$.*

For additional information, we refer to **[BJG08]** for the theory of digraphs, and **[GV11, HH11, MV12, Vil15]** for the theory of edge ideals of graphs and monomial ideals.

Finally, we describe the contents of Chapter 6. Let f be a monomial of R, and let $I \subset R$ be a monomial ideal. The following two inequalities were shown in [**CHH$^+$17**, Theorem 3.1]:

(A) $\operatorname{depth}(R/(I\colon f)) \geq \operatorname{depth}(R/I)$,
(B) $\operatorname{reg}(R/I) \geq \operatorname{reg}(R/(I\colon f))$,

where $\operatorname{depth}(R/I)$ and $\operatorname{reg}(R/I)$ are the depth and regularity of the quotient ring R/I and $(I\colon f) = \{g \in R | gf \in I\}$ is referred to as a colon ideal. If I and f are squarefree, we show that (A) and (B) are equivalent using a duality theorem of Terai **[Ter99]** (Theorem 6.7) and some duality formulas for edge ideals of clutters (Lemma 6.6), that is, (A) and (B) are dual statements in the squarefree case (Proposition 6.8).

We introduce a formula expressing $\operatorname{depth}(R/(I,f)) - \operatorname{depth}(R/I)$, $\operatorname{reg}(R/I)$ and $\operatorname{reg}(R/(f,I))$ in terms of the depth and regularity of polarizations (Proposition 6.11). Then, as an application, we give an alternate proof of (A) and (B), and show some other known inequalities about depth and regularity (Corollary 6.12). If $\operatorname{in}_\prec(I+f) = I + \operatorname{in}_\prec(f)$ for some monomial order $\prec$ and some homogeneous polynomial f, we show that (A) and (B) hold (Corollary 6.13).

The aim is to use these results to study the behavior of the depth and regularity of R/I, locally at a variable x_i, when we lower the degree of all the highest powers of the variable x_i occurring in the minimal generating set of I and, furthermore, to examine the depth and regularity of powers and symbolic powers of edge ideals of clutters and graphs, and their ideals of covers, using combinatorial optimization techniques.

Fix a variable x_i that occurs in the minimal generating set $G(I)$ of I. Let q be the maximum of the degrees in x_i of the monomials of $G(I)$, let $\mathcal{B}_i$ be the set of all monomials of $G(I)$ of degree q in x_i, let p be the maximum of the degrees in x_i of the monomials of $\mathcal{A}_i = G(I) \setminus \mathcal{B}_i$, and consider the $L = (\{x^a/x_i | \, x^a \in \mathcal{B}_i\} \cup \mathcal{A}_i\})$.

One of our main results shows that the depth is locally non-decreasing at each variable x_i when lowering the top degree. Note that if $p = 0$, that is, if all generators of I that are divisible by x_i have degree q in x_i, then $L = (I\colon x_i)$. Thus when $p = 0$ we have from (A) that $\operatorname{depth}(R/L) = \operatorname{depth}(R/(I\colon x_i)) \geq \operatorname{depth}(R/I)$. This theorem allow control over the depth when the degrees in x_i of the generators varies.

Theorem 6.15 (a) *If* $p \geq 1$ *and* $q - p \geq 2$, *then* $\operatorname{depth}(R/I) = \operatorname{depth}(R/L)$.

(b) *If* $p \geq 0$ *and* $q - p = 1$, *then* $\operatorname{depth}(R/L) \geq \operatorname{depth}(R/I)$.

(c) *If* $p = 0$ *and* $q \geq 2$, *then*

$$\operatorname{depth}(R/I) = \operatorname{depth}(R/(\{x^a/x_i^{q-1} \,|\, x^a \in \mathcal{B}_i\} \cup \mathcal{A}_i\})).$$

There are similar results for regularity (Theorem 6.21). As a consequence one recovers a result of Herzog, Takayama and Terai **[HTT05]** showing that

$$\operatorname{depth}(R/\operatorname{rad}(I)) \geq \operatorname{depth}(R/I)$$

and a result of Ravi **[Rav90]** showing that

$$\operatorname{reg}(R/\operatorname{rad}(I)) \leq \operatorname{reg}(R/I).$$

(Corollaries 6.17 and 6.22).The result can also be used to show that the Cohen-Macaulay property of a vertex-weighted digraph is dependent only on knowing which vertices have weight greater than one and not on the actual weights used (5.40). In other words an oriented graph D is CohenMacaulay if and only if the oriented graph U, obtained from D by replacing each weight $d_i > 3$ with $d_i = 2$, is CohenMacaulay. Seemingly, this ought to somewhat facilitate the verification of this property. This answers a question of Aron Simis and a related question of Antonio Campillo.

There are some classes of monomial ideals whose powers have non-increasing depth and non-decreasing regularity **[CHH$^+$17, CPSF$^+$15, Han17, HT$^+$17, SF18]** A natural way to show these properties for a monomial ideal I is to prove the existence of a monomial f such that $(I^{k+1}\colon f) = I^k$ for $k \geq 1$. This was exploited in **[CHH$^+$17, MV12]** and in **[HM10,** Corollary 3.11] in connection to normally torsion free ideals.

Since any squarefree monomial ideal is the edge ideal $I(\mathcal{C})$ of a clutter $\mathcal{C}$, we will study the depth and regularity of powers and symbolic powers of edge ideals of clutters and graphs–and their ideals of covers—that have nice combinatorial optimization properties (e.g., max-flow min-cut, ideal, uniform, and unmixed clutters, strongly perfect and very

well-covered graphs). The k-th symbolic power of an ideal I is denoted by $I^{(k)}$ (Definition 6.27). The *ideal of covers* of a clutter $\mathcal{C}$, denoted $I(\mathcal{C})^\vee$, is the edge ideal of $\mathcal{C}^\vee$, the clutter of minimal vertex covers of $\mathcal{C}$.

If $I(\mathcal{C})$ is the edge ideal of a clutter $\mathcal{C}$ which has a good leaf, then the powers of $I(\mathcal{C})$ have non-increasing depth and non-decreasing regularity [**CHH$^+$17**, Theorem 5.1]. In particular edge ideals of forests or simplicial trees have these properties. Our next result gives a wide family of ideals with these properties.

Theorem 6.34 *If $I = I(\mathcal{C})$ is the edge ideal of an unmixed clutter $\mathcal{C}$ with the max-flow min-cut property, then*

(a) $\operatorname{depth}(R/I^k) \geq \operatorname{depth}(R/I^{k+1})$ *for* $k \geq 1$.
(b) $\operatorname{reg}(R/I^k) \leq \operatorname{reg}(R/I^{k+1})$ *for* $k \geq 1$.

Let G be a graph with vertex set $V(G) = \{x_1, \ldots, x_n\}$ and edge set $E(G)$. A result of T. N. Trung [**TT12**] shows that for $k \gg 0$ one has

$$\operatorname{depth}(R/I(G)^k) = |\operatorname{isol}(G)| + c_0(G),$$

where $\operatorname{isol}(G)$ is the set of isolated vertices of G and $c_0(G)$ is the number of non-trivial bipartite components of G. We complement this fact by observing that $\dim(R) - \ell(I(G))$ is equal to $|\operatorname{isol}(G)| + c_0(G)$, where $\ell(I(G))$ is the analytic spread of $I(G)$, and by showing the inequality

$$\operatorname{depth}(R/(I(G)^k \colon x_i^k)) \leq \operatorname{depth}(R/(I(G \setminus N_G(x_i))^k, N_G(x_i)))$$

for $k \geq 1$ and $i = 1, \ldots, n$ (Proposition 6.36), where $N_G(x_i)$ is the neighbor set of x_i. For $k = 1$ this inequality follows from $(I(G) \colon x_i) = (I(G \setminus N_G(x_i)), N_G(x_i))$ [**Vil15**, p. 293] and using the inequality $\operatorname{depth}(R/(I(G) \colon x_i)) \geq \operatorname{depth}(R/I(G))$. The general case follows by successively applying Theorem 6.15 locally at each variable.

It is an open problem whether or not the powers of the edge ideal of a graph have non-increasing depth. To the best of our knowledge this is open even for bipartite graphs. Our next application extends the fact that the powers of $I(G)^\vee$, the ideal of covers of G, have non-increasing depth if G is bipartite [**CPSF$^+$15, Han17, HT$^+$17**].

Corollary 6.38 *Let G be a bipartite graph. The following hold.*

(a) *If G is unmixed, then $I(G)$ has non-increasing depth.*
(b) ([**CPSF$^+$15**, Theorem 3.2], [**Han17**], [**HT$^+$17**, Corollary 2.4]) *$I(G)^\vee$ has non-increasing depth.*
(c) *$I(G)^\vee$ has non-decreasing regularity.*

An interesting example due to Kaiser, Stehlík, and Škrekovski [**KSŠ14**] shows that the powers of the ideal of covers of a graph does not always have non-increasing depth (Example 6.39), that is, part (b) of Corollary 6.38 fails for non-bipartite graphs. A nice result of L. T. Hoa, K. Kimura, N. Terai and T. N. Trung [**KTT$^+$17**, Theorem 3.2] shows that the symbolic powers of the ideal of covers of a graph have non-increasing depth. A similar result holds for the ideal of covers of a uniform ideal clutter (Corollary 6.35).

If G is a very well-covered graph, then the depths of symbolic powers of $I(G)^\vee$ form a non-increasing sequence [**SF18**]. In this case we show that the symbolic powers of $I(G)$ have non-increasing depth and non-decreasing regularity (Proposition 6.40).

We will give another family of squarefree monomial ideals whose symbolic powers have non-increasing depth and non-decreasing regularity. A *clique* of a graph G is a set of vertices inducing a complete subgraph. The *clique clutter* of the graph G, denoted by $\mathrm{cl}(G)$, is the clutter on $V(G)$ whose edges are the maximal cliques of G.

Proposition 6.42 *Let G be a strongly perfect graph and let $\mathrm{cl}(G)$ be its clique clutter. If J is the ideal of covers of $\mathrm{cl}(G)$, then*

(a) $\operatorname{depth}(R/J^{(k)}) \geq \operatorname{depth}(R/J^{(k+1)})$ *for* $k \geq 1$.
(b) $\operatorname{reg}(R/J^{(k)}) \leq \operatorname{depth}(R/J^{(k+1)})$ *for* $k \geq 1$.

Bipartite graphs, chordal graphs, comparability graphs, and Meyniel graphs are strongly perfect (see [**Rav99**] and the references therein). Thus this result generalizes Corollary 6.38(b) because if G is a bipartite graph, then $\mathrm{cl}(G) = G$ and $I(G^\vee)^{(k)} = I(G^\vee)^k$ for $k \geq 1$ [**GRV09**].

For edge ideals of clutters the Cohen–Macaulay property of its k-th ordinary or symbolic power is well understood if $k \geq 3$. By a result of N. Terai and N. V. Trung [**TT12**], if $I(\mathcal{C})$ is the edge ideal of a clutter $\mathcal{C}$, then $I(\mathcal{C})^k$ (resp. $I(\mathcal{C})^{(k)}$) is Cohen–Macaulay for some $k \geq 3$ if and only if $I(\mathcal{C})$ is a complete intersection (resp. the independence complex $\Delta_\mathcal{C}$ of $\mathcal{C}$ is a matroid).

The case when G is a graph and $k = 2$ is treated in [**KTT$^+$17, T$^+$16**]. The Cohen–Macaulay property of the square of an edge ideal can be expressed in terms of its connected components [**HTT16**]. Edge ideals of graphs whose square is Cohen–Macaulay have a rich combinatorial structure and have been classified combinatorially by D. T. Hoang, N. C. Minh and T. N. Trung [**KTT$^+$17, HTT16**].

As an application we recover the following fact.

Corollary 6.48 [**KTT$^+$17**, Proposition 4.2] *Let G be a bipartite graph without isolated vertices. Then $I(G)^2$ is Cohen-Macaulay if and only if $I(G)$ is a disjoint union of edges.*

For additional information we refer to **[Eis13, Mat89]** (for commutative algebra), **[Cor01, Sch98, Sch03]** (for combinatorial optimization), **[Har]** (for graph theory), and **[FHM13, GV11, HH11, VT13, Vil15]** (for the theory of powers of edge ideals of clutters and monomial ideals).

Acknowledgments

First of all, I would like to thank my advisor, prof. Rafael Villarreal, for his insights, guidance and support. The door to his office was always open whenever I needed mathematical or moral support or had a question about my research. Sharing his ideas with me was really helpful, especially when I was not sure how to continue.

I want to thank the administrative staff, especially Roxana, not only for her administrative support but also for her kindness and her immense help.
I want to thank the reading committee, Manuel González Sarabia, Carlos Rentería Marquez, Jose Martinez-Bernal, and Carlos Valencia Oleta, for taking the time to carefully read the thesis and for the useful comments.

I would like to thank Juliana Restrepo, my family, especially to Mom-with your aching hands you have forged this dream- and friends for their love, support, and encouragement. All of the small accomplishments in my life, including the writing of this Ph.D thesis, would not have been possible without them.
Lastly, I thank Consejo Nacional de Ciencia y Tecnología, CONACyT, for the PhD scholarship to get this Ph.D.CVU 630313.

The question you raise "how can such a formulation lead to computations" doesn't bother me in the least! Throughout my whole life as a mathematician, the possibility of making explicit, elegant computations has always come out by itself, as a byproduct of a thorough conceptual understanding of what was going on. Thus I never bothered about whether what would come out would be suitable for this or that, but just tried to understand - and it always turned out that understanding was all that mattered.

—Alexander Grothendieck (in a letter to Ronnie Brown, 12.04.1983)

CHAPTER 1

Primary Decompositions and Graded Modules

The main topics of this chapter are primary decompositions of modules and ideals, Hilbert series of graded modules, Cohen–Macaulay rings, and Artinian rings. The Hilbert theorem for graded modules is introduced here. As usual the h-vector and the a-invariant of a graded module are defined using the Hilbert–Serre theorem.

1.1. Module theory

Noetherian modules and localizations. Let R be a commutative ring with unit and let M be an R-module. Recall that M is called *Noetherian* if every submodule N of M is finitely generated, that is, $N = Rf_1 + \cdots + Rf_q$, for some $f_1, \ldots, f_q$ in N.

THEOREM 1.1. *The following conditions are equivalent:*

(a) M is Noetherian.

(b) M satisfies the ascending chain condition; that is, for every ascending chain of submodules of M

$$N_1 \subset N_2 \subset \cdots \subset N_n \subset N_{n+1} \subset \cdots \subset M$$

there exists an integer k such that $N_i = N_k$ for every $i \geq k$.

(c) Any nonempty collection $\mathcal{F}$ of submodules of M has a maximal element, that is, there is $N \in \mathcal{F}$ such that if $N \subset N_i$ and $N_i \in \mathcal{F}$, then $N = N_i$.

In particular a *Noetherian ring* R is a commutative ring with unit with the property that every ideal of I is finitely generated; that is, given an ideal I of R there exists a finite number of generators $f_1, \ldots, f_q$ such that

$$I = \left\{ a_1 f_1 + \cdots + a_q f_q \middle| \; a_i \in R, \, \forall \, i \right\}.$$

As usual, if I is generated by $f_1, \ldots, f_q$, we write $I = (f_1, \ldots, f_q)$.

A sequence of R-modules and R-homomorphisms

$$\cdots \xrightarrow{\varphi_{n-2}} M_{n-1} \xrightarrow{\varphi_{n-1}} M_n \xrightarrow{\varphi_n} M_{n+1} \xrightarrow{\varphi_{n+1}} \cdots$$

is said to be *exact* at M_n if $\operatorname{im}\varphi_{n-1} = \ker\varphi_n$. The sequence is said to be *exact* if it is exact at each M_n. An exact sequence of the form $0 \to L \xrightarrow{\iota} M \xrightarrow{\rho} N \to 0$ is said to be *short exact sequence*. Exact sequences were first introduced by Cartan and Eilenberg in their 1956 book.
It is straightforward to see that $0 \to L \xrightarrow{\iota} M \xrightarrow{\rho} N \to 0$ is a short exact sequence if and only if ι is injective, $\operatorname{im}\iota = \ker\rho$ and ρ is surjective.

PROPOSITION 1.2. *Let $0 \to L \xrightarrow{\iota} M \xrightarrow{\rho} N \to 0$ be a short exact sequence of R-modules. Then M is Noetherian if and only if L and N are Noetherian.*

COROLLARY 1.3. *Let M be an R-module and N be a submodule of M. Then M is Noetherian if and only if N and M/N are Noetherian.*

PROPOSITION 1.4. *If M is a finitely generated R-module over a Noetherian ring R, then M is a Noetherian module.*

COROLLARY 1.5. *If R is a Noetherian ring and I is an ideal of R, then R/I and $R^{\oplus n}$ are Noetherian R-modules. In particular any submodule of $R^{\oplus n}$ is finitely generated.*

THEOREM 1.6. (Hilbert Basis Theorem [**Eis13**, Theorem 2.1]) *Let R be a Noetherian ring, then the polynomial ring $R[x]$ is Noetherian.*

An important example of a Noetherian ring is a polynomial ring over a field k. Often we will denote a polynomial ring in several variables by $k[\mathbf{x}]$ and a polynomial ring in one variable by $k[x]$.

The *prime spectrum* of a ring R, denoted by $\operatorname{Spec}(R)$, is the set of prime ideals of R. The *minimal primes* of R are the minimal elements of $\operatorname{Spec}(R)$ with respect to inclusion and the maximal ideals of R are the maximal elements of the set of proper ideals of R with respect to inclusion. We endow $\operatorname{Spec}(R)$ with the structure of a topological space. For every subset $S \subset R$, we define

$$V(S) := \{\mathfrak{p} \in \operatorname{Spec}(R) : S \subset \mathfrak{p}\}.$$

Note that $V(S) = V(\langle S\rangle)$ with $\langle S\rangle$ the ideal generated by S and for each pair of ideals $I \subset J$ of R, we have $V(J) \subset V(I)$. The *minimal primes* of I are the minimal elements of $V(I)$ with respect to inclusion.

LEMMA 1.7. *Let R be a ring, then*

(a) $V(0) = \operatorname{Spec}(R)$ and $V(1) = \emptyset$.

(b) If $\{I_i\}_i$ is any collection of ideals of R, then $V(\bigcup_i I_i) = V(\sum_i I_i) = \bigcap_i V(I_i)$.

(c) If I and J are two ideals of R, then $V(I \cap J) = V(IJ) = V(I) \cup V(J)$.

The above lemma shows that the subsets $V(I)$ of $\mathrm{Spec}(R)$ form the closed sets of a topology on $\mathrm{Spec}(R)$, it is called the *Zariski topology* of the prime spectrum of R.

A *local ring* $(R, \mathfrak{m}, k)$ is a Noetherian ring R with exactly one maximal ideal $\mathfrak{m}$, the field $k = R/\mathfrak{m}$ is called the *residue field* of R.

The *homomorphisms of rings* $\varphi\colon R \to S$ that we consider satisfies $\varphi(1_R) = 1_S$.
Let R be a ring and let $\varphi\colon \mathbb{Z} \to R$ be the canonical homomorphism

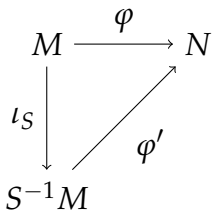
$$\varphi(a) = a \cdot 1_R,$$

then $\ker(\varphi) = n\mathbb{Z}$, for some $n \geq 0$. The integer n is called the *characteristic* of R and is denoted by $\mathrm{char}(R)$.

PROPOSITION 1.8. *Let $(R, \mathfrak{m}, k)$ be a local ring, then R has characteristic zero or a power of a prime.*

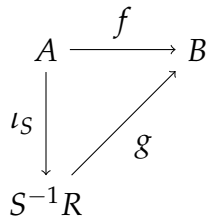
Localizations of Modules. Let R be a ring. A subset $S \subset R$ is a *multiplicative closed subset* if $1 \in S$ and $x, y \in S$ implies $xy \in S$. Let M an R-module, and S a multiplicatively closed subset of R. We define an equivalence relation on $M \times S$ by $(m, s) \sim (n, t)$ if there is $u \in S$ such that $u(mt - ns) = 0$. The reason we need to add the u is that otherwise the equivalence relation would not be transitive, that is, would not be an equivalence relation. Denote by $S^{-1}M$ or $M[S^{-1}]$, the set of equivalence classes, and by m/s the class of (m, s). $S^{-1}M$ is an $S^{-1}R$-module with addition given by $m/s + n/t := (tm + sn)/st$ and scalar multiplication by $a/s \cdot m/t := am/st$. We call to $S^{-1}M$ the *localization* of M at S. Note that $S^{-1}M$ has structure of R-module defining $r \cdot m/s := rm/s$ with $r \in R$.
There is a canonical R-homomorphism $\iota_S\colon M \to S^{-1}M$, given by $\iota_S(m) = m/1$. If $f\colon M \to N$ is an R-homomorphism, then there is an induced $S^{-1}R$-module homomorphism $S^{-1}f\colon S^{-1}M \longrightarrow S^{-1}N$ given by $f(m/s) = f(m)/s$. Consider the multiplication map $\mu_{r_0} : M \longrightarrow M$, given by $m \longmapsto r_0 m$, for $r_0 \in R$ fixed. Then note that for each $s \in S$, $\mu_s : S^{-1}M \longrightarrow S^{-1}M$ is an R-isomorphism.

PROPOSITION 1.9. (Universal Property of Localization) *Let N be an R-module such that the elements of S act by multiplication as automorphisms, that is, $\mu_s : N \longrightarrow N$ is an R-isomorphism for each $s \in S$. If $\varphi : M \longrightarrow N$ is an R-homomorphism, then there exists a unique R-homomorphism $\varphi' : S^{-1}M \longrightarrow N$ such that the following diagram commutes*



If we apply the definition of localization to $M = R$, we obtain the localization for a ring.

COROLLARY 1.10. *Let $f : A \longrightarrow B$ be a ring map that sends every element in S to a unit of B. Then there is a unique homomorphism $g : S^{-1}A \longrightarrow B$ such that the following diagram commutes.*



PROPOSITION 1.11. *Modules over $S^{-1}R$ can be naturally identified with R-modules M having the property that the multiplication map $\mu_s : M \longrightarrow M$ is bijective for all $s \in S$. In other words, the category of $S^{-1}R$-modules is equivalent to the category of R-modules M with the property that every $s \in S$ acts as an automorphism on M.*

EXAMPLE 1.12. If f is in a ring R and $S = \{f^i \mid i \in \mathbb{N}\}$, then $S^{-1}R$ is usually written R_f. For instance if $R = \mathbb{C}[x]$ is a polynomial ring in one variable over the field $\mathbb{C}$ of complex numbers, then $R_x = \mathbb{C}[x, x^{-1}]$ is the ring of Laurent polynomials.

DEFINITION 1.13. Let $\mathfrak{p}$ be a prime ideal of a ring R and $S = R \setminus \mathfrak{p}$. In this case $S^{-1}R$ is written $R_{\mathfrak{p}}$ and is called the *localization* of R at $\mathfrak{p}$.

PROPOSITION 1.14. (Properties of localization) *Let R be a ring, $S \subset R$ be a multiplicative closed subset.*

(a) Every ideal of $S^{-1}R$ is of the form $IS^{-1}R$, the extension under ι_S for some ideal I of R. That is, if $L \subset S^{-1}R$ is an ideal, then there exists an ideal $I \subset R$ such that

$$L = \{a/s : a \in I, s \in S\}.$$

(b) If R is Noetherian, then so it is $S^{-1}R$.

(c) The only prime ideals of $S^{-1}R$ are $\mathfrak{p}S^{-1}R$, where $\mathfrak{p}$ is a prime ideal of R such that $\mathfrak{p} \cap S = \emptyset$. Thus prime ideals of $S^{-1}R$ are in bijective correspondence with the prime ideals of R that do not intersect S.

(d) *The set* $\overline{S} = \{\overline{s} \in R/I : s \in S\}$ *is a multiplicative closed subset of* R/I *and there exist a natural isomorphism*

$$\varphi : S^{-1}R/IS^{-1}R \to \overline{S}^{-1}(R/I).$$

(e) *If* $T \subset R$ *is a multiplicative closed subset such that* $S \subset T$. *Let* $T/1$ *the image of* T *under* ι_S. *Then* $T/1$ *is a multiplicative closed subset and there exists a natural isomorphism*

$$\phi : (T/I)^{-1}(S^{-1}R) \to T^{-1}R.$$

(f) *(Exactness of Localization) Let* $0 \to L \xrightarrow{\iota} M \xrightarrow{\rho} N \to 0$ *be a short exact sequence of* R*-modules, then so it is* $0 \to S^{-1}L \xrightarrow{S^{-1}\iota} S^{-1}M \xrightarrow{S^{-1}\rho} S^{-1}N \longrightarrow 0$, *where* $S^{-1}\iota$ *and* $S^{-1}\rho$ *are the natural induced maps.*

EXAMPLE 1.15. Let $\mathfrak{p}$ be a prime ideal of a ring R. Let $S = R \setminus \mathfrak{p}$, then $\mathrm{Spec}(R_\mathfrak{p})$ correspond to $\{\mathfrak{q} \in \mathrm{Spec}(R) : \mathfrak{q} \subset \mathfrak{p}\}$. Thus

$$(R_\mathfrak{p}, \mathfrak{p}R_\mathfrak{p}, k(\mathfrak{p}))$$

is a local ring, where $k(\mathfrak{p}) = R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$ denotes the residue field of $R_\mathfrak{p}$.

Krull dimension and height. By a *chain* of prime ideals of a ring R we mean a finite strictly increasing sequence of prime ideals

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n,$$

the integer n is called the *length* of the chain. The *Krull dimension* of R, denoted by $\dim(R)$, is the supremum of the lengths of all chains of prime ideals in R. Let $\mathfrak{p}$ be a prime ideal of R, the *height* of $\mathfrak{p}$, denoted by $\mathrm{ht}(\mathfrak{p})$, is the supremum of the lengths of all chains of prime ideals

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n = \mathfrak{p}$$

which end at $\mathfrak{p}$. Since $\mathfrak{p} \longmapsto \mathfrak{p}R_\mathfrak{p}$ is an inclusion-preserving bijection from the set of all primes of R with $\mathfrak{p} \cap S = \emptyset$ to the set of all primes $\mathfrak{q}$ of $S^{-1}R$, then $\dim(R_\mathfrak{p}) = \mathrm{ht}(\mathfrak{p})$. If I is an ideal of R, then $\mathrm{ht}(I)$, the *height* of I, is defined as

$$\mathrm{ht}(I) = \inf\{\mathrm{ht}(\mathfrak{p}) |\, I \subset \mathfrak{p} \text{ and } \mathfrak{p} \in \mathrm{Spec}(R)\}.$$

In general $\dim(R/I) + \mathrm{ht}(I) \leq \dim(R)$: Let $A_0 \subset A_1 \subset \cdots \subset A_n$ be a chain of prime ideals of R/I, then $A_i = \mathfrak{q}_i/I$, where $\mathfrak{q}_i$ is a prime ideal of R containing I for $i = 0, 1, \ldots, n$. Let $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_s = \mathfrak{q}_0$ be a chain of prime ideals of R. Then $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_s = \mathfrak{q}_0 \subset \cdots \subset \mathfrak{q}_n$ is a chain of prime ideals of R. Therefore $n + s \leq \dim(R)$. Taking the infimum on s, we get that $n + \mathrm{ht}(I) \leq \dim(R)$. Again taking the supremum, we get the

inequality.

The difference $\dim(R) - \dim(R/I)$ is called the *codimension* of I and $\dim(R/I)$ is called the *dimension* of I.

Let M be an R-module. The *annihilator* of M is defined as

$$\operatorname{ann}_R(M) = \{x \in R | \, xM = 0\},$$

It is convenient to generalize the notion of annihilator to ideals and submodules. Let N_1 and N_2 be submodules of M, their *ideal quotient* or *colon ideal* as

$$(N_1 : {}_R N_2) = \{x \in R | \, xN_2 \subset N_1\}.$$

Let us recall that the *dimension* of an R-module M is

$$\dim(M) = \dim(R/\operatorname{ann}(M))$$

and the *codimension* of M is $\operatorname{codim}(M) = \dim(R) - \dim(M)$.

Primary decomposition of modules. Let I be an ideal of a ring R. The *radical* of I is

$$\operatorname{rad}(I) = \{x \in R | \, x^n \in I \text{ for some } n > 0\},$$

the radical is also denoted by $\sqrt{I}$. In particular $\operatorname{rad}(0)$, denoted by $\mathfrak{N}_R$ or $\operatorname{nil}(R)$, is the set of *nilpotent elements* of R and is called the *nilradical* of R. A ring is *reduced* if its nilradical is zero. The *Jacobson radical* of R is the intersection of all the maximal ideals of R.

PROPOSITION 1.16. *If I is a proper ideal of a ring R, then* $\operatorname{rad}(I)$ *is the intersection of all prime ideals containing I.*

DEFINITION 1.17. Let M be a module over a ring R. The set of *associated primes* of M, denoted by $\operatorname{Ass}_R(M)$, is the set of all prime ideals $\mathfrak{p}$ of R such that there is an injective homomorphism ϕ of R-modules:

$$R/\mathfrak{p} \xrightarrow{\phi} M.$$

Equivalently, $\mathfrak{p} \subset R$ is an *associated prime* if there exists $u \neq 0$ in M such that $\mathfrak{p} = \operatorname{ann}_R(u) = \{r \in R : ru = 0\}$: Assume that $\mathfrak{p} = \operatorname{ann}_R(u)$, then we define $\phi : R/\mathfrak{p} \to M$, given by $\overline{r} \mapsto ru$. Clearly ϕ is well defined and $ru = 0$ means that $r \in \operatorname{ann}_R(u) = \mathfrak{p}$, therefore $\overline{r} = \overline{0}$ in $R/\mathfrak{p}$, thus ϕ is injective. Conversely, set $u := \phi(\overline{1})$, then

$$\begin{aligned} \operatorname{ann}_R(u) &= \{r \in R : r\phi(\overline{1}) = 0\} \\ &= \{r \in R : \phi(\overline{r}) = 0\} \end{aligned}$$

$$\text{since } \phi \text{ is injective } \rightsquigarrow = \{r \in R : \overline{r} = \overline{0}\}$$
$$= \mathfrak{p}$$

LEMMA 1.18. *Let R be a Noetherian ring. If $M \neq 0$ is an R-module, then the set $\mathrm{Ass}_R(M) \neq \emptyset$.*

PROOF. Let $\mathcal{F} = \{I \subsetneq R \text{ ideal } : I = \mathrm{ann}(u), \text{ for some } 0 \neq u \in M\}$ ordered by inclusion. Clearly $\mathcal{F} \neq \emptyset$. By Theorem 1.1 this family has a maximal element that we denote by $\mathrm{ann}(u_0)$. It suffices to show that $\mathrm{ann}(u_0)$ is prime. Let x, y be two elements of R such that $xy \in \mathrm{ann}(u_0)$. Then $xyu_0 = 0$; if $y \notin \mathrm{ann}(u_0)$, then $yu_0 \neq 0$, thus $\mathrm{ann}(u_0) \subset \mathrm{ann}(yu_0)$, and by maximality of $\mathrm{ann}(u_0)$ we have that $\mathrm{ann}(u_0) = \mathrm{ann}(yu_0)$. Therefore $x \in \mathrm{ann}(u_0)$. ♠

PROPOSITION 1.19. *Let R be a ring and let S be a multiplicatively closed subset of R. If M is an R-module and $\mathfrak{p}$ is a prime ideal of R with $S \cap \mathfrak{p} = \emptyset$, then $\mathfrak{p}$ is an associated prime of M if and only if $\mathfrak{p}S^{-1}R$ is an associated prime of $S^{-1}M$.*

PROOF. If $\mathfrak{p}$ is in $\mathrm{Ass}(M)$, then $R/\mathfrak{p} \hookrightarrow M$. Hence by proposition 1.14 we have

$$S^{-1}R/\mathfrak{p}S^{-1}R \hookrightarrow S^{-1}M.$$

Thus, $\mathfrak{p}S^{-1}R$ is an associated prime of $S^{-1}M$.

Conversely, assume $\mathfrak{p}S^{-1}R = \mathrm{ann}(u/s)$. Take generators for $\mathfrak{p}$, say $a_1, \ldots, a_r$. Then $a_i u/s = 0$. Hence for each i there is $s_i \in S$ such that $s_i a_i u = 0$. Define $s' = s_1 \cdots s_r$, then $s' a_i u = 0$. Thus $\mathfrak{p}s'u = 0$. On the other hand, if $r(s'u) = 0$, then $rs' \in \mathfrak{p}S^{-1}R \cap R = \mathfrak{p}$. Therefore $r \in \mathfrak{p}$. Hence $\mathfrak{p} = \mathrm{ann}(s'm)$. ♠

DEFINITION 1.20. Let M be an R-module. The *support* of M, denoted by $\mathrm{Supp}(M)$, is the set of all prime ideals $\mathfrak{p}$ of R such that $M_\mathfrak{p} \neq 0$.

LEMMA 1.21. *If $0 \to M' \to M \to M'' \to 0$ is a short exact sequence of modules over a ring R, then $\mathrm{Supp}(M) = \mathrm{Supp}(M') \cup \mathrm{Supp}(M'')$.*

PROOF. Let $\mathfrak{p}$ be a prime ideal of R. It suffices to observe that from the exact sequence

$$0 \to M'_\mathfrak{p} \to M_\mathfrak{p} \to M''_\mathfrak{p} \to 0,$$

we get $M_\mathfrak{p} \neq 0$ if and only if $M'_\mathfrak{p} \neq 0$ or $M''_\mathfrak{p} \neq 0$. ♠

THEOREM 1.22. *Let $M \neq 0$ be a finitely generated R-module, where R is Noetherian. Then there is a filtration of submodules*

$$(0) = M_0 \subset M_1 \subset \cdots \subset M_n = M$$

and prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ *of* R *such that* $M_i/M_{i-1} \simeq R/\mathfrak{p}_i$ *for all* i.

PROOF. By Lemma 1.18 there exists a prime ideal $\mathfrak{p}_1$ and a submodule M_1 of M such that $R/\mathfrak{p}_1 \simeq M_1$. If $M_1 \subsetneq M$, then there exists an associated prime ideal $\mathfrak{p}_2$ of M/M_1 such that $R/\mathfrak{p}_2$ is isomorphic to a submodule of M/M_1, that is, $R/\mathfrak{p}_2 \simeq M_2/M_1$, where M_2 is a submodule of M containing M_1. If $M_2 \subsetneq M$, we pick an associated prime $\mathfrak{p}_3$ of M/M_2 and repeat the argument. Since M is Noetherian a repeated use of this procedure yields the required filtration. ♠

In general the primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ that occur in a filtration of the type described in the previous result are not associated primes of the module M; see **[DS93]** for a careful discussion of filtrations and for some of their applications to combinatorics.

LEMMA 1.23. *If* $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ *is a short exact sequence of modules over a ring* R, *then* $\operatorname{Ass}(M') \subset \operatorname{Ass}(M)$ *and* $\operatorname{Ass}(M) \subset \operatorname{Ass}(M') \cup \operatorname{Ass}(M'')$.

PROOF. $\operatorname{Ass}(M') \subset \operatorname{Ass}(M)$ is obvious, since if $R/\mathfrak{p} \hookrightarrow M'$, we have a composite map $R/\mathfrak{p} \hookrightarrow M' \hookrightarrow M$. Now, let $\mathfrak{p} \in \operatorname{Ass}(M)$, then $\mathfrak{p} = \operatorname{ann}(u)$ with $u \in M$. We show that if $\mathfrak{p} \notin \operatorname{Ass}(M')$, then we claim that $\mathfrak{p} = \operatorname{ann}(g(u))$. Clearly $\mathfrak{p}g(u) = 0$. If $\mathfrak{p} \subsetneq \operatorname{ann}(g(u))$, then there is $r \in R$ such that $rg(u) = 0$ and $r \notin \mathfrak{p}$. Since $r \notin \mathfrak{p}$, $ru = f(a) \neq 0$ for some $a \in M'$. But, $0 = \mathfrak{p}ru = \mathfrak{p}f(a)$, also if $0 = zf(a)$ for some $z \in R$, then $zr \in \mathfrak{p}$, thus $z \in \mathfrak{p}$. Therefore $\mathfrak{p} = \operatorname{ann}(f(a))$. Hence, $0 = \mathfrak{p}f(a) = f(\mathfrak{p}a)$, implies $\mathfrak{p}a = 0$ and if $0 = za$ for some $z \in R$, then $0 = zf(a)$, implying $z \in \mathfrak{p}$. Therefore $\mathfrak{p} = \operatorname{ann}(a)$, a contradiction. Thus $\mathfrak{p} \in \operatorname{Ass}(M'')$. ♠

COROLLARY 1.24. *Let* R *be a Noetherian ring. If* $M \neq 0$ *is a finitely generated* R*-module, then* $\operatorname{Ass}_R(M)$ *is a finite set.*

PROOF. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be prime ideals as in Theorem 1.22. We use induction on n. By Lemma 1.23, $\operatorname{Ass}(M) \subset \operatorname{Ass}(M_{n-1}) \cup \operatorname{Ass}(M/M_{n-1})$ and then we may apply the induction to $0 \subset M_1 \subset \cdots \subset M_{n-1}$. Then $\operatorname{Ass}(M_{n-1}) \subset \bigcup_{i=1}^{n-1} \operatorname{Ass}(M_i/M_{i-1})$. Note that, in general, for any prime $\mathfrak{p}$ in R, $\operatorname{Ass}(R/\mathfrak{p}) = \{\mathfrak{p}\}$, since $\mathfrak{p}$ is obviously an associated prime because there certainly is an R-monomorphism from $R/\mathfrak{p}$ to itself. If $\mathfrak{q} \in \operatorname{Ass}(R/\mathfrak{p})$, then $\mathfrak{q} = \operatorname{ann}(\overline{r})$ for some $r \notin \mathfrak{p}$. Then $s \in \mathfrak{q}$ if and only if $sr \in \mathfrak{p}$, thus $s \in \mathfrak{p}$. Thus $\operatorname{Ass}(R/\mathfrak{p}) = \{\mathfrak{p}\}$. Then

$$\begin{aligned}\operatorname{Ass}(M) &\subset \bigcup_{i=1}^{n} \operatorname{Ass}(M_i/M_{i-1}) \\ &= \bigcup_{i=1}^{n} \operatorname{Ass}(R/\mathfrak{p}_i) \\ &= \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \\ &\subset \operatorname{Supp}(M),\end{aligned}$$

where the last containment is obtained using Lemma 1.21, that is,

$$\operatorname{Supp}(M) = \operatorname{Supp}(M_0) \cup \operatorname{Supp}(M_1/M_0) \cup \cdots \cup \operatorname{Supp}(M_n/M_{n-1}),$$

and each $\mathfrak{p}_i \in \operatorname{Supp}(M_i/M_{i-1})$ ♠

Let M be an R-module. An element $x \in R$ is a *zero divisor* of M if there is $0 \neq m \in M$ such that $xm = 0$. The set of zero divisors of M is denoted by $\mathcal{Z}(M)$. If x is not a zero divisor on M or a unit, we say that x is a *regular element* of M.

LEMMA 1.25. *If M is an R-module, where R is Noetherian. Then*

$$\mathcal{Z}(M) = \bigcup_{\mathfrak{p} \in \operatorname{Ass}_R(M)} \mathfrak{p}.$$

PROOF. The right-hand side is clearly contained in the left-hand side by definition of an associated prime. Let r be a zero divisor of M and consider the family $\mathcal{F} = \{\operatorname{ann}(m) | \, 0 \neq m \in M\}$. We prove that if $\operatorname{ann}(m)$ is a maximal element of $\mathcal{F}$ then it is prime: if $a, b \in R$ such that $ab \in \operatorname{ann}(m)$ with and $a, b \notin \operatorname{ann}(m)$. As $bm \neq 0$ and $abm = 0$, then $a \in \operatorname{ann}(bm)$. Thus $\operatorname{ann}(m) \subsetneq \operatorname{ann}(bm)$, a contradiction. Therefore r is in some such maximal. ♠

LEMMA 1.26. *Let S be a multiplicatively closed subset of a ring R, and let M be a finitely generated R-module. Then $S^{-1}M = 0$ if and only if there exists $s \in S$ such that $sM = 0$.*

PROOF. Suppose that $S^{-1}M = 0$. Say that M is generated by $x_1, \ldots, x_n$ as an R-module. Then for every $i = 1, \ldots, n$, $x_i/1 = 0$ in $S^{-1}M$, which means that there is $s_i \in S$ such that $s_i x_i = 0 \in M$. Let $s = s_1 s_2 \cdots s_n$, which is in S. Then $sx_i = 0$ for all $i = 1, \ldots, n$ and therefore $sM = 0$. Conversely, we assume that there exists $s \in S$ such that $sM = 0$. Then for any element $m/t \in S^{-1}M$ we have $m/t = (sm)/(st) = 0/(st) = 0 \in S^{-1}M$. That is, $S^{-1}M = 0$. ♠

PROPOSITION 1.27. *If M is an R-module finitely generated, then*

$$\operatorname{Ass}(M) \subset \operatorname{Supp}(M) = V(\operatorname{ann}(M)),$$

and any minimal element of $\mathrm{Supp}(M)$ *is in* $\mathrm{Ass}(M)$.

PROOF. If $\mathfrak{p}$ is an associated prime of M, then there exists a monomorphism $R/\mathfrak{p} \hookrightarrow M$ and thus $0 \neq (R/\mathfrak{p})_{\mathfrak{p}} \hookrightarrow M_{\mathfrak{p}}$. Hence $\mathfrak{p}$ is in the support of M, this shows the first containment.

Next, we show $\mathrm{Supp}(M) = V(\mathrm{ann}(M))$. Assume that $\mathfrak{p} \in \mathrm{Supp}(M)$ and let $x \in \mathrm{ann}(M)$. If $x \notin \mathfrak{p}$, then $xm = 0$ for all $m \in M$ and $M_{\mathfrak{p}} = (0)$ (above lemma), which is absurd. Therefore $\mathfrak{p}$ is in $V(\mathrm{ann}(M))$. Conversely let $\mathfrak{p}$ be in $V(\mathrm{ann}(M))$ and let $m_1, \ldots, m_r$ be a finite set of generators of M. If $M_{\mathfrak{p}} = (0)$, then for each i there is $s_i \notin \mathfrak{p}$ so that $s_i m_i = 0$, therefore $s_1 \cdots s_r$ is in $\mathrm{ann}(M) \subset \mathfrak{p}$, which is impossible. Hence $M_{\mathfrak{p}} \neq 0$ and $\mathfrak{p}$ is in the support of M.

To prove the last part take a minimal prime $\mathfrak{p}$ in the support of M. As $M_{\mathfrak{p}} \neq (0)$ there is an associated prime $\mathfrak{p}_1 R_{\mathfrak{p}}$ of $M_{\mathfrak{p}}$, where $\mathfrak{p}_1$ is a prime ideal of R contained in $\mathfrak{p}$. Since $M_{\mathfrak{p}_1} \simeq (M_{\mathfrak{p}})_{\mathfrak{p}_1} \neq (0)$, we get that $\mathfrak{p}_1$ is in the support of M and $\mathfrak{p} = \mathfrak{p}_1$. Therefore using Proposition 1.19 one concludes $\mathfrak{p} \in \mathrm{Ass}(M)$. ♠

Let M be an R-module, the *minimal primes* of M are defined to be the minimal elements of $\mathrm{Supp}(M)$ with respect to inclusion. A minimal prime of M is called an *isolated associated prime* of M. An associated prime of M which is not isolated is called an *embedded prime*.

Traditionally, if $M = R/I$ the associated primes of the module R/I are called associated primes of I. If R is a ring and I is an ideal, note that the minimal primes of I are precisely the minimal primes of $\mathrm{Ass}_R(R/I)$, that is, $\mathfrak{p}$ is minimal prime ideal of R/I if and only if $I \subset \mathfrak{p}$ and there is no prime ideal $I \subset \mathfrak{q}$ which is properly contained in $\mathfrak{p}$. In particular the minimal primes of R are precisely the minimal primes of $\mathrm{Ass}_R(R)$.
Note that $\mathrm{Ass}_R(R/I)$ consists of prime ideals of the form $(I : x)$ for some $x \notin I$.

To avoid endlessly repeating the hypotheses, we shall assume throughout the rest of this chapter that R is a Noetherian ring.

DEFINITION 1.28. Let M be an R-module. A submodule N of M is said to be a $\mathfrak{p}$-*primary submodule* if $\mathrm{Ass}_R(M/N) = \{\mathfrak{p}\}$ where $\mathfrak{p}$ is a prime. An ideal $\mathfrak{q}$ of a ring R is called a $\mathfrak{p}$-*primary ideal* if $\mathrm{Ass}_R(R/\mathfrak{q}) = \{\mathfrak{p}\}$ where $\mathfrak{p}$ is a prime.

PROPOSITION 1.29. *An ideal* $\mathfrak{q} \neq R$ *of a ring* R *is a primary ideal if and only if* $xy \in \mathfrak{q}$ *and* $x \notin \mathfrak{q}$ *implies* $y^n \in \mathfrak{q}$ *for some* $n \geq 1$.

PROOF. Assume $\mathfrak{q}$ is a primary ideal. Let $x, y \in R$ such that $xy \in \mathfrak{q}$ and $x \notin \mathfrak{q}$. Hence y is a zero divisor of $R/\mathfrak{q}$ because $y\overline{x} = \overline{0}$ and $\overline{x} \neq \overline{0}$. Since $\mathcal{Z}(R/\mathfrak{q}) = \{\mathfrak{p}\}$ and $\mathrm{rad}(\mathfrak{q}) = \mathfrak{p}$,

we get $y^n \in \mathfrak{q}$ for some positive integer n. Conversely, it is clear that such condition is equivalent to the only zero divisors of $R/\mathfrak{q}$ are nilpotent, that is, the set of zero divisors is equal to the nilradical. Since zero divisors are a union of associated primes, the nilradical is the intersection of all minimal primes, and every minimal prime is an associated prime, then such condition is equivalent to $\bigcup_{\mathfrak{p}\in \mathrm{Ass}(R/\mathfrak{q})} \mathfrak{p} = \bigcap_{\mathfrak{p}\in \min(R/\mathfrak{q})} \mathfrak{p} = \bigcap_{\mathfrak{p}\in \mathrm{Ass}(R/\mathfrak{q})} \mathfrak{p}$. Which occurs if and only if $\mathrm{Ass}(R/\mathfrak{q})$ has one element (since neither side is empty). Also, it follows that $\mathrm{rad}(\mathfrak{q}) = \mathfrak{p}$ for the single associated prime $\mathfrak{p} = \mathrm{Ass}(R/\mathfrak{q})$. ♠

DEFINITION 1.30. Let M be an R-module. A submodule N of M is said to be *irreducible* if N cannot be written as an intersection of two submodules of M that properly contain N.

I shall assume throughout the rest of this chapter that M is a R-module finitely generated. In this section we will see that any proper submodule N of M has a *irredundant primary decomposition*.

DEFINITION 1.31. Let M be an R-module and let $N \subsetneq M$ be a proper submodule. An *irredundant primary decomposition* of N is an expression of N as an intersection of submodules, say $N = N_1 \cap \cdots \cap N_r$, such that:

(a) (Submodules are primary) $\mathrm{Ass}_R(M/N_i) = \{\mathfrak{p}_i\}$ for all i.
(b) (Irredundancy) $N \neq N_1 \cap \cdots \cap N_{i-1} \cap N_{i+1} \cap \cdots \cap N_r$ for all i.
(c) (Minimality) $\mathfrak{p}_i \neq \mathfrak{p}_j$ if $N_i \neq N_j$.

LEMMA 1.32. *Let M be an R-module. If $Q \neq M$ is an irreducible submodule of M, then Q is a primary submodule.*

PROOF. Assume there are $\mathfrak{p}_1$and $\mathfrak{p}_2$ distinct associated prime ideals of M/Q and pick $r_0 \in \mathfrak{p}_1 \setminus \mathfrak{p}_2$ (or vice versa). There is x_i in $M \setminus Q$ such that $\mathfrak{p}_i = \mathrm{ann}(\overline{x}_i)$, where $\overline{x}_i = x_i + Q$. We claim that

$$(Rx_1 + Q) \cap (Rx_2 + Q) = Q.$$

If z is in the intersection, then $z = \lambda_1 x_1 + q_1 = \lambda_2 x_2 + q_2$, for some $\lambda_i \in R$ and $q_i \in Q$. Note that $r_0 z \in Q$, hence $r_0\lambda_2 x_2$ is in Q and consequently $r_0\lambda_2 \in \mathfrak{p}_2$. Thus $\lambda_2 \in \mathfrak{p}_2$ and we get $\lambda_2 x_2 \in Q$. This shows $z \in Q$ and completes the proof of the claim. As Q is irreducible one has $Q = Rx_1 + Q$ or $Q = Rx_2 + Q$, which is a contradiction because $x_i \notin Q$ for $i = 1, 2$. ♠

LEMMA 1.33. *If M, N are R-modules, then* $\mathrm{Ass}(M \oplus N) = \mathrm{Ass}(M) \cup \mathrm{Ass}(N)$.

LEMMA 1.34. *If N_1, N_2 are $\mathfrak{p}$-primary submodules of M, then $N_1 \cap N_2$ is a $\mathfrak{p}$-primary submodule.*

PROOF. Set $N = N_1 \cap N_2$. There is an inclusion $M/N \hookrightarrow M/N_1 \oplus M/N_2$. Hence using Lemma 1.33 we get

$$\mathrm{Ass}(M/N) \subset \mathrm{Ass}(M/N_1 \oplus M/N_2) = \mathrm{Ass}(M/N_1) \cup \mathrm{Ass}(M/N_2) = \{\mathfrak{p}\}.$$

Therefore $\mathrm{Ass}(M/N) = \{\mathfrak{p}\}$. ♠

THEOREM 1.35. *(Emmy Noether) Let M be an R-module. Any proper submodule $N \subsetneq M$ has an irredundant primary decomposition.*

PROOF. First we claim that every submodule N can be expressed as the intersection of finitely many irreducible submodules of M. Let $\mathcal{F}$ be the family of submodules of M such that the claim is false. Then $\mathcal{F} \neq \emptyset$. By Theorem 1.1, $\mathcal{F}$ has a maximal element that we denote by N. Since N is not irreducible, we can write $N = N_1 \cap N_2$, for some submodules N_1, N_2 strictly containing N. By the maximality of N we get that N_1 and N_2 can be written as an intersection of irreducible submodules, and it follows that N is too, a contradiction. Thus $\mathcal{F} = \emptyset$. Hence the result follows from Lemma 1.32 and Lemma 1.34. ♠

LEMMA 1.36. *Let M be an R-module, then*

$$\bigcap_{\mathfrak{p} \in \mathrm{Ass}(M)} \mathfrak{p} = \bigcap_{\mathfrak{p} \in \mathrm{Supp}(M)} \mathfrak{p} = \mathrm{rad}(\mathrm{ann}(M))$$

.

PROOF. Since the minimal associated primes are the same as the minimal supporting primes, the two intersections are equal.
Now, suppose that $a \notin \mathrm{rad}(\mathrm{ann}(M))$, then there is a prime ideal $\mathfrak{p}$ containing $\mathrm{ann}(M)$ so that $a \notin \mathfrak{p}$. But $\mathrm{ann}(M) \subset \mathfrak{p}$, implies that $M_\mathfrak{p} \neq 0$, so $\mathfrak{p} \in \mathrm{Supp}(M)$, thus $a \notin \bigcap_{\mathfrak{p} \in \mathrm{Supp}(M)} \mathfrak{p}$. Note that $\mathrm{ann}(M) \subset \mathrm{ann}(x)$ for all $x \in M$. In particular, $\mathrm{ann}(M)$ is contained in every associated prime $\mathfrak{p}$. But then $\mathrm{rad}(\mathrm{ann}(M))$ is also contained in each such $\mathfrak{p}$. ♠

COROLLARY 1.37. *If R is a Noetherian ring and I a proper ideal of R, then I has an irredundant primary decomposition $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ such that $\mathfrak{q}_i$ is a $\mathfrak{p}_i$-primary ideal and $\mathrm{Ass}_R(R/I) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$.*

PROOF. Let $(0) = I/I = (\mathfrak{q}_1/I) \cap \cdots \cap (\mathfrak{q}_r/I)$ be an irredundant decomposition of the zero ideal of R/I. Then $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ and $\mathfrak{q}_i/I$ is $\mathfrak{p}_i$-primary and $\mathrm{Ass}_R((R/I)/(\mathfrak{q}_i/I)) = \mathrm{Ass}(R/\mathfrak{q}_i) = \{\mathfrak{p}_i\}$. Let us show that $\mathfrak{q}_i$ is a primary ideal. If $xy \in \mathfrak{q}_i$ and $x \notin \mathfrak{q}_i$, then y is a zero-divisor of $R/\mathfrak{q}_i$, but $\mathcal{Z}(R/\mathfrak{q}_i) = \mathfrak{p}_i$, hence by above lemma $y \in \mathfrak{p}_i = \mathrm{rad}(\mathrm{ann}(R/\mathfrak{q}_i)) = \mathrm{rad}(\mathfrak{q}_i)$ and y^n is in $\mathfrak{q}_i$ for some $n > 0$. ♠

COROLLARY 1.38. *If $N \subsetneq M$ and $N = N_1 \cap \cdots \cap N_r$ is an irredundant primary decomposition of N with $\mathrm{Ass}_R(M/N_i) = \{\mathfrak{p}_i\}$, then $\mathrm{Ass}_R(M/N) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$, and $\mathrm{ann}(M/N_i)$ is a $\mathfrak{p}_i$-primary ideal for all i.*

PROOF. There is a natural monomorphism

$$M/(N_1 \cap \cdots \cap N_r) \hookrightarrow (M/N_1) \oplus \cdots \oplus (M/N_r).$$

Hence $\mathrm{Ass}(M/N) \subset \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$. There are natural monomorphisms

$$(N_2 \cap \cdots \cap N_r)/N \hookrightarrow M/N_1; \quad (N_2 \cap \cdots \cap N_r)/N \hookrightarrow M/N.$$

Since $\mathrm{Ass}(M/N_1) = \{\mathfrak{p}_1\}$ we get $\mathfrak{p}_1 \in \mathrm{Ass}(N_2 \cap \cdots \cap N_r/N)$, thus $\mathfrak{p}_1 \in \mathrm{Ass}(M/N)$. Similarly one can show that any other $\mathfrak{p}_i$ is an associated prime of M/N. This proves the asserted equality.

By Corollary 1.36 we have $\mathrm{rad}(\mathrm{ann}(M/N_i)) = \mathfrak{p}_i$. Thus it suffices to show that $I = \mathrm{ann}(M/N_i)$ is a primary ideal. Assume that $xy \in I$ for some $x, y \in R$. If x is not in I, then xM is not contained in N_i. Pick $m \in M$ such that $xm \notin N_i$. Since $y(xm) \subset N_i$, we get that y is a zero divisor of M/N_i, but the zero divisors of this module are precisely the elements of $\mathfrak{p}_i$ according to Lemma 1.25. Hence $y^r \in I$ for some r. ♠

DEFINITION 1.39. Let M be an R-module, let $N \subsetneq M$ be a proper submodule, and let $N = N_1 \cap \cdots \cap N_r$ be a *primary decomposition* of N with $\mathrm{Ass}_R(M/N_i) = \{\mathfrak{p}_i\}$ for all i. The set of *associated primes* of this primary decomposition is $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$.

REMARK 1.40. By Lemma 1.34 any primary decomposition can be refined to one that is irredundant. A submodule N of M may have different primary decompositions but according to Corollary 1.38 the set of associated primes in any primary decomposition of N is the same.

THEOREM 1.41. *If I is an ideal of S and $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$ is an irredundant primary decomposition with $\mathrm{rad}(\mathfrak{q}_i) = \mathfrak{p}_i$, then the set of zero-divisors $\mathcal{Z}(S/I)$ of S/I is given by*

$$\mathcal{Z}(S/I) = \bigcup_{i=1}^{m} \mathfrak{p}_i,$$

and $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ are the associated primes of I.

PROOF. It follows from Lemma 1.25 and Corollary 1.38. ♠

LEMMA 1.42 (Prime Avoidance). *Let $I, \mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ be ideals of a ring R (not necessarily Noetherian) and suppose that at most two of the $\mathfrak{p}_i$ are not prime, say $\mathfrak{p}_1$, $\mathfrak{p}_2$. If*

$$I \subset \bigcup_{i=1}^{n} \mathfrak{p}_i,$$

then there exists i, $1 \leqslant i \leqslant n$, such that $I \subset \mathfrak{p}_i$.

PROOF. Throwing away superfluous $\mathfrak{p}$'s, we may suppose that $I \subset \bigcup_{i=1}^{n} \mathfrak{p}_i$, but $I \nsubseteq \bigcup_{j\neq i} \mathfrak{p}_i$. Reasoning by contradiction, assume $I \nsubseteq \mathfrak{p}_i$ for all i. We can choose $u_t \in I \setminus \bigcup_{i\neq t} \mathfrak{p}_i$. Since $I \subset \bigcup_{i=1}^{n} \mathfrak{p}_i$, $u_t \in \mathfrak{p}_t$. Also note that $u_1 + u_2$ cannot be in $\mathfrak{p}_1$ neither $\mathfrak{p}_2$, therefore $n \neq 2$. Set

$$\mathcal{T} = \{t : 2 < t \leq n, \text{ such that } u_1 + u_2 \notin \mathfrak{p}_t\},$$

and define $w := \prod_{t\in\mathcal{T}} u_t$. We claim that $u_1 + u_2 + w \notin \bigcup_{i=1}^{n} \mathfrak{p}_i$. If there is j such that $u_1 + u_2 + w \in \mathfrak{p}_j$ for some j, then

Case (I): $u_1 + u_2 \notin \mathfrak{p}_j$. Then $j \in \mathcal{T}$, thus $w \in \mathfrak{p}_j$ since by definition u_j appear in w, as $u_1 + u_2 + w \in \mathfrak{p}_j$, $u_1 + u_2 \in \mathfrak{p}_j$, a contradiction.

Case (II): $u_1 + u_2 \in \mathfrak{p}_j$. Then $j \notin \mathcal{T}$, thus $w \notin \mathfrak{p}_j$ since if $w = \prod_{t'\neq j} u_{t'} \in \mathfrak{p}_j$, then $u_{t'\neq j} \in \mathfrak{p}_j$, absurd. As $u_1 + u_2 + w \in \mathfrak{p}_j$, then $w \in \mathfrak{p}_j$, a contradiction.
Therefore, $u_1 + u_2 + w \notin \bigcup_{i=1}^{n} \mathfrak{p}_i$, a contradiction since $u_1 + u_2 + w \in I$.
If $\mathcal{T} = \emptyset$, that is, if $u_1 + u_2 \in \mathfrak{p}_i$ for all $i > 2$, then, $u_1u_2 + u_1 + u_2 \in \mathfrak{p}_k$ for some $k > 2$. But this implies $u_1 \in \mathfrak{p}_k$ or $u_2 \in \mathfrak{p}_k$, a contradiction.
In conclusion, $I \subset \mathfrak{p}_1$, absurd. ♠

LEMMA 1.43. *Let R be a ring (not necessarily Noetherian). If $a \in \mathfrak{p}$ with $\mathfrak{p}$ a minimal prime, then a is a zero divisor.*

PROOF. Since $\mathfrak{p}$ is a minimal prime, then $\mathfrak{p}R_\mathfrak{p}$ is the only prime ideal in $R_\mathfrak{p}$. As the nilradical of a ring is the intersection of the prime ideals then $a/1 \in \mathfrak{p}R_\mathfrak{p}$ is nilpotent, that is, $(a/1)^n = 0$, for some $n \geq 0$. Therefore, there is $b \in R \setminus \mathfrak{p}$ such that $ba^n = 0$. This implies that a is zero divisor by induction on n. ♠

LEMMA 1.44. *Let R be a reduced ring, that is, the nilradical is zero, then every zero divisor is contained in a minimal prime of R. Thus the set of zero divisors of R is the union of the minimal prime ideals of R.*

PROOF. Note that the nilradical of R is the intersection of the minimal prime ideals because every prime ideal contains a minimal prime. Thus the intersection of all minimal primes is 0. If $a \in R$ is a zero divisor such that is not contained in any minimal prime, then

there is $b \neq 0$ in R such that $ab = 0$. But this implies that b is contained in every minimal prime, a contradiction. ♠

DEFINITION 1.45. Let R be a ring and let S be the set of nonzero divisors of R. The ring $S^{-1}R$ is called the *total ring of fractions* of R. If R is a domain, $S^{-1}R$ is the *field of fractions* of R.

PROPOSITION 1.46. *Let R be a ring and let K be the total ring of fractions of R. If R is reduced, that is, the nilradical is zero, then K is a direct product of fields.*

PROOF. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be the minimal primes of R and $S = R \setminus \bigcup_{i=1}^{r} \mathfrak{p}_i$. Since every element in K is either a unit or a zero divisor, then any proper ideal I of K must be consist of zero divisors. Since the set of zero divisors of K is the union of the minimal prime ideals $\mathfrak{p}_i K$ (because K is reduced). By prime avoidance Lemma 1.42, I must be contained in some $\mathfrak{p}_i K$. Thus the ideals $\mathfrak{p}_i K$ are the maximal ideals of K, whose intersection is zero. By the Chinese remainder theorem **[Vil15**, p. 74] applied to K we have

$$K \simeq S^{-1}R/\mathfrak{p}_1 S^{-1}R \times \cdots \times S^{-1}R/\mathfrak{p}_r S^{-1}R,$$

but $S^{-1}R/\mathfrak{p}_i S^{-1}R \simeq (\overline{S})^{-1}(R/\mathfrak{p}_i)$ where $\overline{S}$ is the multiplicative closed subset in $R/\mathfrak{p}_i$ induced by S and $(\overline{S})^{-1}(R/\mathfrak{p}_i)$ is a field. ♠

LEMMA 1.47. *Let M be an R-module and L an ideal of R. If $LM = M$, then there is $x \in R$ such that $x \equiv 1 \pmod{L}$ and $xM = (0)$.*

PROOF. Let $M = R\alpha_1 + \cdots + R\alpha_n$, $\alpha_i \in M$. As $LM = M$, there are b_{ij} in L such that $\alpha_i = \sum_{j=1}^{n} b_{ij}\alpha_i$. Set $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $H = (b_{ij}) - \mathbb{I}$, where $\mathbb{I}$ is the identity matrix. Since $H\alpha^t = 0$ and $H.\mathrm{adj}(H) = \det(H)\mathbb{I}$, one concludes $\det(H)\alpha_i = 0$ for all i. Hence $xM = (0)$ and $x \equiv 1 (\mathrm{mod}\, L)$, where $x = \det(H)$. ♠

DEFINITION 1.48. The *Jacobson radical* of a ring R is the intersection of all the maximal ideals of R .

Nakayama's Lemma is a series of results saying that finitely generated modules are not so very different to finite dimensional vector spaces.

THEOREM 1.49 (Nakayama's Lemma). *Let R be a ring, I be an ideal contained in the Jacobson radical of R and M an R-module.*

(a) If $IM = M$, then $M = 0$.

(b) If $N \subset M$ is a submodule such that $M = IM + N$, then $N = M$.

(c) If $m_1, \dots, m_n \in M$ have images in M/IM that generate it as an R-module, then the m_i generate M as an R-module.

If M is a module over a local ring $(R, \mathfrak{m}, k)$, M/mM is a vectorial space on $k = R/m$. This is called *reduction to linear algebra*. A consequence of Nakayama's lemma is the notion of the *minimum number of generators*:
Let $\{\alpha_1, \dots, \alpha_q\}$ be a minimal generating set for M and $\overline{\alpha}_i = \alpha_i + \mathfrak{m}M$. Note that $\{\overline{\alpha}_1, \dots, \overline{\alpha}_q\}$ is a basis for $M/\mathfrak{m}M$ as a k-vector space. Otherwise some $\overline{\alpha}_i$ would be expressed as a linear combination of the $\overline{\alpha}_j$, with $j \neq i$. Thus, $\{\overline{\alpha}_1, \dots, \overline{\alpha}_q\} \setminus \{\overline{\alpha}_i\}$ is a set generating to M/IM. By Nakayama's lemma $\{\alpha_1, \dots, \alpha_q\} \setminus \{\alpha_i\}$ generates M, contradicting the minimality of $\{\alpha_1, \dots, \alpha_q\}$. Thus $q = \dim_k(M/mM)$.

DEFINITION 1.50. The *minimum number of generators* of a R-module M with (R, m, k) a local ring is $\mu_R(M) := \dim_k(M/mM)$. The *embedding dimension* of R, denoted Emdim(R), is the minimal number of generators for m.

COROLLARY 1.51. *If M is a module over a local ring $(R, \mathfrak{m}, k)$, then*

$$\mu_R(M) = \dim_k(M/\mathfrak{m}M), \text{ where } k = R/\mathfrak{m}.$$

REMARK 1.52. The embedding dimension is the smallest dimension into which we can embed R into a smooth space. But for singular varieties this is not the dimension we want. The above definition has no sense when R is no a local ring: Let $R = \mathbb{Z}$, $M = \mathbb{Z}$, then the sets $B = \{2, 3\}$ and $B' = \{1\}$ generate to $\mathbb{Z}$ and no other generates it.

Modules of finite length. An R-module M has *finite length* if there is a *composition series*

$$(0) = M_0 \subset M_1 \subset \cdots \subset M_n = M, \tag{1.1.1}$$

where M_i/M_{i-1} is a non-zero *simple module* , that is, M_i/M_{i-1} has no proper submodules other than (0) for all i. The number n is independent of the composition series [**Bla11**, Proposition 4.2.16] and is called the *length* of M; it is usually denoted by $\ell_R(M)$ or simply $\ell(M)$.
The concept of length should be understood as the generalization of the dimension of M as vector space: Assume that R is a field k and M a vector space over k of dimension d. Let $\{u_1, \dots, u_d\}$ be a basis for M. Consider the subspaces $M_0 = \langle 0 \rangle, M_1 = \langle u_1 \rangle \dots, M_i = \langle u_1, \dots, u_i \rangle$, for $1 \leq i \leq d$. Then:

(1) $M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_d = M$.
(2) If $M_{i+1}/M_i \cong \langle u_{i+1} \rangle \cong k$, and k is simple as k-module.

Therefore, $\ell_k(M) = d = \dim_K(M)$.

REMARK 1.53. M is a simple R-module if and only if $M \cong R/m$, where $m \subset R$ is a maximal ideal: If M is simple take $u \neq 0$ in M, then $M = {}_R\langle u \rangle$. Define the R-homomorphism $h : R \to M$ as $r \mapsto ru$. Clearly h is surjective. Set $I = \ker(h)$, then h induces an isomorphism $\overline{h} : R/I \to M$. By correspondence theorem, the submodules of R/I are in correspondence with the ideals of R that contains I, but R/I is simple, thus there is not proper ideal that contains I, therefore I is maximal. Conversely is clear.

PROPOSITION 1.54. [**AM94**, Proposition 6.9] *If $0 \to M' \to M \to M'' \to 0$ is an exact sequence of R-modules, then $\ell_R(M) < \infty$ if and only if $\ell_R(M') < \infty$ and $\ell_R(M'') < \infty$. In that case, we have*

$$\ell_R(M) = \ell_R(M') + \ell_R(M'').$$

An R-module M is called *Artinian* if M satisfies the *descending chain condition* for submodules; that is, for every chain of submodules of M

$$\cdots \subset N_{n+1} \subset N_n \subset \cdots \subset N_2 \subset N_1 \subset N_0 = M$$

there exists an integer k such that $N_i = N_k$ for every $i \geq k$. It is easy to verify that M is Artinian if and only if any family $\mathcal{F}$ of submodules of M partially ordered by inclusion has a minimal element, that is, there is $N \in \mathcal{F}$ such that if $N_i \subset N$ and $N_i \in \mathcal{F}$, then $N = N_i$.
From Proposition 1.2 is clear that if $0 \to L \xrightarrow{\iota} M \xrightarrow{\rho} N \to 0$ is a short exact sequence of R-modules. Then M is Artinian if and only if L and N are Artinian.

PROPOSITION 1.55. *Let M be an R-module. Then $\ell_R(M) < \infty$ if and only if M is Noetherian and Artinian.*

PROOF. $\Rightarrow$) We prove by induction on $n = \ell_R(M)$. If $n = 0$, then $M = (0)$, so M is trivially Noetherian and Artinian.
If $n > 0$: Case (I): M is simple. Then we have that $M \cong R/m$, with $m \subset R$ maximal ideal (remark 1.53). Thus M is a field that is clearly Noetherian and Artinian.

Case (II): M is not simple. Then there is a submodule $N \neq (0)$ of M. By the exact sequence $0 \to N \to M \to M/N \to 0$ and using Proposition 1.54 we obtain $\ell_R(M) = \ell_R(N) + \ell_R(M/N)$ with $\ell_R(N), \ell_R(M/N) < \ell_R(M)$. By induction hypothesis N and M/N are Noetherian and Artinian. Again by the exact sequence above M is Noetherian and Artinian.

$\Leftarrow$) We construct a finite composition series as follows. Set $M_0 = M$. Consider the family $\mathcal{F}_1$ of proper submodules of M and pick a maximal element M_1, which exists because M is Noetherian. By induction consider the family $\mathcal{F}_i$ of proper submodules of M_{i-1} and pick a maximal element M_{i+1}. Notice that this process must stop at the zero module because M is Artinian. ♠

LEMMA 1.56. *Let M be a k-vector space. Then, M Artinian if and only if M is of finite dimension as a k-vector space.*

PROOF. Assume that M is Artinian and $\dim_k(M) = \infty$. Let $\mathcal{B} \subset M$ be an infinite linearly independent set, say $\mathcal{B} = \{\alpha_1, \ldots, \alpha_i, \ldots, \}$. Then

$$\cdots \subsetneq k(\mathcal{B} \setminus \{\alpha_1, \ldots, \alpha_i\}) \subsetneq \cdots \subsetneq k(\mathcal{B} \setminus \{\alpha_1, \alpha_2\}) \subsetneq k(\mathcal{B} \setminus \{\alpha_1\}) \subsetneq M,$$

a contradiction. If M has finite dimension as a k-vector space. Then M is Artinian. Indeed, if $M_1 \supset M_2 \supset \cdots$ is a descending chain of submodules of M, then each M_i is a subspace of the k-vector space M, necessarily of finite dimension, so this chain is stationary. ♠

PROPOSITION 1.57. *If $0 \to M' \to M \to M'' \to 0$ is an exact sequence of modules over a ring R, then* $\dim(M) = \max\{\dim(M'),\ \dim(M'')\}$.

PROOF. Set $d = \dim(M)$, $d' = \dim(M')$ and $d'' = \dim(M'')$. First note that $d = \dim(R/\mathfrak{p})$ for some prime $\mathfrak{p}$ containing $\operatorname{ann}(M)$, by Proposition 1.27 we obtain $M_\mathfrak{p} \neq (0)$. Therefore using Lemma 1.21 one has $M'_\mathfrak{p} \neq (0)$ or $M''_\mathfrak{p} \neq (0)$, thus either $\mathfrak{p}$ contains $\operatorname{ann}(M')$ or $\mathfrak{p}$ contains $\operatorname{ann}(M'')$. This proves $d \leq \max\{d', d''\}$. On the other hand $\operatorname{ann}(M)$ is contained in $\operatorname{ann}(M') \cap \operatorname{ann}(M'')$ and consequently $\max\{d', d''\} \leq d$. ♠

PROPOSITION 1.58. *If M is an R-module, then M has finite length if and only if every prime ideal in* $\operatorname{Supp}(M)$ *is a maximal ideal.*

PROOF. $\Rightarrow$) Let $\{M_i\}_{i=0}^n$ be a composition series as in Eq. (1.1.1). By remark 1.53 we have isomorphisms $M_i/M_{i-1} \cong R/\mathfrak{p}_i$ where $\mathfrak{p}_i$ are maximal ideals for all i and also

$$\operatorname{Supp}(M) = \operatorname{Supp}(M_0) \cup \operatorname{Supp}(M_1/M_0) \cup \cdots \cup \operatorname{Supp}(M_n/M_{n-1}).$$

Note that

$$\begin{aligned} \operatorname{Ass}(M_i/M_{i-1}) &= \operatorname{Ass}(R/\mathfrak{p}_i) \\ &= \{\mathfrak{p}_i\} \\ &\subset \operatorname{Supp}(M_i/M_{i-1}) \\ &= V(\operatorname{ann}(M_i/M_{i-1})) \end{aligned}$$

$$= V(\operatorname{ann}(R/\mathfrak{p}_i))$$
$$= V(\mathfrak{p}_i).$$

As $\mathfrak{p}_i$ is maximal, $\operatorname{Supp}(M_i/M_{i-1}) = \{\mathfrak{p}_i\}$. Thus we obtain that $\operatorname{Supp}(M)$ is equal to $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$.

$\Leftarrow$) There is a filtration $(0) = M_0 \subset M_1 \subset \cdots \subset M_n = M$ of submodules and prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ of R such that $M_i/M_{i-1} \simeq R/\mathfrak{p}_i$ for all i (see Theorem 1.22). By the proof of Corollary 1.24 one has

$$\operatorname{Ass}(M) \subset \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \subset \operatorname{Supp}(M).$$

Thus the filtration above is a composition series because $\mathfrak{p}_i$ is a maximal ideal for all i. ♠

THEOREM 1.59. *Let R be a ring. Then R is Artinian if and only if*

(a) *R is Noetherian, and*

(b) *every prime ideal of R is maximal.*

PROOF. $\Rightarrow$) First we show that $\ell_R(R) < \infty$. Let

$$\mathcal{F} = \{\mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_s \,|\, \mathfrak{m}_i \in \operatorname{Max}(R),\ \forall\, i\},$$

we do not require $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$ to be distinct. The family $\mathcal{F}$ has a minimal element that we denote by $I = \mathfrak{m}_1 \cdots \mathfrak{m}_r$. We claim that $I = (0)$. Assume that $I \neq (0)$. Clearly $I^2 \in \mathcal{F}$ and $I^2 \subset I$, thus $I = I^2$. Consider the family

$$\mathcal{G} = \{J \,|\, J \text{ is an ideal; } JI \neq (0)\}.$$

This family is non-empty because $I \in \mathcal{G}$. Since R is Artinian, there exists a minimal element J of $\mathcal{G}$. Then

$$(0) \neq JI = JI^2 = (JI)I \ \Rightarrow\ JI \in \mathcal{G}.$$

Since $IJ \subset J$, we get $J = IJ$. Notice that J is a principal ideal. Indeed since $IJ \neq (0)$, there is $x \in J$ such that $xI \neq (0)$. Hence $(x) \in \mathcal{G}$, and consequently $J = (x)$. If $\mathfrak{m}$ is a maximal ideal of R, then $\mathfrak{m}I \in \mathcal{F}$ and $\mathfrak{m}I \subset I$. Hence $\mathfrak{m}I = I$ and $I \subset \mathfrak{m}$. Thus I is contained in the Jacobson radical of I. From the equality $(x) = J = IJ = Ix$, we obtain that $x = \lambda x$ for some $\lambda \in I$. As $x(1-\lambda) = 0$, with $1-\lambda$ a unit of R, we get $x = 0$. A contradiction to $J \neq (0)$. This proves that $I = (0)$. Set $I_k = \mathfrak{m}_1 \cdots \mathfrak{m}_k$ for $1 \leq k \leq r$ and consider the filtration

$$(0) = I = I_r \subset I_{r-1} \subset I_{r-2} \subset \cdots \subset I_1 \subset I_0 = R.$$

Observe that I_i/I_{i+1} is an $R/\mathfrak{m}_{i+1}$ vector space since it is an R-module and is annihilated by $\mathfrak{m}_{i+1}$. The vector space I_i/I_{i+1} is Artinian because the subspaces of I_i/I_{i+1} correspond

bijectively to the intermediate ideals of $I_{i+1} \subset I_i$. Therefore by Lemma 1.56 we get that I_i/I_{i+1} has finite length as an $R/\mathfrak{m}_{i+1}$ vector space and consequently as an R-module. By a repeated application of Proposition 1.54 we have $\ell_R(R) = \sum_{i=0}^{r} \ell_R(I_i/I_{i+1})$. Hence $\ell_R(R) < \infty$. Therefore R is Noetherian by Proposition 1.55 and (a) holds. To prove (b) take a prime $\mathfrak{p}$ of R. Then $R/\mathfrak{p}$ is an Artinian domain. Let $x \neq 0$ in $R/\mathfrak{p}$. Then the chain $(x) \supset (x^2) \supset \cdots$ becomes stationary, say at t. Thus $(x^t) = (x^{t+1})$, it follows that $x^t = x^{t+1}y$ for some $y \in R/\mathfrak{p}$. Therefore $xy = \overline{1}$. Thus $R/\mathfrak{p}$ is a field.

$\Leftarrow$) Assume that R is not Artinian, then $\ell_R(R) > \infty$. Let

$$\mathcal{F} = \{I \subset R |\ I \text{ is an ideal; } \ell_R(R/I) > \infty\},$$

Clearly $\mathcal{F} \neq \emptyset$. As R is Noetherian, $\mathcal{F}$ has a maximal, say $\mathfrak{m}$. I claim that $\mathfrak{m}$ is prime ideal. Let $ab \in \mathfrak{m}$ and suppose that $a, b \notin \mathfrak{m}$, then we have the following exact sequences of R-modules

$$0 \to R/(\mathfrak{m} : a) \xrightarrow{a} R/\mathfrak{m} \to R/(\mathfrak{m} + (a)) \to 0,$$

Since $a, b \in \mathfrak{m}$, then $\mathfrak{m} \subsetneq (\mathfrak{m} : a)$ and $\mathfrak{m} \subsetneq \mathfrak{m} + (a)$; thus $\ell_R((\mathfrak{m} : a)) < \infty$ and $\ell_R(\mathfrak{m} + (a)) < \infty$. Thus, by Proposition 1.54 we have $\ell_R(R/\mathfrak{m}) < \infty$, a contradiction. Hence $R/\mathfrak{m}$ is a field since $\mathfrak{m}$ is maximal ideal. Therefore $\ell_R(R/\mathfrak{m}) < \infty$, a contradiction. Thus R is Artinian. ♠

COROLLARY 1.60. *An artinian ring R has a finite number of prime ideals, thus maximals. In particular* $\dim(R) = 0$.

PROOF. If it had an infinite number of prime ideals we could find an infinite sequence $\mathfrak{m}_1, \mathfrak{m}_2, \ldots$ of different maximal ideals.
claim: $\mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_n$ is a proper submodule of $\mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_{n-1}$.
proof of the claim: Since the ideals $\mathfrak{m}_i$ are maximal we can for each $i = 1, 2, \ldots, n-1$ find an element $a_i \in \mathfrak{m}_i \setminus \mathfrak{m}_n$. Assume that $\mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_{n-1} = \mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_n$. Then $a_1a_2 \cdots a_{n-1} \in \mathfrak{m}_n$, a contradiction.
Then it follows that we have an infinite chain $\mathfrak{m}_1 \supset \mathfrak{m}_1 m_2 \supset \cdots$ of ideals in R. A contradiction. Therefore R has only a finite number of maximal ideals. ♠

COROLLARY 1.61. *If R is an Artinian ring, then R is a finite product of local Artinian rings.*

PROOF. Let $\mathrm{Spec}(R) = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_t\}$. We know that (0) has an irredundant primary decomposition $(0) = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t$, where $\mathfrak{q}_i$ is a $\mathfrak{m}_i$-primary.
$\mathfrak{q}_i + \mathfrak{q}_j = R$: if $\mathfrak{q}_i + \mathfrak{q}_j \subsetneq R$, then $\mathfrak{q}_i + \mathfrak{q}_j \subset \mathfrak{m}_k$ for some k. Then $\mathfrak{q}_i \subset \mathfrak{m}_k$, implying $\mathrm{rad}(\mathfrak{q}_i) = \mathfrak{m}_i \subset \mathfrak{m}_k$, therefore $i = k$. Thus $\mathfrak{q}_j \subset \mathfrak{m}_i$, then $\mathfrak{m}_j \subset \mathfrak{m}_i$, a contradiction.

By Chinese residue theorem

$$R \simeq R/(0) = R/\bigcap_{i=1}^{t} \mathfrak{q}_i \cong R/\mathfrak{q}_1 \times \cdots \times R/\mathfrak{q}_t.$$

Note that each $R/\mathfrak{q}_i$ is a local ring, since $\mathfrak{q}_i \subset \mathfrak{m}_i$ and $\mathfrak{q}_i \nsubseteq \mathfrak{m}_j$ with $i \neq j$, thus $\overline{m}_i$ is the unique maximal ideal of $R/\mathfrak{q}_i$. ♠

DEFINITION 1.62. Let $\mathfrak{p} \subset R$ be a prime ideal. The n-th *symbolic power* $\mathfrak{p}^{(n)}$ of $\mathfrak{p}$ is the contraction of $\mathfrak{p}^n R_{\mathfrak{p}}$ to R, equivalently

$$\mathfrak{p}^{(n)} = \{r \in R : sr \in \mathfrak{p}^n \text{ for some } s \in R \setminus \mathfrak{p}\}.$$

Note that $\mathfrak{p}^{(1)} = \mathfrak{p}$, and $\mathfrak{p}^{(n)} = \mathfrak{p}^n$ when $\mathfrak{p}$ is a maximal ideal, but in general $\mathfrak{p}^n \subsetneq \mathfrak{p}^{(n)}$ [**Mat80**, Chapter 2.8.H]. It is easy to see that $\mathfrak{p}^{(n)}$ is the smaller $\mathfrak{p}$-primary ideal containing $\mathfrak{p}^n$.

THEOREM 1.63. (Principal Ideal Theorem) *If $(x) \subsetneq R$ is a principal ideal of a ring R and $\mathfrak{p}$ is a minimal prime of (x), then* $\operatorname{ht}(\mathfrak{p}) \leq 1$. *If x is not a zero divisor of R, then* $\operatorname{ht}(\mathfrak{p}) = 1$.

PROOF. After of localize at $\mathfrak{p}$ we have a local ring $(R_{\mathfrak{p}}, \mathfrak{p}R_{\mathfrak{p}})$ with $\mathfrak{p}R_{\mathfrak{p}}$ a minimal prime of $(x/1)$. Therefore we may assume that R is local with maximal ideal $\mathfrak{p}$. For any $\mathfrak{q} \in \operatorname{Spec}(R)$ with $\mathfrak{q} \subsetneq \mathfrak{p}$, we must show that $\operatorname{ht}(\mathfrak{q}) = 0$. Let $\mathfrak{q}^{(i)}$ be the i-th symbolic power of $\mathfrak{q}$. Since $R/(x)$ is Noetherian and $\dim(R/(x)) = 0$, by Theorem 1.59, $R/(x)$ is Artinian. Therefore the descending chain of ideals

$$((x) + \mathfrak{q}^{(1)}) \supset ((x) + \mathfrak{q}^{(2)}) \supset \cdots$$

stabilizes, that is, there is $r \in \mathbb{N}_+$ such that

$$(x) + \mathfrak{q}^{(r)} = (x) + \mathfrak{q}^{(r+1)}. \tag{1.1.2}$$

We claim that $\mathfrak{q}^{(r)} = \mathfrak{p}\mathfrak{q}^{(r)} + \mathfrak{q}^{(r+1)}$. The inclusion "$\supset$" is clear. To show the reverse inclusion take $f \in \mathfrak{q}^{(r)}$. Then, by Eq. (1.1.2), we can write $f = ax + g$, where $a \in R$ and $g \in \mathfrak{q}^{(r+1)}$. Thus $ax \in \mathfrak{q}^{(r)}$. If $a \notin \mathfrak{q}^{(r)}$, then $x \in \operatorname{rad}(\mathfrak{q}^{(r)}) = \mathfrak{q}$, a contradiction by the minimality of $\mathfrak{p}$. Hence $\mathfrak{q}^{(r)} \subset x\mathfrak{q}^{(r)} + \mathfrak{q}^{(r+1)} \subset \mathfrak{p}\mathfrak{q}^{(r)} + \mathfrak{q}^{(r+1)}$. This proves the claim. By Nakayama's lemma we obtain $\mathfrak{q}^{(r)} = \mathfrak{q}^{(r+1)}$. Hence $\mathfrak{q}^r R_{\mathfrak{q}} = \mathfrak{q}^{r+1} R_{\mathfrak{q}}$. Again by Nakayama's lemma one has $\mathfrak{q}^r R_{\mathfrak{q}} = 0$, which implies that $\operatorname{ht}(\mathfrak{q}) = \dim(R_{\mathfrak{q}}) = 0$. Thus $\operatorname{ht}(\mathfrak{p}) \leqslant 1$. If x is not a zero divisor of R, then $\operatorname{ht}(\mathfrak{p}) = 1$; because if $\operatorname{ht}(\mathfrak{p}) = 0$, $\mathfrak{p}$ is a minimal prime, thus $\mathfrak{p}$ consists of zero divisors (see Lemma 1.25 and Proposition 1.27), a contradiction. ♠

LEMMA 1.64. *Let R be a ring, and $x \in R$. Then for any chain of prime ideals $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ of R such that $x \in \mathfrak{p}_n$ and $n \geq 1$, there exists a chain of prime ideals $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_n = \mathfrak{p}_n$ with $a \in \mathfrak{q}_1$.*

PROOF. Let us show this assertion by induction on n. It is trivial for $n = 1$. Let us suppose that $n \geq 2$. We may assume that $x \notin \mathfrak{p}_{n-1}$ (otherwise we apply the induction hypothesis to the sequence $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_{n-1}$). Set $S = (R/\mathfrak{p}_{n-2})_{\overline{\mathfrak{p}_n}}$, $\mathfrak{q} = \overline{\mathfrak{p}_n}S$, and $\mathfrak{a} = \overline{\mathfrak{p}_{n-1}}S$. Then S is a local ring with maximal ideal $\mathfrak{q}$, with $\overline{x}/1 \in \mathfrak{q}$, and $\overline{x}/1 \notin \mathfrak{a}$.

$$\begin{array}{ccccc}
R & \longrightarrow & R/\mathfrak{p}_{n-2} & \longrightarrow & S \\
\vert & & \vert & & \vert \\
\mathfrak{p}_n & \longrightarrow & \overline{\mathfrak{p}_n} & \longrightarrow & \mathfrak{q} \\
\vert & & \vert & & \vert \\
a & & \overline{x} & & \overline{x}/1 \\
\vert & & \vert & & \vert \\
\mathfrak{p}_{n-1} & \longrightarrow & \overline{\mathfrak{p}_{n-1}} & \longrightarrow & \mathfrak{a} \\
\vert & & \vert & & \vert \\
\mathfrak{p}_{n-2} & \longrightarrow & 0 & \longrightarrow & 0 \\
\vert & & & & \\
\cdot & & & &
\end{array}$$

Note that $\mathfrak{q}$ is not minimal prime over $(\overline{x}/1)$, otherwise, by Krull's principle ideal theorem we have $\mathrm{ht}(\mathfrak{q}) \leq 1$, but $\mathrm{ht}(\mathfrak{q}) \geq 2$, since $(0) \subsetneq \mathfrak{a} \subsetneq \mathfrak{q}$ is a chain of prime ideals of S. Thus there exists a prime ideal $\mathfrak{b} \subsetneq \mathfrak{q}$ such that $(\overline{x}/1) \subset \mathfrak{b}$. By correspondence theorems we get a prime ideal $\mathfrak{p}'_{n-1} \subsetneq \mathfrak{p}_n$ such that $(x) \subset \mathfrak{p}'_{n-1}$. Thus applying the induction hypothesis to $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_{n-2} \subsetneq \mathfrak{p}'_{n-1}$ we shows the assertion. ♠

DEFINITION 1.65. Let M be an R-module. A sequence $\theta_1, \ldots, \theta_n$ in R is called a *regular sequence* of M or an *M-regular sequence* if $\theta_i \notin \mathcal{Z}(M/(\theta_1, \ldots, \theta_{i-1})M)$ and $(\theta_1, \ldots, \theta_n)M \neq M$ and for all i.

THEOREM 1.66. (Generalized Principal Ideal Theorem) *Let R be a ring. If $I \subsetneq R$ is an ideal generated by $x_1, \ldots, x_m$ and $\mathfrak{p}$ is a minimal prime of I, then* $\mathrm{ht}(\mathfrak{p}) \leq m$. *If $x_1, \ldots, x_m$ is a regular sequence, then* $\mathrm{ht}(\mathfrak{p}) = m$.

PROOF. We proceed by induction on m. If $m = 1$, the result follows from Theorem 1.63. Assume that $m > 1$. Let $\mathfrak{p}_0 \subset \ldots \subset \mathfrak{p}_s = \mathfrak{p}$ be a chain of prime ideals. We want to show that $s \leq m$. Since $I \subset \mathfrak{p}$ and by Lemma 1.64 there are primes $\mathfrak{p}'_0 \subset \mathfrak{p}'_1 \subset \ldots \subset \mathfrak{p}'_{s-1} \subset \mathfrak{p}$ with $x_1 \in \mathfrak{p}'_1$. Set $S = R/(x_1)$ and let $\mathfrak{q}_i$ be the image of $\mathfrak{p}'_i$ in the quotient S for $i = 1, \ldots, s$.

Clearly $\overline{I} = (\overline{x}_2, \ldots, \overline{x}_m) \subset \mathfrak{q}_s = \mathfrak{q}$ and $\mathfrak{q}$ is a minimal prime of $\overline{I}$. By induction hypothesis we have that $\mathrm{ht}(\mathfrak{q}) \leq m-1$, thus $s-1 \leq m-1$, implying $s \leq m$.
To show the second part assume that $x_1, \ldots, x_m$ is a regular sequence and define $L_1 = (x_1, \ldots, x_{m-1})$ and $L = (x_1, \ldots, x_m)$. Since x_m is not zero divisor of R/L_1, L/L_1 is a principal ideal and $\mathfrak{p}/L_1$ is minimal over L/L_1 one has $\mathrm{ht}(\mathfrak{p}/L_1) = 1$, thus there is a prime ideal $\mathfrak{p}_0$ minimal over L_1 such that $L_1 \subset \mathfrak{p}_0 \subset \mathfrak{p}$ and consequently $\mathrm{ht}(\mathfrak{p}) \geq m$. Since $\mathrm{ht}(\mathfrak{p}) \leq m$ one gets $\mathrm{ht}(\mathfrak{p}) = m$. ♠

LEMMA 1.67. (Converse Principal Ideal Theorem) *If $\mathfrak{p}$ is a prime ideal of height $g \geq 1$ of a ring R, then there are $x_1, \ldots, x_g$ in $\mathfrak{p}$ such that $\mathfrak{p}$ is a minimal prime of $(x_1, \ldots, x_g)$.*

PROOF. By Lemma 1.42 we can pick x_1 in $\mathfrak{p}$ and not in any of the minimal primes of the ring R. Then, by Theorem 1.66, we get $\mathrm{ht}(x_1) = 1$. For $1 < k < g$ assume we have chosen $x_1, \ldots, x_k$ in $\mathfrak{p}$ such that the height of $(x_1, \ldots, x_k)$ is k. By Lemma 1.42, we can pick x_{k+1} in $\mathfrak{p}$ and x_{k+1} not in any of the minimal primes of $R/(x_1, \ldots, x_k)$, by Theorem 1.66, we get that the height of $(x_1, \ldots, x_{k+1})$ is $k+1$. ♠

THEOREM 1.68. *Let $(R, \mathfrak{m})$ be a local ring. Then*

$$\dim(R) = \min\{d \mid \exists\, x_1, \ldots, x_d \in \mathfrak{m} \text{ with } m^s \subset (x_1, \ldots, x_d) \text{ for } s \gg 0\}.$$

PROOF. Since $d = \mathrm{ht}(\mathfrak{m}) = \dim(R)$, by Lemma 1.67 there are $x_1, \ldots, x_d$ in $\mathfrak{m}$ such that $\mathfrak{m}$ is minimal over $(x_1, \ldots, x_d)$. Thus $\mathrm{rad}(x_1, \ldots, x_d) = \mathfrak{m}$, and consequently $\mathfrak{m}^s \subset (x_1, \ldots, x_d)$ for $s \gg 0$. Thus the inequality "$\geq$" holds. On the other hand if $\mathfrak{m}^s \subset (x_1, \ldots, x_d) \subset \mathfrak{m}$ for $s \gg 0$ then $\mathfrak{m}$ is minimal over $(x_1, \ldots, x_d)$, and by Theorem 1.66 one has $\mathrm{ht}(\mathfrak{m}) \leq d$. Thus the inequality "$\leq$" also holds. ♠

COROLLARY 1.69. *If $(R, \mathfrak{m})$ is a local ring and $x \in \mathfrak{m}$, then*

$$\dim(R/(x)) \geq \dim(R) - 1,$$

with equality of x is not a zero divisor of R.

PROOF. We set $d' = \dim(R/(x))$ and $d = \dim(R)$. By Theorem 1.68, there are $\overline{x_1}, \ldots, \overline{x_{d'}}$ in $R/(x)$ such that $\overline{\mathfrak{m}}^s \subset (\overline{x_1}, \ldots, \overline{x_{d'}})$ for $s \gg 0$. Hence $\mathfrak{m}^s \subset (x_1, \ldots, x_{d'}, x)$ for $s \gg 0$, and again by Theorem 1.68 we get $d \leq d' + 1$. Assume that x is not a zero divisor of R. Let

$$\mathfrak{p}_0/(x) \subsetneq \cdots \subsetneq \mathfrak{p}_{d'}/(x)$$

be a saturated chain of prime ideals of $R/(x)$ of length d' with $x \in \mathfrak{p}_i$ and $\mathfrak{p}_i \in \mathrm{Spec}(R)$ for all i. Then $\mathfrak{p}_0$ is a minimal prime of (x) and by Theorem 1.63 one has $\mathrm{ht}(\mathfrak{p}_0) = 1$. Thus $d \geq d' + 1$. ♠

EXAMPLE 1.70. If $R = K[x_1, x_2, x_3]/I$, where $I = (x_1 f, x_2 f, x_3 f)$ and $f = x_1 x_2 x_3 - 1$. Then $\dim(R) = 2$ and $\dim(R/(\overline{x_1})) = 0$. This example shows that in Corollary 1.69 it is essential to assume that the ring is local.

Polynomial rings. We want to give a formula to calculate $\dim(R[x])$ when R is Noetherian.

PROPOSITION 1.71. *Let $R[x]$ be the polynomial ring in one variable. For each ideal $I \subset R$, let $I[x]$ be the set of all polynomials in $R[x]$ with coefficients in I, then*

(a) $I[x]$ is the extension of I to $R[x]$, that is, $I[x] = IR[x]$.
(b) If $\mathfrak{p}$ is a prime ideal in R, then $\mathfrak{p}[x]$ is a prime ideal in $R[x]$.
(c) If $\mathfrak{q}$ is a $\mathfrak{p}$-primary ideal in R, then $\mathfrak{q}[x]$ is a $\mathfrak{p}[x]$-primary ideal in $R[x]$.
(d) If $I = \bigcap_{i=1}^n \mathfrak{q}_i$ is a minimal primary decomposition in R, then $I[x] = \bigcap_{i=1}^n \mathfrak{q}_i[x]$ is a minimal primary decomposition in $R[x]$.
(e) If $\mathfrak{p}$ is a minimal prime ideal of I, then $\mathfrak{p}[x]$ is a minimal prime ideal of $I[x]$.
(f) If $\mathfrak{p}$ is a prime ideal in R, then $\mathfrak{p}[x] + xR[x]$ is a prime ideal in $R[x]$ such that contains properly $\mathfrak{p}[x]$. In particular it follows that in general, if $P \in R[x]$ is a prime ideal, then $(P \cap R)R[x] \subset P$.

LEMMA 1.72. *For a multiplicative system $S \subset R$ we get $(S^{-1}R)[X] \simeq S^{-1}(R[X])$.*

PROOF. Consider the following commutative diagrams

$$\begin{array}{ccc} R[x] & \xrightarrow{\eta_1} & S^{-1}R[x] \\ {\scriptstyle \iota_S}\downarrow & \nearrow_{g} & \\ S^{-1}(R[x]) & & \end{array} \qquad \begin{array}{ccc} S^{-1}R & \xrightarrow{\eta_2} & S^{-1}(R[x]) \\ {\scriptstyle \iota}\downarrow & \nearrow_{f} & \\ (S^{-1}R)[x] & & \end{array}$$

with $\eta_1(\sum a_i x^i) = \sum (a_i/1)x^i$, $\eta_2(r/s) = r/s$, $f(x) = x/1$, and where ι is the inclusion and g is obtained by the universal property of the localisation. Clearly $f \circ g = \mathbb{1}_{S^{-1}(R[x])}$ and $g \circ f = \mathbb{1}_{(S^{-1}R)[x]}$. ♠

COROLLARY 1.73. *Let R be a integral domain. Then*

$$(R \setminus \{0\})^{-1}(R[x]) \cong ((R \setminus \{0\})^{-1}R) \cong K[x]$$

where K is the quotient field of R. In particular, there exists a correspondence between the prime ideals of $K[x]$ and the prime ideals $\mathfrak{p}$ of $R[x]$ such that $\mathfrak{p} \cap R = 0$.

LEMMA 1.74. *Let R be a ring and consider $P_1 \subsetneq P_2 \subsetneq P_3$ primes ideals in $R[x]$, then $P_1 \cap R \neq P_3 \cap R$.*

PROOF. Let $\mathfrak{p} := P_1 \cap R$, then $\mathfrak{p}[x] \subset P_1$. Assume that $P_3 \cap R = \mathfrak{p}$. As we have $\mathfrak{p}[x] \subset P_1$, then we obtain a chain $\overline{P}_1 \subset \overline{P}_2 \subset \overline{P}_3$ in the integral domain $R[x]/\mathfrak{p}[x] \simeq (R/\mathfrak{p})[x]$ where $\overline{P}_1 \cap (R/\mathfrak{p}) = \overline{P}_3 \cap (R/\mathfrak{p}) = \overline{0}$. So by above lemma we have a chain of prime ideals $Q_1 \subset Q_2 \subset Q_3$ in $K[x]$, where K is the quotient field of $R/\mathfrak{p}$, obtaining that $\dim(K[x]) \geq 2$, a contradiction. ♠

LEMMA 1.75. *Let R be a ring. Let $P \in \operatorname{Spec}(R[x])$ and $\mathfrak{p} := P \cap R$ in $\operatorname{Spec}(R)$. If $\mathfrak{p}[x] \subsetneq P$, then $\operatorname{ht}(P) = \operatorname{ht}(\mathfrak{p}[x]) + 1$.*

PROOF. By induction on $\operatorname{ht}(\mathfrak{p})$. If $\operatorname{ht}(\mathfrak{p}) = 0$, then $\operatorname{ht}(\mathfrak{p}[x]) = 0$ since if $Q \subsetneq \mathfrak{p}[x]$ with $Q \in \operatorname{Spec}(R[x])$. Then $Q \cap R \subset \mathfrak{p}[x] \cap R = \mathfrak{p}$, thus $Q \cap R = \mathfrak{p}$ because $\operatorname{ht}(\mathfrak{p}) = 0$. On the other hand the prime ideal $\mathfrak{p}[x] + xR[x]$ also contracts to $\mathfrak{p}$ contradicting the Lemma 1.74. Thus we need to show that $\operatorname{ht}(P) = 1$. If $\operatorname{ht}(P) > 1$, then there are prime ideals $P_1 \subsetneq P_2 \subsetneq P$. Now $\mathfrak{p}_1 := P_1 \cap R \subset P \cap R = \mathfrak{p}$, but $\operatorname{ht}(\mathfrak{p}) = 0$ yielding $\mathfrak{p}_1 = \mathfrak{p}$, so all prime ideals in $P_1 \subsetneq P_2 \subsetneq P$ have the same contraction in R, contradicting the Lemma 1.74.
If $\operatorname{ht}(\mathfrak{p}) \neq 0$. It is clear that $\operatorname{ht}(P) \geq \operatorname{ht}(\mathfrak{p}[x]) + 1$. Let $P_0 \subset P_1 \subset \ldots P_{s-1} \subset P_s = P$ be a chain of prime ideals of $R[x]$. Let $\mathfrak{p}_{s-1} := P_{s-1} \cap R$. Then, $\mathfrak{p}_{s-1} \subset \mathfrak{p}$.
If $\mathfrak{p}_{s-1} = \mathfrak{p}$, then $P_{s-1} = \mathfrak{p}[x]$, otherwise we would obtain $\mathfrak{p}[x] \subsetneq P_{s-1} \subsetneq P$ and by Lemma 1.74 $\mathfrak{p} \subsetneq \mathfrak{p}$, a contradiction. Thus $s \leq \operatorname{ht}(\mathfrak{p}[x]) + 1$.
If $\mathfrak{p}_{s-1} \neq \mathfrak{p}$, then by the induction hypothesis, $\operatorname{ht}(P_{s-1}) \leq \operatorname{ht}(\mathfrak{p}_{s-1}[x]) + 1$. Also $\operatorname{ht}(\mathfrak{p}_{s-1}[x]) + 1 \leq \operatorname{ht}(\mathfrak{p}[x])$. Thus $s \leq \operatorname{ht}(P_{s-1}) + 1 \leq \operatorname{ht}(\mathfrak{p}_{s-1}[x]) + 2 \leq \operatorname{ht}(\mathfrak{p}[x]) + 1$. Therefore, $\operatorname{ht}(P) = \operatorname{ht}(\mathfrak{p}[x]) + 1$. ♠

THEOREM 1.76. *If R is a Noetherian ring, then $\dim(R[x]) = \dim(R) + 1$.*

PROOF. Let $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_n$ be a chain of prime ideals in R. Then we obtain a chain of prime ideals in $R[x]$, $\mathfrak{p}_0[x] \subset \cdots \subset \mathfrak{p}_n[x]$ since for all i, $\mathfrak{p}_i[x] \neq \mathfrak{p}_{i+1}[x]$ as $\mathfrak{p}_i[x] \cap R = \mathfrak{p}_i$. As $\mathfrak{p}_n[x] + xR[x]$ is a prime ideal in $R[x]$ (Proposition 1.71 (f)). Thus $\dim(R[x]) \geq \dim(R) + 1$. Show that $\dim(R) + 1 \geq \dim(R[x])$: Let $\mathfrak{p}$ be a prime ideal of height m in R. Then, there exist $a_1, \ldots, a_m \in \mathfrak{p}$ such that $\mathfrak{p}$ is minimal prime ideal belonging to $I = (a_1, \ldots, a_m)$ ♠

Depth and regular sequences.

DEFINITION 1.77. Let $(R, \mathfrak{m})$ be a local ring and let M be an R-module of dimension d. A *system of parameters* (s.o.p for short) s.o.p, of M is a set of elements $\theta_1, \ldots, \theta_d$ in $\mathfrak{m}$ such that $\ell_R(M/(\theta_1, \ldots, \theta_d)M) < \infty$.

PROPOSITION 1.78. *Let M be an R-module and let I be an ideal of R such that $IM \neq M$. If $\underline{\theta} = \theta_1, \ldots, \theta_r$ is an M-regular sequence in I, then $\underline{\theta}$ can be extended to a maximal M-regular sequence in I.*

PROOF. By induction assume there is an M-regular sequence $\theta_1, \ldots, \theta_i$ in I for some $i \geq r$. Set $\overline{M} = M/(\theta_1, \ldots, \theta_i)M$. If $I \not\subset \mathcal{Z}(\overline{M})$, pick θ_{i+1} in I which is regular on $\overline{M}$. Since

$$(\theta_1) \subset (\theta_1, \theta_2) \subset \cdots \subset (\theta_1, \ldots, \theta_i) \subset (\theta_1, \ldots, \theta_{i+1}) \subset R$$

is an increasing sequence of ideals in a Noetherian ring R, this inductive construction must stop at a maximal M-regular sequence in I. ♠

LEMMA 1.79. *Let M be a module over a local ring $(R, \mathfrak{m})$. If $\theta_1, \ldots, \theta_r$ is an M-regular sequence in $\mathfrak{m}$, then $r \leq \dim(M)$.*

PROOF. By induction on dimension of M. If $\dim(M) = 0$, then $\mathfrak{m}$ is an associated prime of M and every element of $\mathfrak{m}$ is a zero divisor of M. We claim $\dim(M/\theta_1 M) < \dim(M)$. If this equality does not hold, there is a saturated chain of prime ideals

$$\operatorname{ann}(M) \subset \operatorname{ann}(M/\theta_1 M) \subset \mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_d,$$

where d is the dimension of M and $\mathfrak{p}_0$ is minimal over $\operatorname{ann}(M)$. By Proposition 1.27 the ideal $\mathfrak{p}_0$ consists of zero divisors, but $\theta_1 \in \operatorname{ann}(M/\theta_1 M) \subset \mathfrak{p}_0$, a contradiction. This proves the claim. Since $\theta_2, \ldots, \theta_r$ is a regular sequence on $M/\theta_1 M$ by induction one derives $r \leq \dim(M)$. ♠

Let $M \neq (0)$ be a module over a local ring $(R, \mathfrak{m})$. The *depth* of M, denoted by $\operatorname{depth}(M)$, is the length of any maximal regular sequence on M which is contained in $\mathfrak{m}$.

LEMMA 1.80. $\operatorname{depth}(M) \leq \dim(M)$.

PROOF. It follows from Lemma 1.79. ♠

DEFINITION 1.81. Let $(R, \mathfrak{m})$ be a local ring. An R-module M is called *Cohen–Macaulay* (C–M for short) if $\operatorname{depth}(M) = \dim(M)$, or if $M = (0)$.

LEMMA 1.82. (Depth lemma [**Vas04**, p. 305]) *If $0 \to N \to M \to L \to 0$ is a short exact sequence of modules over a local ring R, then*

(a) *If* $\operatorname{depth}(M) < \operatorname{depth}(L)$, *then* $\operatorname{depth}(N) = \operatorname{depth}(M)$.

(b) *If* $\operatorname{depth}(M) = \operatorname{depth}(L)$, *then* $\operatorname{depth}(N) \geq \operatorname{depth}(M)$.

(c) *If* $\operatorname{depth}(M) > \operatorname{depth}(L)$, *then* $\operatorname{depth}(N) = \operatorname{depth}(L) + 1$.

LEMMA 1.83. *If M is a module over a local ring $(R, \mathfrak{m})$ and $z \in \mathfrak{m}$ is a regular element of M, then* $\operatorname{depth}(M/zM) = \operatorname{depth}(M) - 1$.

PROOF. As depth$M >$ depthM/zM applying the depth lemma to the exact sequence

$$0 \longrightarrow M \xrightarrow{z} M \longrightarrow M/zM \longrightarrow 0$$

yields depth$(M) =$ depth(M/zM)+1. ♠

PROPOSITION 1.84. [**BH98**, p. 58] *If M is a Cohen–Macaulay R-module, then $S^{-1}M$ is Cohen–Macaulay for every multiplicatively closed set S of R.*

PROPOSITION 1.85. [**BH98**, p. 58] *Let M be an R-module and let $\underline{x}$ be an M-regular sequence. If M is Cohen–Macaulay, then $M/\underline{x}M$ is Cohen–Macaulay (over R or $R/(\underline{x})$). The converse holds if R is local.*

PROPOSITION 1.86. [**Mat80**, Theorem 30] *If $M \neq (0)$ is a Cohen–Macaulay R-module over a local ring R and $\mathfrak{p} \in \mathrm{Ass}(M)$, then* $\dim(R/\mathfrak{p}) = \mathrm{depth}(M)$.

DEFINITION 1.87. Let $(R, \mathfrak{m})$ be a local ring of dimension d. A *system of parameters* (s.o.p) of R is a set $\theta_1, \ldots, \theta_d$ generating an $\mathfrak{m}$-primary ideal.

COROLLARY 1.88. *If $(R, \mathfrak{m}, k)$ is a local ring, then* $\dim(R) \leq \dim_k(\mathfrak{m}/\mathfrak{m}^2)$ *and R has finite Krull dimension.*

PROOF. Let $x_1, \ldots, x_q$ be a set of elements in $\mathfrak{m}$ whose images in $\mathfrak{m}/\mathfrak{m}^2$ form a basis of this vector space. Then $\mathfrak{m} = (x_1, \ldots, x_q) + \mathfrak{m}^2$. Hence by Nakayama's lemma we get $\mathfrak{m} = (x_1, \ldots, x_q)$. Hence dim $R \leq q$ by Theorem 1.68. ♠

Remark. If R is a Noetherian ring, then dim $R_{\mathfrak{p}} < \infty$ for all $\mathfrak{p} \in \mathrm{Spec}(R)$. There are examples of Noetherian rings of infinite Krull dimension [**AM94**].

DEFINITION 1.89. A local ring $(R, \mathfrak{m}, k)$ is called *regular* if

$$\dim(R) = \dim_k(\mathfrak{m}/\mathfrak{m}^2).$$

A ring R is *regular* if $R_{\mathfrak{p}}$ is a regular local ring for every $\mathfrak{p} \in \mathrm{Spec}(R)$.

Cohen–Macaulay rings. A local ring $(R, \mathfrak{m})$ is called *Cohen–Macaulay* if R is Cohen–Macaulay as an R-module. If R is non local and $R_{\mathfrak{p}}$ is a C–M local ring for all $\mathfrak{p} \in \mathrm{Spec}(R)$, then we say that R is a *Cohen–Macaulay ring*. An ideal I of R is *Cohen–Macaulay* if R/I is a Cohen–Macaulay R-module.

If R is a Cohen–Macaulay ring and S is a multiplicatively closed subset of R, then $S^{-1}(R)$ is a Cohen–Macaulay ring (see [**BH98**, Theorem 2.1.3]).

PROPOSITION 1.90. [**Vil15**, Proposition 2.3.19] *Let M be a module of dimension d over a local ring $(R, \mathfrak{m})$ and let $\underline{\theta} = \theta_1, \ldots, \theta_d$ be a system of parameters of M. Then M is Cohen–Macaulay if and only if $\underline{\theta}$ is an M-regular sequence.*

LEMMA 1.91. *Let $(R,\mathfrak{m})$ be a local ring and let $(f_1,\ldots,f_r)$ be an ideal of height equal to r. Then there are $f_{r+1},\ldots,f_d$ in $\mathfrak{m}$ such that $f_1,\ldots,f_d$ is a system of parameters of R.*

PROOF. Set $d=\dim(R)$ and $I=(f_1,\ldots,f_r)$. One may assume $r<d$, otherwise there is nothing to prove. Let $\mathfrak{p}_1,\ldots,\mathfrak{p}_s$ be the minimal primes of I. Note that $\operatorname{ht}(\mathfrak{p}_i)=r$ for all i by Theorem 1.66. Hence if we pick f_{r+1} in $\mathfrak{m}\setminus\cup_{i=1}^{s}\mathfrak{p}_i$, one has the equality $\operatorname{ht}(I,f_{r+1})=r+1$, and the result follows by induction. ♠

DEFINITION 1.92. Let I be an ideal of a ring R. If I is generated by a regular sequence we say that I is a *complete intersection* (CI for short).

DEFINITION 1.93. An ideal I of a ring R is called a *set-theoretic complete intersection* if there are $f_1,\ldots,f_r$ in I such that $\operatorname{rad}(I)=\operatorname{rad}(f_1,\ldots,f_r)$, where $r=\operatorname{ht}(I)$.

DEFINITION 1.94. An ideal I of a ring R is *height unmixed* or *unmixed* if satisfies $\operatorname{ht}(I)=\operatorname{ht}(\mathfrak{p})$ for all $\mathfrak{p}$ in $\operatorname{Ass}_R(R/I)$.

PROPOSITION 1.95. *Let $(R,\mathfrak{m})$ be a Cohen–Macaulay local ring and let I be an ideal of R. If I is a complete intersection, then R/I is Cohen–Macaulay and I is unmixed.*

PROOF. Set $d=\dim(R)$ and $r=\operatorname{ht}(I)$. By Lemma 1.83 R/I is Cohen–Macaulay and $\dim(R/I)=d-r$. Let $\mathfrak{p}$ be an associated prime of R/I, then using Proposition 1.86 yields

$$\dim(R)-\operatorname{ht}(\mathfrak{p})\geq\dim(R/\mathfrak{p})=\operatorname{depth}(R/I)=d-r.$$

As a consequence $\operatorname{ht}(\mathfrak{p})\leq r$ and thus $\operatorname{ht}(\mathfrak{p})=r$. Hence I is unmixed. ♠

THEOREM 1.96. (Unmixedness theorem [**Mat80**, Theorem 17.6]) *A ring R is Cohen–Macaulay if and only if every proper ideal I of R of height r generated by r elements is unmixed.*

Let A be a (Noetherian) ring one says that A is a *catenary* ring if for every pair $\mathfrak{p}\subset\mathfrak{q}$ of prime ideals $\operatorname{ht}(\mathfrak{q}/\mathfrak{p})$ is equal to the length of any maximal chain of prime ideals between $\mathfrak{p}$ and $\mathfrak{q}$. If A is a domain, then A is catenary if and only if $\operatorname{ht}(\mathfrak{q}/\mathfrak{p})=\operatorname{ht}(\mathfrak{q})-\operatorname{ht}(\mathfrak{p})$ for every pair of prime ideals $\mathfrak{p}\subset\mathfrak{q}$.

THEOREM 1.97. [**BH98**, Theorem 2.1.12] *If R is a Cohen–Macaulay ring, then R is catenary.*

Gorenstein rings. Let $M\neq(0)$ be a module over a local ring $(R,\mathfrak{m})$ and let $k=R/\mathfrak{m}$ be the residue field of R. The *socle* of M is defined as

$$\operatorname{Soc}(M)=(0\colon_M\mathfrak{m})=\{z\in M|\,\mathfrak{m}z=(0)\},$$

and the *type* of M is defined as $\operatorname{type}(M)=\dim_k\operatorname{Soc}(M/\underline{x}M)$,

where $\underline{x}$ is a maximal M-sequence in $\mathfrak{m}$. Observe that the type of M is well-defined because by one has:

$$\operatorname{Ext}^r_R(k, M) \simeq \operatorname{Hom}_R(k, M/\underline{x}M) \simeq \operatorname{Soc}(M/\underline{x}M),$$

where $r = \operatorname{depth}(M)$, see [**Vil15**, Proposition 2.3.7]. The ring R is said to be *Gorenstein* if R is a Cohen–Macaulay ring of type 1. An ideal $I \subset R$ is called *Gorenstein* if R/I is a Gorenstein ring. For a thorough study of Gorenstein rings see [**Bas63, BH98**].

1.2. Graded modules and Hilbert polynomials

Let $(H, +)$ be an abelian semigroup. An *H-graded ring* is a ring R together with a decomposition

$$R = \bigoplus_{a \in H} R_a \ \ (\text{as a } \mathbb{Z}\text{-module}),$$

such that $R_a R_b \subset R_{a+b}$ for all $a, b \in H$. A *graded ring* is by definition a $\mathbb{Z}$-graded ring.

If R is an H-graded ring and M is an R-module with a decomposition

$$M = \bigoplus_{a \in H} M_a,$$

such that $R_a M_b \subset M_{a+b}$ for all $a, b \in H$, we say that M is an *H-graded module*. An element $0 \neq f \in M$ is said to be *homogeneous* of degree a if $f \in M_a$, in this case we set $\deg(f) = a$. The non-zero elements in R_a are also called *forms* of degree a. Any element $f \in M$ can be written uniquely as $f = \sum_{a \in H} f_a$ with only finitely many $f_a \neq 0$.

A map $\varphi\colon M \to N$ between H-graded modules is *graded* if $\varphi(M_a) \subset N_a$ for all $a \in H$. Let $M = \oplus_{a \in H} M_a$ be an H-graded module and N a *graded submodule*; that is, N is graded with the induced grading $N = \oplus_{a \in H} N \cap M_a$. Then M/N is an H-graded R-module with $(M/N)_a = M_a/N \cap M_a$ for $a \in H$, $R_0 \subset R$ is a subring and M_a is an R_0-module for $a \in H$.

PROPOSITION 1.98. [**Mat89**, p. 92] *Let $M = \oplus_{a \in H} M_a$ be an H-graded module and $N \subset M$ a submodule. Then the following conditions are equivalent:*

(a) *N is generated over R by homogeneous elements.*
(b) *If $f = \sum_{a \in H} f_a$ is in N, $f_a \in M_a$ for all a, then each f_a is in N.*
(c) *N is a graded submodule of M.*

Let $R = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K and let $d_1, \ldots, d_n$ be a sequence in $\mathbb{N}_+$. For $a = (a_i)$ in $\mathbb{N}^n$ we set $x^a = x_1^{a_1} \cdots x_n^{a_n}$ and $|a| = \sum_{i=1}^n a_i d_i$. The *induced* $\mathbb{N}$-*grading* on R is given by:

$$R = \bigoplus_{i=0}^{\infty} R_i, \text{ where } R_i = \bigoplus_{|a|=i} K x^a.$$

Notice that $\deg(x_i) = d_i$ for all i. The induced grading extends to a $\mathbb{Z}$-grading by setting $R_i = 0$ for $i < 0$. The homogeneous elements of R are called *quasi-homogeneous polynomials*. Let I be a *homogeneous* ideal of R generated by a set $f_1, \ldots, f_r$ of homogeneous polynomials. Setting $\deg(f_i) = \delta_i$, I becomes a *graded ideal* with the grading

$$I_i = I \cap R_i = f_1 R_{i-\delta_1} + \cdots + f_r R_{i-\delta_r}.$$

Hence R/I is an $\mathbb{N}$-graded R-module graded by $(R/I)_i = R_i/I_i$.

DEFINITION 1.99. The *standard grading* or *usual grading* of a polynomial ring $K[x_1, \ldots, x_n]$ is the $\mathbb{N}$-grading induced by setting $\deg(x_i) = 1$ for all i.

1.2.1. Graded primary decomposition. Let $R = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K endowed with a positive grading induced by setting $\deg(x_i) = d_i$ for all i, where d_i is a positive integer for $i = 1, \ldots, n$.

LEMMA 1.100. **[BH98**, Lemma 1.5.6] *If M is an $\mathbb{N}$-graded R-module and $\mathfrak{p}$ is in $\operatorname{Ass}(M)$, then $\mathfrak{p}$ is a graded ideal and there is $m \in M$ homogeneous such that $\mathfrak{p} = \operatorname{ann}(m)$.*

PROPOSITION 1.101. **[Mat80**, p. 63] *Let M be an $\mathbb{N}$-graded R-module and let Q be a $\mathfrak{p}$-primary submodule of M. If $\mathfrak{p}$ is graded and Q^* is the submodule of M generated by the homogeneous elements in Q, then Q^* is again a $\mathfrak{p}$-primary submodule.*

THEOREM 1.102. *Let M be an $\mathbb{N}$-graded R-module and let N be a proper graded submodule of M. Then N has an irredundant primary decomposition $N = N_1 \cap \cdots \cap N_r$ such that N_i is a graded submodule for all i.*

PROOF. Use Lemma 1.100, Proposition 1.101, and Theorem 1.35. ♠

Finding primary decompositions of graded ideals in polynomial rings over fields is a difficult task. For a treatment consult **[Vas04**, Chapter 3].

Notation If $R = \oplus_{i=0}^{\infty} R_i$ is an $\mathbb{N}$-graded ring, we set $R_+ = \oplus_{i \geq 1} R_i$.

LEMMA 1.103 (Graded Nakayama lemma). *Let R be an $\mathbb{N}$-graded ring and let M be an $\mathbb{N}$-graded R-module. If N is a graded submodule of M and $I \subset R_+$ is a graded ideal of R such that $M = N + IM$, then $N = M$.*

PROOF. Since $M/N = I(M/N)$, one may assume $N = (0)$. If $x \in M$ is a homogeneous element of degree r, then a recursive use of the equality $M = IM$ yields that $x \in I^{r+1}M$ and x must be zero. ♠

LEMMA 1.104. *Let $R = \oplus_{i=0}^{\infty} R_i$ be an $\mathbb{N}$-graded ring and let $M = \oplus_{i=0}^{\infty} M_i$ be an $\mathbb{N}$-graded R-module. If M is Artinian, then there is $k \in \mathbb{N}$ such that $M_i = (0)$ for $i > k$.*

PROOF. Setting $N_i = \oplus_{j=i}^{\infty} M_j$, we get a descending chain

$$M = N_0 \supset N_1 \supset \cdots \supset N_i \supset \cdots$$

of R-modules. As M is Artinian, there is $k \in \mathbb{N}$ such that $N_i = N_k$ for $i > k$. As M is $\mathbb{N}$-graded, it follows that $M_i = (0)$ for $i > k$. ♠

THEOREM 1.105. **[Vas04**, Proposition 3.1.6] *Let $R = K[x_1, \ldots, x_n]$ be a polynomial ring with the standard grading over a field K and let I be a graded ideal. If R/I is Artinian and $I = I_1 \cap \cdots \cap I_r$ is an irredundant representation with I_i irreducible for all i, then $r = \dim_K (I\colon \mathfrak{m})/I$, where $\mathfrak{m} = (x_1, \ldots, x_n)$.*

PROOF. Since $\operatorname{Ass}(R/I_i) = \{\mathfrak{m}\}$ for $1 \leq i \leq r$, there is $e_i \notin I_i$ such that $\mathfrak{m} = (I_i\colon e_i)$. Notice that $\dim_{R/\mathfrak{m}} (I_i\colon \mathfrak{m})/I_i = 1$. Indeed if the dimension is greater than 1, pick two linearly independent elements $\overline{x}$ and $\overline{y}$ in $(I_i\colon \mathfrak{m})/I_i$. Then I_i decomposes as

$$I_i = (I_i + (x)) \cap (I_i + (y)),$$

a contradiction because I_i is irreducible. Hence the linear map

$$R/\mathfrak{m} \to (I_i\colon \mathfrak{m})/I_i, \quad \overline{r} \mapsto \overline{re_i} \tag{1.2.1}$$

is an isomorphism. We set $J_i = I_i + \cap_{j \neq i} I_j$ for $1 \leq i \leq r$. Notice that $I_i \subsetneq J_i$ because the representation $I = \cap_{i=1}^{r} I_i$ is irredundant. Hence, using that I_i is irreducible and that $I_i \subsetneq (e_i) + I_i$, we get $I_i \subsetneq ((e_i) + I_i) \cap J_i$. Therefore

$$(\overline{0}) \neq (((e_i) + I_i)/I_i) \cap (J_i/I_i) \subset ((e_i) + I_i)/I_i.$$

Since $\dim_{R/\mathfrak{m}}((e_i) + I_i)/I_i = 1$, the inclusion above is an equality. Thus one has the inclusion $((e_i) + I_i)/I_i) \subset (J_i/I_i)$. Then we can write $e_i = z_i + y_i$ with $z_i \in \cap_{j \neq i} I_j$ and $y_i \in I_i$ for all i. There is an injection

$$0 \to (I\colon \mathfrak{m})/I \xrightarrow{\psi} \bigoplus_{i=1}^{r} (I_i\colon \mathfrak{m})/I_i$$

induced by the map $R/I \to \bigoplus_{i=1}^{r} R/I_i$, $\overline{a} \mapsto (\overline{a}, \ldots, \overline{a})$. Thus, by Eq. (1.2.1), $\dim_K(\operatorname{im}(\psi))$ is at most r. As $z_i \in (I\colon \mathfrak{m})$ and $z_i - e_i \in I_i$ for all i, it follows that $\operatorname{im}(\psi)$ contains $\oplus_{i=1}^{r} ((e_i) + I_i)/I_i$. As the latter K-vector space has dimension r, we get that $\dim_K(\operatorname{im}(\psi))$ is at least r. Therefore the map ψ is an isomorphism of K-vector spaces and $\dim_K(I\colon \mathfrak{m})/I$ is equal to r. ♠

LEMMA 1.106. *Let R be a polynomial ring over a field K and let $I \subset R$ be a graded ideal. Then I is a complete intersection if and only if I is generated by a homogeneous regular sequence with* $\operatorname{ht}(I)$ *elements.*

PROOF. It follows from Propositions 1.90, 1.95, and Lemma 1.91. ♠

1.2.2. The Hilbert–Serre and Hilbert Theorems. Let $R = \oplus_{i=0}^{\infty} R_i$ be an $\mathbb{N}$-graded ring. We recall that R is a Noetherian ring if and only if R_0 is a Noetherian ring and $R = R_0[x_1, \ldots, x_n]$ for some $x_1, \ldots, x_n$ in R.

DEFINITION 1.107. An $\mathbb{N}$-graded ring $R = \oplus_{i=0}^{\infty} R_i$ is called a *homogeneous ring* if $R = R_0[x_1, \ldots, x_n]$, where $\deg(x_i) = 1$ for all i.

Let $R = R_0[x_1, \ldots, x_n]$ be a homogeneous ring over an Artinian local ring R_0, where $\deg(x_i) = 1$ for all i and $R = \oplus_{i=0}^{\infty} R_i$. If

$$M = M_0 \oplus M_1 \oplus \cdots \oplus M_i \oplus \cdots$$

is a finitely generated $\mathbb{N}$-graded module over R, its *Hilbert function* and *Hilbert series* are defined by

$$H(M, i) = \ell(M_i) \text{ and } F(M, t) = \sum_{i=0}^{\infty} H(M, i) t^i,$$

respectively, where $\ell(M_i)$ denotes the length of M_i as an R_0-module, if R_0 is a field $\ell(M_i) = \dim_{R_0}(M_i)$.

LEMMA 1.108. *If $0 \to M' \to M \to M'' \to 0$ is a degree preserving short exact sequence of $\mathbb{N}$-graded R-modules, then*

(a) $H(M, i) = H(M', i) + H(M'', i)$ *for all i, and*

(b) $F(M, t) = F(M', t) + F(M'', t)$.

PROOF. It follows Proposition 1.54. ♠

If $j \in \mathbb{N}$, then $M(-j)$ is the *regrading* of M obtained by a *shift* of the graduation of M; more precisely

$$M(-j) = \bigoplus_{i=0}^{\infty} M(-j)_i,$$

where $M(-j)_i = M_{-j+i}$. Note that we are assuming $M_i = 0$ for $i < 0$. In this way $M(-j)$ becomes an $\mathbb{N}$-graded R-module.

LEMMA 1.109. $F(M(-j), t) = t^j F(M, t)$.

PROOF. Since $M(-j)_i = M_{i-j}$ one has:

$$F(M(-j),t) = t^j \sum_{i=j}^{\infty} \ell(M_{i-j}) t^{i-j} = t^j F(M,t),$$

where the first equality follows using that $M_{i-j} = 0$ for $i = 0, \ldots, j-1$. ♠

LEMMA 1.110. *If $z \in R_j$, there is a degree preserving exact sequence*

$$0 \longrightarrow (M/(0\colon z))(-j) \xrightarrow{z} M \xrightarrow{\phi} M/zM \longrightarrow 0 \ \ (\phi(m) = m + zM),$$

where $(0\colon z) = \{m \in M \mid zm = 0\}$ and the first map is multiplication by z.

PROOF. As the map $\psi\colon M(-j) \to M$, given by $\psi(m) = zm$, is a degree zero homomorphism one has that $(0\colon z)(-j)$ is a graded submodule of $M(-j)$. The exactness of the sequence above follows because ψ induces an exact sequence

$$0 \longrightarrow (0\colon z)(-j) \xrightarrow{\iota} M(-j) \xrightarrow{\psi} M \xrightarrow{\phi} M/zM \longrightarrow 0,$$

where ι is an inclusion. ♠

THEOREM 1.111. (Hilbert–Serre Theorem) *The Hilbert series $F(M,t)$ of M is a rational function that can be written uniquely as*

$$F(M,t) = \frac{h(t)}{(1-t)^d},$$

where $d = \dim(M)$ and $h(t)$ is a polynomial in $\mathbb{Z}[t]$ such that $h(1) > 0$.

PROOF. We proceed by induction on d, the dimension of M. Assume $d = 0$. By Proposition 1.27 we have $\operatorname{Supp}(M) = V(\operatorname{ann}(M))$. Since $\dim(M)$ is equal to $\dim(R/\operatorname{ann}(M))$, we get that every prime ideal in $\operatorname{Supp}(M)$ is maximal. Thus, by Proposition 1.58, M has finite length. In particular M is Artinian. Thus, by Lemma 1.104, there is $k \in \mathbb{N}$ such that $M_i = (0)$ for $i > k$. Hence $F(M,t) = h(t)$ for some polynomial $h(t)$ with non-negative coefficientes and such that $h(1) > 0$.

Assume that $d > 0$. As M is graded, by Theorem 1.22 and its proof, there is a filtration of submodules

$$(0) = N_0 \subset N_1 \subset \cdots \subset N_r = M$$

and graded prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ of R such that $N_i/N_{i-1} \simeq (R/\mathfrak{p}_i)[-a_i]$ and $a_i \in \mathbb{N}$ for all i. If $\mathfrak{p}_i = R_+$, then $R/R_+ \simeq R_0$ and $F(R/\mathfrak{p}_i) = f_i(t)$, where $f_i(t)$ is the constant polynomial $\ell(R_0)$. If $\mathfrak{p}_i \subsetneq R_+$, pick $x \in R_1 \setminus \mathfrak{p}_i$. Using the exact sequence

$$0 \to (R/\mathfrak{p}_i)[-1] \xrightarrow{x} R/\mathfrak{p}_i \to R/(\mathfrak{p}_i, x) \to 0,$$

together with Lemma 1.108, Corollary 1.69, and the induction hypothesis, we get that $F(R/\mathfrak{p}_i, t) = f_i(t)/(1-t)^{d_i}$, where $d_i = \dim(R/\mathfrak{p}_i)$, $f_i(1) > 0$ and $f_i(t) \in \mathbb{Z}[t]$. Then, by Lemma 1.108, we get

$$F(M,t) = \sum_{i=1}^{r} F((R/\mathfrak{p}_i)[-a_i], t) = \sum_{i=1}^{r} t^{a_i} F(R/\mathfrak{p}_i, t) = \sum_{i=1}^{r} \frac{t^{a_i} f_i(t)}{(1-t)^{d_i}}.$$

Using that $\dim(M) = \max_i\{\dim(R/\mathfrak{p}_i)\}$ (see Proposition 1.57) it is not hard to see that $F(M,t)$ has the required form. ♠

DEFINITION 1.112. The degree of $F(M,t)$ as a rational function is denoted by $a(M)$; it is called the *a-invariant* of M.

Below we see how the a-invariant measures the difference between the Hilbert polynomial and the Hilbert function.

LEMMA 1.113. *Let $f(t) \in \mathbb{Q}[t]$ be a polynomial of degree $d-1$ such that $f(n) \in \mathbb{Z}$ for $n \in \mathbb{Z}$, then there are unique integers $a_0, \ldots, a_{d-1}$ such that*

$$f(t) = \sum_{i=0}^{d-1} a_i f_i(t), \quad \textit{where} \quad f_i(t) = \binom{t+i}{i}.$$

PROOF. The polynomials $f_i(t)$, $i \in \mathbb{N}$, are a basis for $\mathbb{Q}[t]$ as a $\mathbb{Q}$-vector space. Hence $f(t) = \sum_{i=0}^{d-1} a_i f_i(t)$, for some $a_i \in \mathbb{Q}$. Using the Pascal triangle we get

$$f(t) - f(t-1) = \sum_{i=0}^{d-1} a_i \left[\binom{t+i}{i} - \binom{t+i-1}{i} \right] = \sum_{i=0}^{d-1} a_i \binom{t+i-1}{i-1},$$

thus by induction on the degree it follows that $a_i \in \mathbb{Z}$ for all i. ♠

For use below, by convention the zero polynomial has degree -1.

PROPOSITION 1.114. *If M is a graded R-module of dimension d. Then, there are integers $a_{-d}, \ldots, a_{-1}$ so that*

$$H(M,i) = \sum_{j=0}^{d-1} a_{-(d-j)} \binom{i+d-j-1}{d-j-1}, \ \forall\, i \geq a(M)+1,$$

where $a(M)$ is the degree of $F(M,t)$ as a rational function.

PROOF. By the Hilbert–Serre Theorem there is a polynomial $h(t) \in \mathbb{Z}[t]$ such that

$$F(M,t) = \frac{h(t)}{(1-t)^d}$$

and $h(1) > 0$. If $d = 0$, then $a(M)$ is equal to $\deg(h)$ and $H(M,i) = 0$ for $i \geq a(M)+1$. Thus one may assume $d > 0$. Observe that by the division algorithm we can find $e(t) \in \mathbb{Z}[t]$ so that the Laurent expansion of $F(M,t) - e(t)$, in negative powers of $(1-t)$, is equal to

$$F(M,t) - e(t) = \sum_{j=0}^{d-1} \frac{a_{-(d-j)}}{(1-t)^{d-j}}, \text{ where } a_{-(d-j)} = \frac{(-1)^j h^{(j)}(1)}{j!},$$

where $h^{(j)}$ is the jth derivative of h. Next we expand $(1-t)^{d-j}$ in powers of t to obtain

$$F(M,t) = e(t) + \sum_{i=0}^{\infty} \left[\sum_{j=0}^{d-1} a_{-(d-j)} \binom{i+d-j-1}{d-j-1} \right] t^i = e(t) + \sum_{i=0}^{\infty} \varphi(i) t^i,$$

observe that $\varphi(i) = H(M,i)$ for $i \geq \deg e(t) + 1$, where the degree of the zero polynomial is set equal to -1. To complete the proof note that $a_{-d}, \ldots, a_{-1}$ are integers by Lemma 1.113. ♠

THEOREM 1.115. (Hilbert) *Let $R = \oplus_{i=0}^{\infty} R_i$ be a homogeneous ring and let M be a finitely generated $\mathbb{N}$-graded R-module with $d = \dim(M)$. If R_0 is an Artinian local ring, then there is a unique polynomial $\varphi_M(t) \in \mathbb{Q}[t]$ of degree $d-1$ such that $\varphi_M(i) = H(M,i)$ for $i \gg 0$.*

PROOF. It follows at once from Proposition 1.114. ♠

DEFINITION 1.116. The polynomial $\varphi_M(t)$ is called the *Hilbert polynomial* of M. If $\varphi_M(t) = a_{d-1}t^{d-1} + \cdots + a_0$, the *multiplicity* or *degree* of M, denoted by $e(M)$ or $\deg(M)$, is $(d-1)!a_{d-1}$ if $d \geq 1$ and $\ell_{R_0}(M)$ if $d = 0$.

REMARK 1.117. The leading coefficient of the Hilbert polynomial $\varphi_M(t)$ of M is equal to $h(1)/(d-1)!$, where $h(t)$ is the polynomial $F(M,t)(1-t)^d$. If $d = 0$, then $h(1) = \ell(M)$ and $\ell(M) = \dim_K(M)$ if R is a polynomial ring over a field K.

DEFINITION 1.118. The *index of regularity* of M is the least integer $\ell \geq 0$ such that $H(M,i) = \varphi_M(i)$ for $i \geq \ell$.

COROLLARY 1.119. *Let M be a graded R-module. If*

$$r_0 = \min\{r \in \mathbb{N} \,|\, H(M,i) = \varphi_M(i),\ \forall\, i \geq r\},$$

then $r_0 = 0$ if $a(M) < 0$ and $r_0 = a(M)+1$ otherwise.

PROPOSITION 1.120. **[Vil15**, Propositions 3.1.33 and 5.1.11] *Let $A = R_1/I_1$, $B = R_2/I_2$ be two standard graded algebras over a field K, where $R_1 = K[\mathbf{x}]$, $R_2 = K[\mathbf{y}]$ are polynomial rings in disjoint sets of variables and I_i is an ideal of R_i. If $R = K[\mathbf{x},\mathbf{y}]$ and $I = I_1 + I_2$, then*

$$(R_1/I_1) \otimes_K (R_2/I_2) \simeq R/I \text{ and } F(A \otimes_K B, t) = F(A,t)F(B,t),$$

where $F(A,t)$ and $F(B,t)$ are the Hilbert series of A and B, respectively.

1.3. Multiplicities of modules over local rings

Let $(R,\mathfrak{m})$ be a Noetherian local ring and let M be a finitely generated R-module. The *associated graded module* of $\mathfrak{m}$ is given by

$$\mathrm{gr}_{\mathfrak{m}}(M) := \bigoplus_{i=0}^{\infty} \mathfrak{m}^i M/\mathfrak{m}^{i+1}M.$$

THEOREM 1.121. *The function $\chi_M^{\mathfrak{m}}(i) := \ell(M/\mathfrak{m}^{i+1}M)$ is a polynomial function of degree $d = \dim(\mathrm{gr}_{\mathfrak{m}}(M))$.*

PROOF. As $\mathrm{gr}_{\mathfrak{m}}(M)$ is a finitely generated $\mathrm{gr}_{\mathfrak{m}}(R)$-module and $A_0 = R/\mathfrak{m}$ is Artinian, by Theorem 1.115, there exists a polynomial $P(t) \in \mathbb{Q}[t]$ of degree $d-1$ such that

$$P(i) = \ell_{A_0}(\mathfrak{m}^i M/\mathfrak{m}^{i+1}M), \text{ for } i \geq n_0.$$

By Lemma 1.113 there are integers $a_0, \ldots, a_{d-1}$ such that

$$P(i) = \sum_{j=0}^{d-1} a_j \binom{i+j}{j}, \text{ for all } i \geq 0.$$

From the short exact sequences

$$0 \longrightarrow \mathfrak{m}^i M/\mathfrak{m}^{i+1}M \longrightarrow M/\mathfrak{m}^{i+1}M \longrightarrow M/\mathfrak{m}^i M \longrightarrow 0,$$

one derives $\ell(M/\mathfrak{m}^{i+1}M) - \ell(M/\mathfrak{m}^i M) = P(i)$ for $i \geq n_0$. Hence, using the identity

$$\binom{d+m}{d} = \sum_{j=0}^{m} \binom{j+d-1}{d-1}, \; d,m \in \mathbb{N},$$

we get

$$\begin{aligned} \chi_M^{\mathfrak{m}}(i) := \ell(M/\mathfrak{m}^{i+1}M) &= \ell(M/\mathfrak{m}^{n_0}M) + \sum_{j=n_0}^{i} P(j) \\ &= c_0 + \sum_{j=0}^{d-1} a_j \binom{j+i+1}{j+1}, \end{aligned}$$

for $i \geq n_0$. ♠

DEFINITION 1.122. The function $\chi_M^{\mathfrak{m}}(i) = \ell(M/\mathfrak{m}^{i+1}M)$ is called the *Hilbert Samuel function* of M. The integer a_{d-1}, is the *multiplicity* or *degree* of M and is denoted by $e(M)$ or $e(\mathfrak{q}, M)$.

Note that $e(M)/d!$ is the leading coefficient of $\chi_M^{\mathfrak{m}}$. The following result in dimension theory relates the degree of the Hilbert Samuel function with the dimension of the module.

THEOREM 1.123. [**Mat89**, Theorem 13.4] *$\chi_M^{\mathfrak{m}}$ is a polynomial function of degree equal to the dimension of M.*

DEFINITION 1.124. Let $(R,\mathfrak{m})$ be a local ring of dimension d and let M be an R-module. We define

$$e_d(M) = \begin{cases} e(M) & \text{if } \dim(M) = d, \\ 0 & \text{if } \dim(M) < d. \end{cases}$$

In order to show how the "multiplicity" behaves under short exact sequences we need to recall a result of E. Artin and D. Rees.

THEOREM 1.125. (Artin–Rees lemma [**Mat89**, Theorem 8.5]) *Let M be a module over a ring R. If N is a submodule of M and I an ideal of R, then there is a positive integer c such that*

$$I^n M \cap N = I^{n-c}(I^c M \cap N),\ \forall\, n > c.$$

PROPOSITION 1.126. *Let $(R,\mathfrak{m})$ be a local ring of dimension d. If*

$$0 \longrightarrow N \longrightarrow M \longrightarrow N' \longrightarrow 0$$

is an exact sequence of R-modules, then $e_d(M) = e_d(N) + e_d(N')$.

PROOF. By Proposition 1.57, $\dim(M) = \max\{\dim(N), \dim(N')\}$. Hence, one may assume $d = \dim(M)$. Tensoring with $R/\mathfrak{m}^{n+1}$ the exact sequence above yields an exact sequence

$$0 \to (N \cap \mathfrak{m}^{n+1}M)/\mathfrak{m}^{n+1}N \to N/\mathfrak{m}^{n+1}N \to M/\mathfrak{m}^{n+1}M \to N'/\mathfrak{m}^{n+1}N' \to 0.$$

Taking lengths with respect to $R/\mathfrak{m}$ gives

$$\chi_M^{\mathfrak{m}}(n) = \chi_N^{\mathfrak{m}}(n) + \chi_{N'}^{\mathfrak{m}}(n) - \ell(N \cap \mathfrak{m}^{n+1}M/\mathfrak{m}^{n+1}N). \qquad (*)$$

By Theorem 1.125, $N \cap \mathfrak{m}^{n+1}M \subset \mathfrak{m}^{n+1-c}N$, for some integer $c > 0$. Hence

$$\ell(N \cap \mathfrak{m}^{n+1}M/\mathfrak{m}^{n+1}N) \leq \ell(\mathfrak{m}^{n+1-c}N/\mathfrak{m}^{n+1}N) = \chi_N^{\mathfrak{m}}(n) - \chi_N^{\mathfrak{m}}(n-c),$$

as $\chi_N^{\mathfrak{m}}(n) - \chi_N^{\mathfrak{m}}(n-c)$ is a polynomial function of degree at most $d-1$, the result follows by dividing Eq. $(*)$ by n^d and taking limits when n goes to infinity. ♠

Next we show that the multiplicity is additive (cf. Proposition 4.2).

PROPOSITION 1.127. *Let $(R,\mathfrak{m})$ be a local ring of dimension d. If M is a finitely generated R-module and $\mathcal{A}$ is the set of all prime ideals $\mathfrak{p}$ of R with $\dim(R/\mathfrak{p}) = d$, then*

$$e_d(M) = \sum_{\mathfrak{p}\in\mathcal{A}} \ell(M_{\mathfrak{p}})e_d(R/\mathfrak{p}).$$

PROOF. Set $\mathcal{B} = \mathcal{A} \cap \operatorname{Supp}(M)$. If $\mathcal{B} = \emptyset$, then $\dim(M) < d$ and $e_d(M)$ is equal to 0, thus in this case the identity above holds. Hence we may assume $\mathcal{B} \neq \emptyset$, this yields the equality $\dim(M) = d$. By Theorem 1.22 there are prime ideals $\mathfrak{p}_1,\ldots,\mathfrak{p}_n$ of R and a filtration of submodules:

$$(0) = M_0 \subset M_1 \subset \cdots \subset M_n = M,$$

such that $M_i/M_{i-1} \simeq R/\mathfrak{p}_i$ for all i. Note $\mathcal{B} = \{\mathfrak{p}_i |\ \dim(R/\mathfrak{p}_i) = d\}$. To show this equality observe that

$$\operatorname{Ass}(M) \subset \{\mathfrak{p}_1,\ldots,\mathfrak{p}_n\} \subset \operatorname{Supp}(M),$$

see Corollary 1.24 and its proof, and recall that the minimal elements of $\operatorname{Supp}(M)$ are in $\operatorname{Ass}(M)$. Using Lemma 1.126 and the exact sequences

$$0 \longrightarrow M_{i-1} \longrightarrow M_i \longrightarrow R/\mathfrak{p}_i \longrightarrow 0 \quad (i = 1,\ldots,n),$$

we get $e(M) = \sum e(R/\mathfrak{p}_i)$, where the sum is taken over all $\mathfrak{p}_i$, in the multiset $\{\mathfrak{p}_1,\ldots,\mathfrak{p}_n\}$, such that $\dim(R/\mathfrak{p}_i) = d$. Let $\mathfrak{p} \in \mathcal{B}$, then

$$(M_i/M_{i-1})_{\mathfrak{p}} \simeq \begin{cases} (0) & \text{if} \quad \mathfrak{p} \neq \mathfrak{p}_i \\ R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}} & \text{if} \quad \mathfrak{p} = \mathfrak{p}_i. \end{cases} \tag{1.3.1}$$

Since the second module is a field we get that the length of $M_{\mathfrak{p}}$ is equal to the number of times that $\mathfrak{p}$ occurs in the multiset $\{\mathfrak{p}_1,\ldots,\mathfrak{p}_n\}$. Therefore

$$e(M) = \sum_{\mathfrak{p}_i\in\mathcal{B}} \ell(M_{\mathfrak{p}_i})e(R/\mathfrak{p}_i),$$

as required. This proof was adapted from [**BH98**]. ♠

CHAPTER 2

Hilbert Functions and Vanishing Ideals in Affine and Projective Varieties

In this chapter we study monomial ideals, Gröbner bases and the footprint of an ideal, projective closures, vanishing ideals, and Hilbert functions. The role of Hilbert functions and vanishing ideals in affine and projective varieties is discussed here. The number of zeros that a homogeneous polynomial has in any given finite set of points in an affine or projective space is expressed in terms of vanishing ideals and the notion of degree.

2.1. Monomial ideals

We study primary and irreducible decompositions of monomial ideals.

Let $R = K[\mathbf{x}] = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K. To make notation simpler, we will use the following multi-index notation:

$$x^a := x_1^{a_1} \cdots x_n^{a_n} \text{ for } a = (a_1, \ldots, a_n) \in \mathbb{N}^n.$$

DEFINITION 2.1. An ideal I of R is called a *monomial ideal* if there is $\mathcal{A} \subset \mathbb{N}_+^n$ such that I is generated by $\{x^a | a \in \mathcal{A}\}$. If I is a monomial ideal the quotient ring R/I is called a *monomial ring*.

Note that, by Dickson's lemma (see Lemma 2.21), a monomial ideal I is always minimally generated by a unique finite set of monomials. This unique set of generators of I is denoted by $G(I)$.

LEMMA 2.2. *Let I and J be two ideals generated by finite sets of monomials F and G, then the intersection $I \cap J$ is generated by the set*

$$\{\operatorname{lcm}(f, g) | \, f \in F \text{ and } g \in G\}.$$

DEFINITION 2.3. A *face ideal* is an ideal $\mathfrak{p}$ of R generated by a subset of the set of variables, that is, $\mathfrak{p} = (x_{i_1}, \ldots, x_{i_k})$ for some variables x_{i_j}.

DEFINITION 2.4. A monomial f in R is called *square-free* if $f = x_{i_1} \ldots x_{i_r}$ for some $1 \leq i_1 < \cdots < i_r \leq n$. A *square-free monomial* is an ideal generated by square-free monomials.

Any square-free monomial ideal is a finite intersection of face ideals:

THEOREM 2.5. *Let $I \subset R$ be a monomial ideal. The following hold.*

(i) *Every associated prime of I is a face ideal.*

(ii) *If I is square-free, then $I = \cap_{i=1}^{s} \mathfrak{p}_i$, where $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ are the associated primes of I. In particular $\mathfrak{p}_i$ is a minimal prime of I for all i.*

PROOF. (i): By induction on the number of variables that occur in $G(I)$. Set $\mathfrak{m} = (x_1, \ldots, x_n)$. Let $\mathfrak{p}$ be an associated prime of I. If $\operatorname{rad}(I) = \mathfrak{m}$, then $\mathfrak{p} = \mathfrak{m}$. Hence we may assume $\operatorname{rad}(I) \neq \mathfrak{m}$. Pick a variable x_1 not in $\operatorname{rad}(I)$ and consider the ascending chain of ideals

$$I_0 = I \text{ and } I_{i+1} = (I_i \colon x_1) \quad (i \geq 0).$$

Since R is Noetherian, one has $I_k = (I_k \colon x_1)$ for some k. There are two cases to consider. If $\mathfrak{p}$ is an associated prime of (I_i, x_1) for some i, then by induction $\mathfrak{p}$ is a face ideal because one can write $(I_i, x_1) = (I_i', x_1)$, where I_i' is an ideal minimally generated by a finite set of monomials in the variables $x_2, \ldots, x_n$. Assume we are in the opposite case. By Lemma 1.110 for each i there is an exact sequence

$$0 \longrightarrow R/(I_i \colon x_1) \xrightarrow{x_1} R/I_i \longrightarrow R/(I_i, x_1) \longrightarrow 0,$$

hence making a recursive application of Lemma 1.23 one obtains that $\mathfrak{p}$ is an associated prime of I_i for all i. Since x_1 is regular on R/I_k one concludes that I_k is an ideal minimally generated by monomials in the variables $x_2, \ldots, x_n$, thus by induction $\mathfrak{p}$ is a face ideal.

(ii): We only have to check $\cap_{i=1}^{s} \mathfrak{p}_i \subset I$ because I is contained in any of its associated primes. Take a monomial f in $\cap_{i=1}^{s} \mathfrak{p}_i$ and write $f = x_{i_1}^{a_1} \cdots x_{i_r}^{a_r}$, where $i_1 < \cdots < i_r$ and $a_i > 0$ for all i. By Corollary 1.36, $f^k \in I$ for some $k \geq 1$. Then, using that I is generated by square-free monomials, we obtain $x_{i_1} \cdots x_{i_r} \in I$. Hence $f \in I$. To finish the proof observe that, by part (i), $\cap_{i=1}^{s} \mathfrak{p}_i$ is a monomial ideal because the intersection of monomial ideals is again a monomial ideal (see Lemma 2.2). ♠

DEFINITION 2.6. Let $x^a = x_1^{a_1} \cdots x_n^{a_n}$ be a monomial in R. The *support* of x^a is given by $\operatorname{supp}(x^a) := \{x_i \,|\, a_i > 0\}$.

PROPOSITION 2.7. *A monomial ideal $\mathfrak{q} \subset R$ is primary if and only if, after permutation of the variables, $\mathfrak{q}$ has the form:*

$$\mathfrak{q} = (x_1^{a_1}, \ldots, x_r^{a_r}, x^{b_1}, \ldots, x^{b_s}),$$

where $a_i \geq 1$ and $\cup_{i=1}^{s} \operatorname{supp}(x^{b_i}) \subset \{x_1, \ldots, x_r\}$.

PROOF. If $\operatorname{Ass}(R/\mathfrak{q}) = \{\mathfrak{p}\}$, then by permuting the variables $x_1, \ldots, x_n$ and using Theorem 2.5 one may assume that $\mathfrak{p}$ is equal to $(x_1, \ldots, x_r)$. Since $\sqrt{(\mathfrak{q})} = \mathfrak{p}$, the ideal $\mathfrak{q}$ is

minimally generated by a set of the form:

$$\{x_1^{a_1}, \ldots, x_r^{a_r}, x^{b_1}, \ldots, x^{b_s}\}.$$

Let $x_j \in \operatorname{supp}(x^{b_i})$, then $x^{b_i} = x_j x^c$, where x^c is a monomial not in $\mathfrak{q}$. Since $\mathfrak{q}$ is primary, a power of x_j is in $\mathfrak{q}$. Thus $x_j \in (x_1, \ldots, x_r)$ and consequently $1 \leq j \leq r$, as required.

For the converse note that any associated prime $\mathfrak{p}$ of $R/\mathfrak{q}$ can be written as $\mathfrak{p} = (\mathfrak{q} \colon f)$, for some monomial f. It follows readily that $(x_1, \ldots, x_r)$ is the only associated prime of $\mathfrak{q}$. ♠

COROLLARY 2.8. *If $\mathfrak{p}$ is a face ideal, then $\mathfrak{p}^n$ is a primary ideal for all n.*

PROPOSITION 2.9. *If $I \subset R$ is a monomial ideal, then I has an irredundant primary decomposition $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$, where $\mathfrak{q}_i$ is a primary monomial ideal for all i and $\sqrt{(\mathfrak{q}_i)} \neq \sqrt{(\mathfrak{q}_j)}$ if $i \neq j$.*

PROOF. Let $G(I) = \{f_1, \ldots, f_q\}$ be the set of monomials that minimally generate I. We proceed by induction on the number of variables that occur in the union of the supports of $f_1, \ldots, f_q$.

One may assume that one of the variables in $\cup_{i=1}^{q} \operatorname{supp}(f_i)$, say x_n, satisfy $x_n^i \notin I$ for all i, otherwise I is a primary ideal and there is nothing to prove. Next we permute the f_i in order to find integers $0 \leq a_1 \leq \cdots \leq a_q$, with $a_q \geq 1$, such that f_i is divisible by $x_n^{a_i}$ but by not higher power of x_n. If we apply this procedure to $(I, x_n^{a_q})$, instead of I, note that one must choose a variable different from x_n.

Since $(I \colon x_n^{a_q})$ is generated by monomials in less than n variables and because of the equality

$$I = (I, x_n^{a_q}) \cap (I \colon x_n^{a_q})$$

one may apply the argument above recursively to the two monomial ideals occurring in the intersection— and use induction—to obtain a decomposition of I into primary monomial ideals $\mathfrak{q}_1', \ldots, \mathfrak{q}_s'$ of R. Finally we remove redundant primary ideals from $\mathfrak{q}_1', \ldots, \mathfrak{q}_s'$ and group those primary ideals with the same radical. ♠

Even for monomial ideals a minimal irredundant primary decomposition is not unique. What is unique is the number of terms in such a decomposition and the primary components that correspond to minimal primes **[AM94]**.

EXAMPLE 2.10. If $I = (x^2, xy) \subset K[x, y]$, then

$$I = (x) \cap (x^2, xy, y^2) = (x) \cap (x^2, y),$$

are two minimal irredundant primary decompositions of I.

The computation of a primary decomposition of a monomial ideal can be carried out by successive elimination of powers of variables, as described in the proof of Proposition 2.9.

EXAMPLE 2.11. If $R = K[x, y, z]$ and $I = (yz^2, x^2z, x^3y^2)$, then

$$I = (z, y^2) \cap (x^2, y) \cap (z^2, x^3, x^2z).$$

COROLLARY 2.12. *If $I \subset R$ is a monomial ideal, then there is a primary decomposition $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$, such that $\mathfrak{q}_i$ is generated by powers of variables for all i.*

PROOF. Let $\mathfrak{q}$ be a primary ideal. Then, by Proposition 2.7, $\mathfrak{q}$ is minimally generated by a set of monomials $x_1^{a_1}, \ldots, x_r^{a_r}, f_1, \ldots, f_s$ such that

$$\bigcup_{i=1}^{s} \operatorname{supp}(f_i) \subset \{x_1, \ldots, x_r\},$$

where $a_i > 0$ for all i. Note that if $f_1 = x_1^{b_1} \cdots x_r^{b_r}$ and $b_1 > 0$, then $a_1 > b_1$ and one has a decomposition:

$$\mathfrak{q} = (x_1^{b_1}, x_2^{a_2}, \ldots, x_r^{a_r}, f_2, \ldots, f_s) \cap (x_1^{a_1}, x_2^{a_2}, \ldots, x_r^{a_r}, x_2^{b_2} \cdots x_r^{b_r}, f_2, \ldots, f_s),$$

where in the first ideal of the intersection we have lower the degree of $x_1^{a_1}$ and have eliminated f_1, while in the second ideal we have eliminated the variable x_1 from f_1. Applying the same argument repeatedly it follows that one can write $\mathfrak{q}$ as an intersection of primary monomial ideals such that for each of those ideals the only minimal generators that contain x_1 are pure powers of x_1. Therefore, by induction, $\mathfrak{q}$ is the intersection of ideals generated by powers of variables. Hence the result follows from Proposition 2.9. ♠

PROPOSITION 2.13. *Let I be an ideal of $R = K[x_1, \ldots, x_n]$ generated by monomials in the variables $x_1, \ldots, x_r$ with $r < n$. If*

$$I = I_1 \cap \cdots \cap I_s$$

is an irredundant decomposition of I into monomial ideals, then none of the ideals I_i can contain a monomial in $K[x_{r+1}, \ldots, x_n]$.

PROOF. Set $X = \{x_1, \ldots, x_n\}$ and $X' = X \setminus \{x_1, \ldots, x_r\}$. Assume some of the I_i's contain monomials in $K[X']$. One may split the I_i's into two sets so that $I_1, \ldots, I_m$ do not contain monomials in $K[X']$ (note m could be zero), while $I_{m+1}, \ldots, I_s$ contain monomials in the set of variables X'. For $i \geq m+1$ pick a monomial g_i in I_i whose support is contained in X'. Since the decomposition of I is irredundant there is a monomial $f \in \cap_{i=1}^{m} I_i$ and $f \notin \cap_{i=m+1}^{s} I_i$, where we set $f = 1$ if $m = 0$. To derive a contradiction consider $f_1 = f g_{m+1} \cdots g_s$. As $f_1 \in I$, we get $f \in I$ which is absurd. ♠

COROLLARY 2.14. *Let $I \subset R = K[x_1, \ldots, x_n]$ be an ideal generated by monomials in the variables $x_1, \ldots, x_r$ with $r < n$. If*

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$$

is an irredundant primary decomposition into monomial ideals, then $\mathfrak{q}_i$ is generated by monomials in $K[x_1, \ldots, x_r]$.

PROOF. It follows from Propositions 2.7 and 2.13. ♠

DEFINITION 2.15. An ideal I of a ring R is called *irreducible* if I cannot be written as an intersection of two ideals of R that properly contain I.

PROPOSITION 2.16. *If $I \subset R = K[x_1, \ldots, x_n]$ is a monomial ideal, then I is irreducible if and only if up to permutation of the variables*

$$I = (x_1^{a_1}, \ldots, x_r^{a_r}), \;\; a_i > 0 \, \forall \, i.$$

PROOF. $\Rightarrow$) Since I must be primary (see Proposition 1.32) from the proof of Corollary 2.12 one derives that I is generated by powers of variables.

$\Leftarrow$) If I is reducible, then $I = I_1 \cap I_2$ for some ideals I_1 and I_2 that properly contain I. Pick $f \in I_1 \setminus I$ (resp. $g \in I_2 \setminus I$) with the smallest possible number of terms. We can write

$$f = \lambda_1 x^{\gamma_1} + \cdots + \lambda_s x^{\gamma_s}; \quad 0 \neq \lambda_i \in K \text{ for all } i.$$

Let $1 \leq k \leq r$ be an integer and let $x_k^{b_i}$ be the maximum power of x_k that divides x^{γ_i}, i.e., we can write $x^{\gamma_i} = x_k^{b_i} x^{\delta_i}$, where x_k does not divide x^{δ_i}. After permuting terms we may assume that $b_1 \geq \cdots \geq b_s$. Note that $x_k^{a_k}$ does not divide x^{γ_i} for all i, k, otherwise we can find a polynomial in $I_1 \setminus I$, namely $f - \lambda_i x^{\gamma_i}$, with less than s terms. Thus $b_i < a_k$ for all i. We claim that $b_1 = \cdots = b_s$. We proceed by contradiction assuming that $b_p > b_{p+1}$ for some p. From the equality

$$x_k^{a_k - b_p} f = x_k^{a_k - b_p}(\lambda_1 x^{\gamma_1} + \cdots + \lambda_p x^{\gamma_p}) + x_k^{a_k - b_p}(\lambda_{p+1} x^{\gamma_{p+1}} + \cdots + \lambda_s x^{\gamma_s})$$

we obtain that the polynomial $x_k^{a_k - b_p}(\lambda_{p+1} x^{\gamma_{p+1}} + \cdots + \lambda_s x^{\gamma_s})$ is in $I_1 \setminus I$ and has fewer terms than f, a contradiction. This completes the proof of the claim. Therefore we can write $f = x_1^{c_1} \cdots x_r^{c_r} f_1$ and $g = x_1^{d_1} \cdots x_r^{d_r} g_1$, where f_1 and f_2 are in $R' = K[x_{r+1}, \ldots, x_n]$. Setting $e_i = \max\{c_i, d_i\}$ we get that $h = x_1^{e_1} \cdots x_r^{e_r} f_1 g_1$ is in $I_1 \cap I_2$, i.e., $h \in I$, a contradiction because $e_i < a_i$ for all i and $f_1 g_1 \in R'$. Thus I is irreducible. ♠

THEOREM 2.17. *If $I \subset R$ is a monomial ideal, then there is a unique irredundant decomposition $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ such that $\mathfrak{q}_i$ is an irreducible monomial ideal.*

PROOF. The existence follows from Corollary 2.12. For the uniqueness assume one has two irredundant decompositions:

$$\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r = \mathfrak{q}'_1 \cap \cdots \cap \mathfrak{q}'_s,$$

where $\mathfrak{q}_i$ and $\mathfrak{q}'_j$ are irreducible for all i, j. Using the arguments given in the proof of Proposition 2.16 one concludes that for each i, there is σ_i such that $\mathfrak{q}_{\sigma_i} \subset \mathfrak{q}'_i$ and vice versa for each j there is π_j such that $\mathfrak{q}'_{\pi_j} \subset \mathfrak{q}_j$. Therefore $r = s$ and $\mathfrak{q}_i = \mathfrak{q}'_{\rho_i}$ for some permutation ρ. ♠

COROLLARY 2.18. *Let $R = K[x_1, \ldots, x_n]$ be a polynomial ring with the standard grading over a field K and let I be a graded ideal of R of dimension 0. Then the following hold.*

(a) *I is Gorenstein if and only if I is irreducible.*
(b) *If I is a monomial ideal, then I is Gorenstein if and only if it has the form $I = (x_1^{a_1}, \ldots, x_n^{a_n})$.*

PROOF. (a) Recall that the socle of R/I is $\operatorname{Soc}(R/I) = (I \colon \mathfrak{m})/I$ and that R/I is Gorenstein if and only if $\dim_K(I \colon \mathfrak{m})/I = 1$. Thus this part follows from Theorem 1.105.

(b) It follows from part (a) and Proposition 2.16. ♠

2.2. Gröbner bases

In this part we review some basic facts and definitions on Gröbner bases, including the division algorithm and elimination theory.

Let K be a field and let $S = K[t_1, \ldots, t_s]$ be a polynomial ring with the standard grading. A *monomial* of S is an element of the form:

$$t^a = t_1^{a_1} \cdots t_s^{a_s}, \quad a = (a_1, \ldots, a_s) \in \mathbb{N}^s.$$

The set of monomials of S is denoted by $\mathbb{M}_s = \{t^a \mid a \in \mathbb{N}^s\}$.

DEFINITION 2.19. A total order $\succ$ of $\mathbb{M}_s$ is called a *monomial order* if

(a) $t^a \succeq 1$ for all $t^a \in \mathbb{M}_s$, and
(b) for all $t^a, t^b, t^c \in \mathbb{M}_s$, $t^a \succ t^b$ implies $t^a t^c \succ t^b t^c$.

Two examples of monomial orders of $\mathbb{M}_s$ are the *lexicographical order* (*lex order* for short) defined as $t^b \succ t^a$ iff the first non-zero entry of $b - a$ is positive, and the *reverse lexicographical order* (*revlex order* for short) given by $t^b \succ t^a$ iff the last non-zero entry of $b - a$ is negative.

In what follows we assume that a monomial order $\prec$ for $\mathbb{M}_s$ has been fixed. Let f be a non-zero polynomial in S. Then one can write

$$f = \sum_{i=1}^{r} \lambda_i t^{\alpha_i},$$

with $\lambda_i \in K^* = K \setminus \{0\}$, $t^{\alpha_i} \in \mathbb{M}_s$ and $t^{\alpha_1} \succ \cdots \succ t^{\alpha_r}$. The *leading monomial* t^{α_1} of f is denoted by $\mathrm{in}_\prec(f)$ or $\mathrm{lm}_\prec(f)$, or simply by $\mathrm{in}(f)$. The *leading coefficient* λ_1 of f and the *leading term* $\lambda_1 t^{\alpha_1}$ of f are denoted by $\mathrm{lc}(f)$ and $\mathrm{lt}(f)$, respectively.

DEFINITION 2.20. Let I be an ideal of S. The *initial ideal* of I, denoted by $\mathrm{in}_\prec(I)$ or simply by $\mathrm{in}(I)$, is the monomial ideal given by

$$\mathrm{in}_\prec(I) = (\{\mathrm{in}_\prec(f) | \, f \in I\}).$$

LEMMA 2.21 (Dickson). *If $\{t^{\alpha_i}\}_{i=1}^{\infty}$ is a sequence in $\mathbb{M}_s$, then there is an integer k so that t^{α_i} is a multiple of some monomial in the set $\{t^{\alpha_1}, \ldots, t^{\alpha_k}\}$ for every $i > k$.*

PROOF. Let $I \subset K[t_1, \ldots, t_s]$ be the ideal generated by $\{t^{\alpha_i}\}_{i=1}^{\infty}$. By the Hilbert's basis theorem I is finitely generated (see Theorem 1.6). It is seen that I can be generated by a finite set of monomials $t^{\alpha_1}, \ldots, t^{\alpha_k}$. Hence for each $i > k$, there is $1 \leq j \leq k$ such that t^{α_i} is a multiple of t^{α_j}. ♠

DEFINITION 2.22. Let $\mathcal{F} = \{f_1, \ldots, f_s\} \subset S \setminus \{0\}$ be a set of polynomials in S. One says that f *reduces* to g *modulo* $\mathcal{F}$, denoted $f \longrightarrow_{\mathcal{F}} g$, if

$$g = f - (\lambda u / \mathrm{lc}(f_i)) f_i$$

for some $f_i \in \mathcal{F}$, $u \in \mathbb{M}_s$, $\lambda \in K^*$ such that $\lambda \cdot u \cdot \mathrm{in}_\prec(f_i)$ occurs in f with coefficient λ.

PROPOSITION 2.23. *The reduction relation "$\longrightarrow_{\mathcal{F}}$" is Noetherian, that is, any sequence of reductions $g_1 \longrightarrow_{\mathcal{F}} \cdots \longrightarrow_{\mathcal{F}} g_i \longrightarrow_{\mathcal{F}} \cdots$ is stationary.*

PROOF. Notice that at the ith step of the reduction some term of g_i is replaced by terms of lower degree. Therefore if the sequence above is not stationary, then there is a never ending decreasing sequence of terms in $\mathbb{M}_s$, but this is impossible according to Dickson's lemma. ♠

THEOREM 2.24. (Division algorithm [**ErH11**, Theorem 2.11]) *If $f, f_1, \ldots, f_r$ are polynomials in S, then f can be written as*

$$f = a_1 f_1 + \cdots + a_r f_r + g,$$

where $a_i, g \in S$ and either $g = 0$ or $g \neq 0$ and no term of g is divisible by one of $\mathrm{in}_\prec(f_1), \ldots, \mathrm{in}_\prec(f_r)$. Furthermore if $a_i f_i \neq 0$, then $\mathrm{in}_\prec(f) \geq \mathrm{in}_\prec(a_i f_i)$.

DEFINITION 2.25. The polynomial g in the division algorithm is called a *remainder* of f with respect to $\mathcal{F} = \{f_1, \ldots, f_r\}$.

DEFINITION 2.26. Let $I \neq (0)$ be an ideal of S and let $\mathcal{G} = \{g_1, \ldots, g_r\}$ be a subset of I. The set $\mathcal{G}$ is called a *Gröbner basis* of I if

$$\text{in}_\prec(I) = (\text{in}_\prec(g_1), \ldots, \text{in}_\prec(g_r)).$$

DEFINITION 2.27. A Gröbner basis $\mathcal{G} = \{g_1, \ldots, g_r\}$ of an ideal I is called a *reduced Gröbner basis* for I if:

(i) $\text{lc}(g_i) = 1$ for all i, and
(ii) none of the terms occurring in g_i belongs to $\text{in}_\prec(\mathcal{G} \setminus \{g_i\})$ for all i.

THEOREM 2.28. **[ErH11**, Theorem 2.17] *Each ideal I has a unique reduced Gröbner basis.*

DEFINITION 2.29. Let $f, g \in S$ and let $[f, g] = \text{lcm}(f, g)$be its least common multiple. The S-*polynomial* of f and g is given by

$$\text{S}(f, g) = \frac{[\text{in}(f), \text{in}(g)]}{\text{lt}(f)} f - \frac{[\text{in}(f), \text{in}(g)]}{\text{lt}(g)} g,$$

Given a set of generators of a polynomial ideal one can determine a Gröbner basis using the next fundamental procedure:

THEOREM 2.30. (Buchberger **[Buc]**) If $\mathcal{F} = \{f_1, \ldots, f_r\}$ is a set of generators of an ideal I of S, then one can construct a Gröbner basis for I using the following algorithm:

Input: $\mathcal{F}$
Output: a Gröbner basis $\mathcal{G}$ for I
Initialization: $\mathcal{G} := \mathcal{F}$, $B := \{\{f_i, f_j\} \,|\, f_i \neq f_j \in \mathcal{G}\}$
while $B \neq \emptyset$ do
  pick any $\{f, g\} \in B$
  $B := B \setminus \{\{f, g\}\}$
  $r :=$ remainder of $\text{S}(f, g)$ with respect to $\mathcal{G}$
  if $r \neq 0$ then
    $B := B \cup \{\{r, h\} \,|\, h \in \mathcal{G}\}$
    $\mathcal{G} := \mathcal{G} \cup \{r\}$

PROPOSITION 2.31. *Let I be an ideal of S and let $\mathcal{G} = \{g_1, \ldots, g_r\}$ be a Gröbner basis of I. If*

$$\mathcal{B} = \{\overline{u} \,|\, u \in \mathbb{M}_n \text{ and } u \notin (\text{in}(g_1), \ldots, \text{in}(g_r))\},$$

then $\mathcal{B}$ is a basis for the K-vector space S/I.

PROOF. First we show that $\mathcal{B}$ is a generating set for S/I. Take $\overline{f} \in S/I$. Since "$\longrightarrow_{\mathcal{G}}$" is Noetherian, we can write $f = \sum_{i=1}^{r} a_i g_i + \sum_{i=1}^{p} \lambda_i u_i$, where $\lambda_i \in K^*$ and such that every u_i is a term which is not a multiple of any of the terms $\text{in}(g_j)$. Accordingly $\overline{u}_i$ is in $\mathcal{B}$ for all i and $\overline{f}$ is a linear combination of the $\overline{u}_i$'s.

To prove that $\mathcal{B}$ is linearly independent assume $h = \sum_{i=1}^{r} \lambda_i u_i \in I$, where $u_i \in \mathcal{B}$ and $\lambda_i \in K$. We must show $h = 0$. If $h \neq 0$, then we can label the u_i's so that $u_1 \succ \cdots \succ u_s$ and $\lambda_1 \neq 0$. Hence $\text{in}(h) = u_1 \in \text{in}(I)$, but this is a clear contradiction because $\text{in}(I) = (\text{in}(g_1), \ldots, \text{in}(g_r))$. Therefore $h = 0$, as required. ♠

DEFINITION 2.32. An ideal $I \subset S$ is *graded* if I is generated by homogeneous polynomials.

PROPOSITION 2.33. *Let $I \subset S$ be an ideal. The following conditions are equivalent*:

(a) *I is a graded ideal.*

(b) *If $f = \sum_{d=0}^{r} f_d$ is in I, $f_d \in S_d$ for $d = 0, \ldots, r$, then each f_d is in I.*

PROOF. It follows at once from Proposition 1.98. ♠

COROLLARY 2.34 (Macaulay). *If I is a graded ideal of S, then S/I and $S/\text{in}_{\prec}(I)$ have the same Hilbert function and the same degree and index of regularity.*

LEMMA 2.35. **[ErH11**, Proposition 2.15] *Let f, g be polynomials in S and let $\mathcal{F} = \{f, g\}$. If $\text{in}(f)$ and $\text{in}(g)$ are relatively prime, then $\text{S}(f, g) \longrightarrow_{\mathcal{F}} 0$.*

THEOREM 2.36. **[Buc]** *Let I be an ideal of S and let $\mathcal{F} = \{f_1, \ldots, f_s\}$ be a set of generators of I, then $\mathcal{F}$ is a Gröbner basis for I if and only if*

$$\text{S}(f_i, f_j) \longrightarrow_{\mathcal{F}} 0 \text{ for all } i \neq j.$$

Elimination of variables. Let $K[x_1, \ldots, x_n, t_1, \ldots, t_s]$ be a polynomial ring over a field K. A useful monomial order is the *elimination order* with respect to the variables $x_1, \ldots, x_n$. This order is given by

$$x^a t^c \succ x^b t^d$$

if and only if $\deg(x^a) > \deg(x^b)$, or both degrees are equal and the last non-zero entry of $(a, c) - (b, d)$ is negative. The elimination order with respect to all variables $x_1, \ldots, x_n, t_1, \ldots, t_s$ is defined accordingly. This order is called the GRevLex order.

THEOREM 2.37. *Let $B = K[x_1, \ldots, x_n, t_1, \ldots, t_s]$ be a polynomial ring over a field K with a monomial order $\prec$ such that monomials in the x_i's are greater than monomials in the t_i's. If I is an ideal of B with a Gröbner basis $\mathcal{G}$, then $\mathcal{G} \cap K[t_1, \ldots, t_s]$ is a Gröbner basis of $I \cap K[t_1, \ldots, t_s]$.*

PROOF. Set $S = K[t_1, \ldots, t_s]$ and $I^c = I \cap S$. If M is a monomial in $\text{in}(I^c)$, there is $f \in I^c$ with $\text{lm}(f) = M$. Hence $M = m\text{lm}(g)$ for some $g \in \mathcal{G}$, because $\mathcal{G}$ is a Gröbner basis. Since $M \in S$ and $x^\alpha \succ t^\beta$ for all α and β we obtain $g \in \mathcal{G} \cap S$, that is, $M \in (\text{in}(\mathcal{G} \cap S))$. Thus $\text{in}(I^c) = (\text{in}(\mathcal{G} \cap S))$, as required. ♠

EXAMPLE 2.38. Let $\prec$ be the *elimination order* with respect to $x_1, \ldots, x_4$. Using *Macaulay*2 **[GSb]**, we can compute the reduced Gröbner basis of

$$I = (t_1 - x_1x_2, t_2 - x_1x_3, t_3 - x_1x_4, t_4 - x_2x_3, t_5 - x_2x_4, t_6 - x_3x_4).$$

By Theorem 2.37, it follows that $I \cap K[t_1, \ldots, t_6] = (t_3t_4 - t_1t_6, t_2t_5 - t_1t_6)$.

DEFINITION 2.39. Let I and J be two ideals of a ring S. The ideal

$$(I\colon J) := \{f \in S \mid fJ \subset I\}$$

is called the *colon ideal* of I w.r.t J. If $f \in S$, we set $(I\colon (f)) := (I\colon f)$ and we call $(I\colon f)$ the *colon ideal* of I with respect to f.

DEFINITION 2.40. Let I and J be two ideals of a ring S. The ideal

$$(I\colon J^\infty) = \bigcup_{i \geq 1} (I\colon J^i)$$

is the *saturation* of I w.r.t J.If $f \in S$, we set $(I\colon (f)^\infty) := (I\colon f^\infty)$.

The saturation can be computed by elimination of variables using the following result.

PROPOSITION 2.41. *Let $S[t]$ be a polynomial ring in one variable over a ring S and let I be an ideal of S. If $f \in S$, then*

$$(I\colon f^\infty) = \bigcup_{i \geq 1} (I\colon f^i) = (I, 1 - tf) \cap S.$$

PROOF. Let $g \in (I, 1 - tf) \cap S$. Then $g = \sum_{i=1}^{s} a_i f_i + a_{s+1}(1 - tf)$, where $f_i \in I$ and $a_i \in S[t]$. Making $t = 1/f$ in the last equation and multiplying by f^m, with m large enough, one derives an equality

$$gf^m = b_1f_1 + \cdots + b_sf_s,$$

where $b_i \in S$. Hence $gf^m \in I$ and $g \in (I\colon f^\infty)$.

Conversely let $g \in (I\colon f^\infty)$, hence there is $m \geq 1$ such that $gf^m \in I$. Since one can write

$$g = (1 - t^m f^m)g + t^m f^m g \text{ and } 1 - t^m f^m = (1 - tf)b,$$

for some $b \in S[t]$, one derives $g \in (I, 1 - tf) \cap S$. ♠

LEMMA 2.42. *Let $B = K[y_1, \ldots, y_n, t_1, \ldots, t_s]$ be a polynomial ring over a field K. If I is a binomial ideal of B, then the reduced Gröbner basis of I with respect to any term order consists of binomials and $I \cap K[t_1, \ldots, t_s]$ is a binomial ideal.*

PROOF. Let $\mathcal{B}$ be a finite set of generators of I consisting of binomials and let $f, g \in \mathcal{B}$. Since the S-polynomial $\mathrm{S}(f, g)$ is again a binomial and the remainder of $S(f, g)$ with respect to $\mathcal{B}$ is also a binomial, it follows that the output of the Buchberger's algorithm (see Theorem 2.30) is a Gröbner basis of I consisting of binomials. Hence if $\mathcal{G}$ is the reduced Gröbner basis of I, then $\mathcal{G}$ consists of binomials.

If $\prec$ is the lex order $y_1 \succ \cdots \succ y_n \succ t_1 \succ \cdots \succ t_s$ and $K[\mathbf{t}]$ is the ring $K[t_1, \ldots, t_s]$, then by elimination theory (see Theorem 2.37) $\mathcal{G} \cap K[\mathbf{t}]$ is a Gröbner basis of $I \cap K[\mathbf{t}]$. Hence $I \cap K[\mathbf{t}]$ is a binomial ideal. ♠

Computation of Hilbert series. Let R be a polynomial ring over a field K with a monomial order $\prec$ and let $I \subset R$ be a graded ideal. Since R/I and $R/\mathrm{in}_\prec(I)$ have the same Hilbert function (see Corollary 2.34), the actual computation of the Hilbert series of R/I is a two-step process:

- first one finds a Gröbner basis of I using Buchberger's algorithm, and
- second one computes the Hilbert series of $R/\mathrm{in}_\prec(I)$ using elimination of variables.

EXAMPLE 2.43. Let $R = K[x_1, x_2, x_3]$ be a polynomial ring and let $I = (x_1^2, x_2^2 x_3, x_2^3)$. Let us compute the Hilbert series of R/I using elimination. Pick any monomial involving more than one variable, say $x_2^2 x_3$. The idea is to eliminate x_2^2 from the monomials containing more than one variable. From the exact sequence of graded modules:

$$0 \longrightarrow R/(x_1^2, x_3, x_2)(-2) \xrightarrow{x_2^2} R/I \longrightarrow R/(x_1^2, x_2^2) \longrightarrow 0,$$

and we get,

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

2.3. Hilbert functions

In this section we introduced the tools from commutative algebra and affine and projective varieties needed to study Reed-Muller type codes. In particular we study the behavior of Hilbert functions and examine the main algebraic invariants of graded ideals and affine algebras (e.g., degree, index of regularity,regularity).

Let $S = K[t_1, \ldots, t_s] = \oplus_{d=0}^{\infty} S_d$ be a graded polynomial ring, over the field K, with the standard grading, that is, each t_i is homogeneous of degree one and S_d is the set of homogeneous polynomials of total degree d in S, together with the zero polynomial. The set S_d is a K-vector space of dimension $\binom{d+s-1}{s-1}$. As usual, $\mathfrak{m}$ will denote the maximal ideal of S generated by $t_1, \ldots, t_s$. The vector space of polynomials in S (resp. I) of degree at most i is denoted by $S_{\leq i}$ (resp. $I_{\leq i}$). The functions

$$H_I^a(i) = \dim_K(S_{\leq i}/I_{\leq i}) \quad \text{and} \quad H_I(i) = H_I^a(i) - H_I^a(i-1)$$

are called the *affine Hilbert function* and the *Hilbert function* of the *affine algebra* S/I, respectively.

DEFINITION 2.44. The *graded reverse lexicographical order* (GRevLex for short) on the monomials of S is defined as $t^b \succ t^a$ if and only if $\deg(t^b) > \deg(t^a)$, or $\deg(t^b) = \deg(t^a)$ and the last nonzero entry of $b - a$ is negative.

Let $\succ$ be the GRevLex order on the monomials of $S[u]$, where $u = t_{s+1}$ is a new variable this order extends the GRevLex on the monomials of S. For $f \in S$ of degree e define

$$f^h = u^e f\,(t_1/u, \ldots, t_s/u)\,;$$

that is, f^h is the *homogenization* of the polynomial f with respect to u. The *homogenization* of I is the ideal I^h of $S[u]$ given by $I^h = (f^h | \, f \in I)$, and $S[u]$ is given the standard grading.

The Gröbner bases of I and I^h are nicely related.

DEFINITION 2.45. The integer $a_k(k!)$, denoted by $\deg(S/I)$, is called the *degree* of S/I.

LEMMA 2.46. *Let I be an ideal of S spanned by a finite set $\mathcal{G}$ and let $\succ$ be the GRevLex order on S and $S[u]$, respectively. Setting $\mathcal{G}^h = \{g^h | \, g \in \mathcal{G}\}$ and $\operatorname{in}\{\mathcal{G}^h\} = \{\operatorname{in}(g^h) | \, g \in \mathcal{G}\}$, the following hold.*

(a) *If* $\operatorname{in}(\mathcal{G}^h) = (\operatorname{in}\{\mathcal{G}^h\})$, *then* $\operatorname{in}(I) = (\{\operatorname{in}(g) | \, g \in \mathcal{G}\})$ *and* $I^h = (\mathcal{G}^h)$.
(b) $\mathcal{G}$ *is a Gröbner basis of I if and only if $\mathcal{G}^h$ is a Gröbner basis of I^h.*
(c) $\dim(S[u]/I^h) = \dim(S/I) + 1$.
(d) $H_I^a(i) = H_{I^h}(i)$ *for* $i \geq 0$.
(e) $\deg(S/I) = \deg(S[u]/I^h)$.

PROOF. (a) We set $\mathcal{G} = \{g_1, \ldots, g_r\}$ and $\operatorname{in}\{\mathcal{G}\} = \{\operatorname{in}(g) | \, g \in \mathcal{G}\}$. To show the first equality we need only show that $\operatorname{in}(I) \subset (\operatorname{in}\{\mathcal{G}\})$. Let m be a monomial in the ideal $\operatorname{in}(I)$. There is $g \in I$, of degree e, such that $\operatorname{in}(g) = m$. Writing $g = \sum_{i=1}^r f_i g_i$ for some $f_1, \ldots, f_r$

in S, from the equality

$$\frac{g^h}{u^e} = \sum_{i=1}^{r} f_i\left(\frac{t_1}{u},\ldots,\frac{t_s}{u}\right) g_i\left(\frac{t_1}{u},\ldots,\frac{t_s}{u}\right) \tag{2.3.1}$$

we get $u^s g^h \in (\mathcal{G}^h)$ for $s \gg 0$. As $\operatorname{in}(g^h) = \operatorname{in}(g)$, one has $\operatorname{in}(u^s g^h) = u^s m$. Hence $u^s m \in (\operatorname{in}\{\mathcal{G}^h\})$. Using $\operatorname{in}(g_i) = \operatorname{in}(g_i^h)$ yields $m \in (\operatorname{in}\{\mathcal{G}\})$.

To show the second equality it is enough to show that $\{g^h | \, g \in I\} \subset (\mathcal{G}^h)$. By the first equality $\mathcal{G}$ is a Gröbner basis of I. Hence any $g \in I$ can be written as $g = \sum_{i=1}^{r} f_i g_i$, where $\operatorname{in}(g) \succeq \operatorname{in}(f_i g_i)$ for all i. Notice that $e = \deg(g) \geq \deg(f_i g_i) = \deg(f_i) + \deg(g_i)$. Since Eq. (2.3.1) holds, it follows that $g^h \in (g_1^h, \ldots, g_r^h)$.

(b) $\Rightarrow$) By part (a) we need only show that $\operatorname{in}(\mathcal{G}^h) \subset (\operatorname{in}\{\mathcal{G}^h\})$. Let $m \in \operatorname{in}(\mathcal{G}^h)$ be a term, then $m = \operatorname{in}(g)$ for some $g \in (\mathcal{G}^h)$. We may assume that g is homogeneous. We can write $g = u^p(m_1 + m_2 u^{e_2} + \cdots + m_s u^{e_s})$, where $m_1, \ldots, m_s$ are monomials in S such that $m_1 \succ m_2 u^{e_2} \succ \cdots \succ m_s u^{e_s}$. As all $m_i u^{e_i}$ have the same degree we obtain $0 \leq e_2 \leq \cdots \leq e_s$. It follows that $g' = g(t_1, \ldots, t_s, 1)$ belongs to I and $\operatorname{in}(g') = m_1$. Therefore m_1 belongs to $\operatorname{in}(I) = (\operatorname{in}\{\mathcal{G}\})$. Since $\operatorname{in}(g_i) = \operatorname{in}(g_i^h)$ we obtain that $m \in (\operatorname{in}\{\mathcal{G}^h\})$.

$\Leftarrow$) This implication follows from part (a).

(c): By (b) $\{g^h | \, g \in \mathcal{G}\}$ is a Gröbner basis of I^h and $\operatorname{in}_\prec(g) = \operatorname{in}_\prec(g^h)$ for $g \in \mathcal{G}$. Since $\dim(S/I) = \dim(S/\operatorname{in}_\prec(I))$ and

$$\dim(S[u]/I) = \dim(S[u]/\operatorname{in}_\prec(I^h)),$$

the equality follows.

(d): Fix $i \geq 0$. The mapping $S[u]_i \to S_{\leq i}$ induced by mapping $u \mapsto 1$ is a K-linear surjection. Consider the induced composite K-linear surjection $S[u]_i \to S_{\leq i} \to S_{\leq i}/I_{\leq i}$. An easy check shows that this has kernel I_i^h. Hence, we have a K-linear isomorphism of finite-dimensional K-vector spaces

$$S[u]_i/I_i^h \simeq S_{\leq i}/I_{\leq i}.$$

Thus $H_I^a(i) = H_{I^h}(i)$.

(e): By (c), $\dim(S[u]/I^h)$ is equal to $\dim(S/I) + 1$. Hence the equality follows from (d). ♠

PROPOSITION 2.47. *Let $I \subset S$ be an ideal and let k be the Krull dimension of S/I. Then there are unique polynomials*

$$h_I^a(t) = \sum_{j=0}^{k} a_j t^j \in \mathbb{Q}[t] \;\; \textit{and} \;\; h_I(t) = \sum_{j=0}^{k-1} c_j t^j \in \mathbb{Q}[t]$$

of degrees k and $k-1$, respectively, such that $h_I^a(i) = H_I^a(i)$ and $h_I(i) = H_I(i)$ for $i \gg 0$.

PROOF. Let I^h be the homogenization of I relative to a new variable u. By Lemma 2.46, $H_I^a(i) = H_{I^h}(i)$ for $i \gg 0$. Thanks to Theorem 1.115, the Hilbert function of I^h is a polynomial function of degree equal to $\dim(S[u]/I^h) - 1$. Since $\dim(S[u]/I^h) = \dim(S/I) + 1$, we get that H_I^a is a polynomial function of degree k. That H_I is a polynomial function of degree $k-1$ follows recalling that $H_I(i) = H_I^a(i) - H_I^a(i-1)$ for $i \geq 1$. ♠

DEFINITION 2.48. The polynomials h_I^a and h_I are called the *affine Hilbert polynomial* and the *Hilbert polynomial* of S/I.

REMARK 2.49. Notice that $a_k(k!) = c_{k-1}((k-1)!)$ for $k \geq 1$. If $k = 0$, then $H_I^a(i) = \dim_K(S/I)$ for $i \gg 0$ and the degree of S/I is just $\dim_K(S/I)$.

DEFINITION 2.50. The *regularity index* of S/I, denoted by $\mathrm{ri}(S/I)$, is the least integer $r \geq 0$ such that $h_I(d) = H_I(d)$ for $d \geq r$. The *affine regularity index* of S/I, denoted by $\mathrm{ri}^a(S/I)$, is the least integer $r \geq 0$ such that $h_I^a(d) = H_I^a(d)$ for $d \geq r$.

DEFINITION 2.51. Let $I \subset S$ be a graded ideal and let $\mathbb{F}_\star$ be the minimal graded free resolution of S/I as an S-module:

$$\mathbb{F}_\star: \quad 0 \to \bigoplus_j S(-j)^{b_{gj}} \to \cdots \to \bigoplus_j S(-j)^{b_{1j}} \to S \to S/I \to 0.$$

The *Castelnuovo–Mumford regularity* of S/I (*regularity* of S/I for short) is defined as

$$\mathrm{reg}(S/I) = \max\{j - i \,|\, b_{ij} \neq 0\}.$$

A reference for the regularity of graded ideals see **[Eis05]**. There are methods to compute the regularity of S/I avoiding the construction of a minimal graded free resolution; see **[BG00, BG06]** and **[GP12]**. These methods work for any homogeneous ideal over an arbitrary field.

LEMMA 2.52. **[Eis13]** *If $0 \to N \to M \to L \to 0$ is a short exact sequence of graded finitely generated R-modules, then*

(a) $\mathrm{reg}(N) \leq \max(\mathrm{reg}(M), \mathrm{reg}(L) + 1)$.
(b) $\mathrm{reg}(M) \leq \max(\mathrm{reg}(N), \mathrm{reg}(L))$.
(c) $\mathrm{reg}(L) \leq \max(\mathrm{reg}(N) - 1, \mathrm{reg}(M))$.

The a-invariant, the regularity, and the depth of S/I are closely related.

THEOREM 2.53. **[Vas04**, Corollary B.4.1] *$a(S/I) \leq \mathrm{reg}(S/I) - \mathrm{depth}(S/I)$, with equality if S/I is Cohen–Macaulay.*

If S has the standard grading and I is a graded Cohen-Macaulay ideal of S of dimension 1, then $\operatorname{reg}(S/I)$, the Castelnuovo-Mumford regularity of S/I is equal to the regularity index of S/I. This follows from Theorem 2.53. In this case we call $\operatorname{ri}(S/I)$ (resp. $\operatorname{ri}^a(S/I)$) the regularity (resp. affine regularity) of S/I and denote this number by $\operatorname{reg}(S/I)$ (resp. $\operatorname{reg}^a(S/I)$).

DEFINITION 2.54. Let $I \subset S$ be a graded ideal and let $f_1, \ldots, f_r$ be a minimal homogeneous generating set of I. The *big degree* of I is defined as $\operatorname{bigdeg} I = \max_i\{\deg(f_i)\}$.

If I is graded its regularity is related to the degrees of a minimal generating set of I. From the definition of the regularity of S/I, one has:

PROPOSITION 2.55. **[Eis05]** $\operatorname{bigdeg} I - 1 \leq \operatorname{reg}(S/I)$.

REMARK 2.56. If I is graded, I_d is a vector subspace of S_d and

$$H^a_I(d) = \textstyle\sum_{i=0}^{d} \dim_K(S_d/I_d)$$

for $d \geq 0$. Thus, one has $H_I(d) = \dim_K(S_d/I_d)$ for all d.

DEFINITION 2.57. Let $I \subset S$ be a graded ideal. The *Hilbert series* of S/I, denoted by $F_I(t)$, is given by

$$F_I(t) := \sum_{d=0}^{\infty} H_I(d)t^d = \sum_{d=0}^{\infty} \dim_K(S/I)_d t^d.$$

THEOREM 2.58. (Hilbert–Serre) *Let $I \subset S$ be a graded ideal. Then there is a unique polynomial $h(t) \in \mathbb{Z}[t]$ such*

$$F_I(t) = \frac{h(t)}{(1-t)^{\rho}} \ \text{ and } \ h(1) > 0,$$

where $\rho = \dim(S/I)$.

PROOF. It follows from Theorem 1.111 because K is an Artinian ring. ♠

DEFINITION 2.59. Let $I \subset S$ be a graded ideal. The *a-invariant* of the graded ring S/I, denoted by $a(S/I)$, is the degree of $F_I(t)$ as a rational function, i.e.,

$$a(S/I) = \deg(h(t)) - \rho.$$

THEOREM 2.60. (Hilbert **[BH98**, Theorem 4.1.3]) *Let $I \subset S$ be a graded ideal of dimension k. Then there is a polynomial $h_I(t) \in \mathbb{Q}[t]$ of degree $k-1$ such that $h_I(d) = H_I(d)$ for $d \gg 0$.*

PROOF. It follows from Theorem 1.115 because K is an Artinian ring. ♠

REMARK 2.61. The leading coefficient of the Hilbert polynomial $h_I(t)$ is $h(1)/(k-1)!$. Thus $h(1)$ is equal to $\deg(S/I)$.

LEMMA 2.62. *If $I \subset S$ is an ideal generated by homogeneous polynomials $f_1, \ldots, f_r$, with $r = \operatorname{ht}(I)$ and $\delta_i = \deg(f_i)$, then the Hilbert series, the degree, and the regularity of S/I are given by*

$$F_I(t) = \frac{\prod_{i=1}^{r}(1-t^{\delta_i})}{(1-t)^s},\ \deg(S/I) = \delta_1 \cdots \delta_r,\ \textit{and}\ \operatorname{reg}(S/I) = \sum_{i=1}^{r}(d_i - 1).$$

PROOF. As S/I is Cohen–Macaulay, the result follows from Lemma 1.106, Theorem 2.53, and Remark 2.61. ♠

LEMMA 2.63. *If $I \subset S$ is a graded ideal and u is a new variable, then $a(S/I) = a(S[u]/I) + 1$.*

PROOF. Let $F_1(t)$ and $F_2(t)$ be the Hilbert series of the graded rings S/I and $S[u]/I$ respectively. Using additivity of Hilbert series, from the exact sequence

$$0 \to (S[u]/I)[-1] \xrightarrow{u} S[u]/I \to S[u]/(I,u) \to 0,$$

we get $F_2(t) = F_1(t)/(1-t)$, that is, $\deg(F_1) = 1 + \deg(F_2)$. ♠

LEMMA 2.64. **[Vil15**, Corollary 5.1.9] *Let $I \subset S$ be a graded ideal. Then $\operatorname{ri}(S/I) = 0$ if $a(S/I) < 0$, and $\operatorname{ri}(S/I) = a(S/I) + 1$ otherwise.*

PROOF. It follows from Corollary 1.119. ♠

LEMMA 2.65. *Let $I \subset S$ be a graded ideal. If $\dim(S/I) = 1$ and $\deg(S/I) \geq 2$, then $\operatorname{ri}(S/I) = \operatorname{ri}^a(S/I) + 1$.*

PROOF. Let u be a new variable. The affine regularity index of S/I is the regularity index of $S[u]/I$ because I is graded. Hence, by Lemmas 2.63 and 1.119 it suffices to show that $a(S/I) \geq 0$. If $a(S/I) < 0$, the Hilbert series of S/I has the form $F_I(t) = 1/(1-t)$, i.e., $H_I(d) = 1$ for $d \geq 0$ and $\deg(S/I) = 1$, a contradiction. ♠

LEMMA 2.66. Let $I \subset S$ be an ideal and let $I = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \cdots \cap \mathfrak{q}_m$ be an irredundant primary decomposition. If $J = \cap_{i=2}^{m} \mathfrak{q}_i$, then $\dim(S/(\mathfrak{q}_1 + J)) < \dim(S/J)$.

PROPOSITION 2.67. (Additivity of the degree) *If I is an ideal of S and $I = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \cdots \cap \mathfrak{q}_m$ is an irredundant primary decomposition, then*

$$\deg(S/I) = \sum_{\operatorname{ht}(\mathfrak{q}_i) = \operatorname{ht}(I)} \deg(S/\mathfrak{q}_i).$$

PROOF. We may assume that $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are the associated primes of I of height $\operatorname{ht}(I)$ and that $\operatorname{rad}(\mathfrak{q}_i) = \mathfrak{p}_i$ for $i = 1, \ldots, r$. The proof is by induction on m. We set $J = \cap_{i=2}^{m} \mathfrak{q}_i$. There is an exact sequence of K-vector spaces

$$0 \to S_{\leq i}/(\mathfrak{q}_1 \cap J)_{\leq i} \xrightarrow{\varphi} S_{\leq i}/(\mathfrak{q}_1)_{\leq i} \oplus S/(J)_{\leq i} \xrightarrow{\phi} S_{\leq i}/(\mathfrak{q}_1 + J)_{\leq i} \to 0,$$

where $\varphi(\overline{f}) = (\overline{f}, -\overline{f})$ and $\phi(\overline{f}_1, \overline{f}_2) = \overline{f_1 + f_2}$. Hence

$$H^a_{\mathfrak{q}_1}(i) + H^a_J(i) = H^a_I + H^a_{\mathfrak{q}_1 + J}(i). \tag{2.3.2}$$

As the decomposition of I is irredundant, by Lemma 2.66, one has $\dim(S/(\mathfrak{q}_1 + J)) < \dim(S/J)$. If $r = 1$, then $\dim(S/J) < \dim(S/I)$. Hence, from Eq. (2.3.2), we get that $\deg(S/I) = \deg(S/\mathfrak{q}_1)$. If $r > 1$, then $\dim(S/J) = \dim(S/I) = \dim(S/\mathfrak{q}_1)$. Hence, from Eq. (2.3.2), we get that $\deg(S/I)$ is $\deg(S/\mathfrak{q}_1) + \deg(S/J)$. Therefore, by induction, we get the required formula. ♠

LEMMA 2.68. *Let $V \neq \{0\}$ be a vector space over an infinite field K. Then V is not a finite union of proper subspaces of V.*

PROOF. By contradiction. Assume that there are proper subspaces $V_1, \ldots, V_m$ of V such that $V = \bigcup_{i=1}^m V_i$, where m is the least positive integer with this property. Let

$$v_1 \in V_1 \setminus (V_2 \cup \cdots \cup V_m) \text{ and } v_2 \in V_2 \setminus (V_1 \cup V_3 \cup \cdots \cup V_m).$$

Pick $m+1$ distinct non-zero scalars $k_0, \ldots, k_m$ in K. Consider the vectors $\beta_i = v_1 - k_i v_2$ for $i = 0, \ldots, m$. By the pigeon-hole principle there are distinct vectors β_r, β_s in V_j for some j. Since $\beta_r - \beta_s \in V_j$ we get $v_2 \in V_j$. Thus $j = 2$ by the choice of v_2. To finish the proof observe that $\beta_r \in V_2$ imply $v_1 \in V_2$, which contradicts the choice of v_1. ♠

PROPOSITION 2.69. *Let I be a graded ideal of S. If K is infinite and $\mathfrak{m}$ is not in* $\operatorname{Ass}(S/I)$, *then there is $h_1 \in S_1$ such that $h_1 \notin \mathcal{Z}(S/I)$.*

PROOF. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ be the associated primes of S/I. As S/I is graded, $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ are graded ideals by Lemma 1.100. We proceed by contradiction. Assume that S_1, the degree 1 part of S, is contained in $\mathcal{Z}(S/I)$. Thanks to Lemma 1.25, one has that $\mathcal{Z}(S/I) = \cup_{i=1}^m \mathfrak{p}_i$. Hence

$$S_1 \subset (\mathfrak{p}_1)_1 \cup (\mathfrak{p}_2)_1 \cup \cdots \cup (\mathfrak{p}_m)_1 \subset S_1,$$

where $(\mathfrak{p}_i)_1$ is the homogeneous part of degree 1 of the graded ideal $\mathfrak{p}_i$. Since K is infinite, from Lemma 2.68, we get $S_1 = (\mathfrak{p}_i)_1$ for some i. Hence, $\mathfrak{p}_i = \mathfrak{m}$, a contradiction. ♠

The hypothesis that $\mathfrak{m} \notin \operatorname{Ass}(S/I)$ is equivalent to require that S/I has positive depth.

LEMMA 2.70. *Let I be a graded ideal of S. Then $\mathfrak{m} \in \operatorname{Ass}(S/I)$ if and only if* $\operatorname{depth}(S/I)$ *is zero.*

PROOF. It follows from Lemma 1.25. ♠

THEOREM 2.71. *Let I be a graded ideal of S. If* $\operatorname{depth}(S/I) > 0$, *and H_I is the Hilbert function of S/I, then $H_I(i) \leq H_I(i+1)$ for $i \geq 0$.*

PROOF. Case (I): If K is infinite, by Proposition 2.69, there exists $h \in S_1$ a non-zero divisor of S/I. The homomorphism of K-vector spaces

$$(S/I)_i \longrightarrow (S/I)_{i+1}, \quad \overline{z} \mapsto \overline{hz}$$

is injective, therefore $H_I(i) = \dim_K(S/I)_i \leq \dim_K(S/I)_{i+1} = H_I(i+1)$.

Case (II): If K is finite, consider the algebraic closure $\overline{K}$ of K. We set

$$\overline{S} = S \otimes_K \overline{K}, \qquad \overline{I} = I\overline{S}.$$

Hence, from [**Sta78**, Lemma 1.1], one has that $H_I(i) = H_{\overline{I}}(i)$. This means that the Hilbert function does not change when the base field is extended from K to $\overline{K}$. Applying Case (I) to $H_{\overline{I}}(i)$ we obtain the result. ♠

LEMMA 2.72. *Let I be a graded ideal of R. The following hold.*

(a) *If $R_i = I_i$ for some i, then $R_\ell = I_\ell$ for all $\ell \geq i$.*
(b) *If* $\dim\ R/I \geq 2$, *then* $\dim_K(R/I)_i > 0$ *for $i \geq 0$.*

PROOF. (a) It suffices to prove the case $\ell = i+1$. As $I_{i+1} \subset R_{i+1}$, we need only show $R_{i+1} \subset I_{i+1}$. Take a non-zero monomial x^a in R_{i+1}. Then, $x^a = x_1^{a_1} \cdots x_n^{a_n}$ with $a_j > 0$ for some j. Thus, $x^a \in R_1 R_i$. As $R_1 I_i \subset I_{i+1}$, we get $x^a \in I_{i+1}$.

(b) If $\dim_K(R/I)_i = 0$ for some i, then $R_i = I_i$. Thus, by (a), $H_I(j)$ vanishes for $j \geq i$, a contradiction because the Hilbert polynomial of R/I has degree $\dim(R/I) - 1 \geq 1$; see Theorem 1.115. ♠

THEOREM 2.73. **[GKR93]** *Let I be a graded ideal with* $\operatorname{depth}(R/I) > 0$.

(i) *If* $\dim(R/I) \geq 2$, *then $H_I(i) < H_I(i+1)$ for $i \geq 0$.*
(ii) *If* $\dim(R/I) = 1$, *then there is an integer r and a constant c such that:*

$$1 = H_I(0) < H_I(1) < \cdots < H_I(r-1) < H_I(i) = c \quad \text{for } i \geq r.$$

PROOF. Consider the algebraic closure $\overline{K}$ of K. Notice that $|\overline{K}| = \infty$. As in the proof of Theorem 2.71, we make a change of coefficients using the functor $(\cdot) \otimes_K \overline{K}$. Hence we may assume that K is infinite. By Proposition 2.69, there is $h \in R_1$ a non-zero divisor of R/I. From the exact sequence

$$0 \longrightarrow (R/I)[-1] \xrightarrow{h} R/I \longrightarrow R/(h, I) \longrightarrow 0,$$

we get $H_I(i+1) - H_I(i) = H_S(i+1)$, where $S = R/(h, I)$.

(i) If $H_S(i+1) = 0$, then, by Lemma 2.72, $\dim_K(S) < \infty$. Hence S is Artinian (see Lemma 1.56). Thus, by Theorem 1.59, $\dim(S) = 0$, a contradiction.

(ii) Let $r \geq 0$ be the first integer such that $H_I(r) = H_I(r+1)$, thus $S_{r+1} = (0)$ and $R_{r+1} = (h, I)_{r+1}$. Then, by Lemma 2.72, $S_k = (0)$ for $k \geq r+1$. Hence, the Hilbert function of R/I is constant for $k \geq r$ and strictly increasing on $[0, r-1]$. ♠

Hilbert Nullstellensatz. Let K be a field and let $S = K[t_1, \ldots, t_s]$ be a polynomial ring. In what follows $\mathbf{t}$ stands for the set of variables of S, that is, $S = K[\mathbf{t}]$. We define the *affine space* of dimension s over K, denoted by $\mathbb{A}^s_K$ or $\mathbb{A}^s$, to be the cartesian product $K^s = K \times \cdots \times K$.

Given an ideal $I \subset S$, define the *zero set* or *affine variety* of I as

$$V(I) = \{\alpha \in \mathbb{A}^s_K | \, f(\alpha) = 0, \, \forall f \in I\}.$$

By the Hilbert's basis theorem $V(I)$ is the zero locus of a finite collection of polynomials (see Theorem 1.6). Conversely, for any $X \subset \mathbb{A}^s_K$ define $I(X)$,the *vanishing ideal* of X, as the set of polynomials of S that vanish at all points of X. An *affine variety* is the zero set of an ideal. The *dimension* of a variety X is the Krull dimension of its *coordinate ring* $S/I(X)$.

PROPOSITION 2.74. (Zariski topology [**Har13**, Proposition 1.1])

(a) $V(1) = \emptyset$ *and* $V(0) = \mathbb{A}^s_K$.

(b) $V(I \cap J) = V(I) \cup V(J) = V(IJ)$, *for all ideals* I *and* J *of* S.

(c) $\cap V(I_\alpha) = V(\cup I_\alpha)$, *where* $\{I_\alpha\}$ *is any family of ideals of* S.

DEFINITION 2.75. Given $X \subset \mathbb{A}^s_K$, the *Zariski closure* of X, denoted by $\overline{X}$, is the closure of X in the Zariski topology of $\mathbb{A}^s_K$, i.e., $\overline{X}$ is the smallest affine variety of $\mathbb{A}^s_K$ containing X.

PROPOSITION 2.76. [**Har13**, Proposition 1.2] *If* $X \subset \mathbb{A}^s_K$, *then* $\overline{X} = V(I(X))$.

LEMMA 2.77. *Let* X *and* Y *be affine varieties in* $\mathbb{A}^s_K$. *If* $I(X) = I(Y)$, *then* $X = Y$

PROOF. By symmetry it suffices to show the inclusion $X \subset Y$. Take $\alpha \in X$. There are $g_1, \ldots, g_r$ in S such that $Y = V(g_1, \ldots, g_r)$. Clearly $g_i \in I(Y)$ for all i. Then any g_i vanishes at all points of X because $I(Y) = I(X)$. Thus $g_i(\alpha) = 0$ for all i, that is, $\alpha \in Y$. ♠

DEFINITION 2.78. An affine variety $X \subset \mathbb{A}^s_K$ is *reducible* if there are affine varieties $X_1 \neq X$ and $X_2 \neq X$ such that $X = X_1 \cup X_2$; otherwise, X is *irreducible*.

THEOREM 2.79. [**Har13**, Corollary 1.4] *Let* K *be a field and let* X *be an affine variety of* $\mathbb{A}^s_K$, *then* X *is irreducible if and only if* $I(X)$ *is a prime ideal.*

THEOREM 2.80. (Noether normalization lemma [**Vil15**, Corollary 3.1.8]) *If $S = K[t_1, \ldots, t_s]$ is a polynomial ring over a field K and $I \neq S$ is an ideal, then there is an integral extension*

$$K[h_1, \ldots, h_d] \hookrightarrow S/I,$$

where $h_1, \ldots, h_d$ are in S and $d = \dim(S/I)$.

THEOREM 2.81. *Let $S = K[t_1, \ldots, t_s]$ be a polynomial ring over a field K and let $\mathfrak{m}$ be a maximal ideal of S. If K is algebraically closed, then there are $a_1, \ldots, a_s \in K$ such that $\mathfrak{m} = (t_1 - a_1, \ldots, t_s - a_s)$.*

PROOF. There is an integral extension $K[h_1, \ldots, h_d] \hookrightarrow S/\mathfrak{m}$, where $d = \dim(S/\mathfrak{m}) = 0$; see Theorem 2.80. Hence, the canonical map $\varphi\colon K \to S/\mathfrak{m}$ is an isomorphism because K is algebraically closed. To complete the proof choose $a_i \in K$ so that $\varphi(a_i) = \bar{a}_i = \bar{t}_i = \varphi(t_i)$. ♠

PROPOSITION 2.82. *If I is an ideal of a ring S and $f \in S$, then $f \in \sqrt{I}$ if and only if $(I, 1 - tf) = S[t]$, where t is a new variable.*

PROOF. $\Rightarrow$) Let f be an element in $\sqrt{I}$. If $(I, 1 - tf) \neq S[t]$, take a prime ideal $\mathfrak{p}$ containing $(I, 1 - tf)$. Since f must be in $\mathfrak{p}$, because f^n is in I for some $n > 0$, one concludes $1 \in \mathfrak{p}$ which is impossible.

$\Leftarrow$) If $1 = a_1 f_1 + \cdots + a_q f_q + a_{q+1}(1 - tf)$, where $f_i \in I$, $f \in S$ and $a_i \in S[t]$. Set $u = 1/t$ and note $1 - tf = (u - f)/t$, multiplying the first equation by u^m, with m large enough, one derives an equality

$$u^m = b_1 f_1 + \cdots + b_q f_q + b_{q+1}(u - f),$$

where $b_i \in S[u]$. As $S[u]$ is a polynomial ring over S, making $u = f$ gives $f^m \in I$ and $f \in \sqrt{I}$. ♠

THEOREM 2.83 (Hilbert Nullstellensatz). [**Har13**, Theorem 1.3A] *Let S be a polynomial ring over an algebraically closed field K and let I be an ideal of S, then*

$$I(V(I)) = \sqrt{I}.$$

COROLLARY 2.84. *Let $X = V(f_1, \ldots, f_r)$ be an affine variety, defined by polynomials $f_1, \ldots, f_r$ in s variables over an algebraically closed field K. Then $r \geq s - \dim(X)$.*

PROOF. By the Nullstellensatz $I(X) = \sqrt{(f_1, \ldots, f_r)}$. Let $\mathfrak{p}$ be a minimal prime of $(f_1, \ldots, f_r)$ of height $s - \dim(X)$. Applying Theorem 1.66 we get $s - \dim(X) \leq r$. ♠

Projective closure and Gröbner bases. Let K be a field. We define the *projective space* of dimension $s-1$ over K, denoted by $\mathbb{P}_K^{s-1}$or simply by $\mathbb{P}^{s-1}$, to be the quotient space

$$(K^s \setminus \{0\})/\sim$$

where two points α, β in $K^s \setminus \{0\}$ are equivalent under $\sim$ if $\alpha = c\beta$ for some $c \in K$. It is usual to denote the equivalence class of α by $[\alpha]$.

For any set $\mathbb{Y} \subset \mathbb{P}^{s-1}$ define $I(\mathbb{Y})$, the *vanishing ideal* of $\mathbb{Y}$, as the ideal generated by the homogeneous polynomials in S that vanish at all points of $\mathbb{Y}$. Conversely, given a graded ideal $I \subset S$ define its *zero set* as

$$V(I) = \left\{ [\alpha] \in \mathbb{P}^{s-1} | \, f(\alpha) = 0, \, \forall f \in I \text{ homogeneous} \right\}.$$

A *projective variety* is the zero set of a graded ideal. It is not difficult to see that the members of the family

$$\tau = \{\mathbb{P}^{s-1} \setminus V(I) | \, I \text{ is a graded ideal of } S\}$$

are the open sets of a topology on $\mathbb{P}^{s-1}$, called the *Zariski topology*. The Zariski closure of $\mathbb{Y}$ is denoted by $\overline{\mathbb{Y}}$.

If $\mathbb{Y}$ (resp. Y) is a subset of $\mathbb{P}^{s-1}$ (resp. $\mathbb{A}^s$) it is usual to denote the Hilbert function and Hilbert polynomial of $S/I(\mathbb{Y})$ (resp. affine Hilbert function and affine Hilbert polynomial of $S/I(Y)$) by $H_{\mathbb{Y}}$ and $h_{\mathbb{Y}}(t)$ (resp. H_Y^a and $h_Y^a(t)$).

LEMMA 2.85. *Let K be a field. If Y is a subset of $\mathbb{A}^s$ or a subset of $\mathbb{P}^{s-1}$ and $Z = V(I(Y))$, then $I(Z) = I(Y)$. In particular $I(Y) = I(\overline{Y})$.*

DEFINITION 2.86. Let $Y \subset \mathbb{A}_K^s$. The *projective closure* of Y is defined as $\widetilde{Y} := \overline{\phi(Y)}$, where ϕ is the map $\phi\colon \mathbb{A}_K^s \to \mathbb{P}_K^s$, $\alpha \mapsto [(\alpha, 1)]$, and $\overline{\phi(Y)}$ is the closure of $\phi(Y)$ in the Zariski topology of $\mathbb{P}_K^s$.

PROPOSITION 2.87. *If $Y \subset \mathbb{A}_K^s$, then $\widetilde{Y} = V(I(\phi(Y)))$.*

PROPOSITION 2.88. *If $Y \subset \mathbb{A}^s$ and $\mathbb{Y} = \phi(Y)$, then the following hold:*

(a) $H_Y^a(d) = H_{\mathbb{Y}}(d)$ *for* $d \geq 0$,
(b) $\deg S/I(Y) = \deg S[u]/I(\mathbb{Y})$,
(c) $\mathrm{ri}^a(S/I(Y)) = \mathrm{ri}(S[u]/I(\mathbb{Y}))$,
(d) $I(\overline{\mathbb{Y}}) = I(\mathbb{Y}) = I(Y)^h$.

PROOF. (a) Let $f \in S_{\leq d}$ and let u be a new variable. The *homogenization* of f with respect to u and d, denoted by $f^{\mathfrak{h}}$, is given by

$$f^{\mathfrak{h}}(t_1, \ldots, t_s, u) := u^d f(t_1/u, \ldots, t_s/u).$$

Notice that the polynomial $f^{\mathfrak{h}}$ is homogeneous of degree d. Fix $d \geq 1$. The homogenization map $\psi\colon S_{\leq d} \to S[u]_d$, $f \mapsto f^{\mathfrak{h}}$, is an isomorphism of K-vector spaces such that $\psi(I(Y)_{\leq d}) = I(\mathbb{Y})_d$. Hence, the induced map

$$\Phi\colon S_{\leq d} \to S[u]_d/I(\mathbb{Y})_d, \quad f \longmapsto f^{\mathfrak{h}} + I(\mathbb{Y})_d, \tag{2.3.3}$$

is a surjection. Since $\ker(\Phi) = I(Y)_{\leq d}$, we get that $H^a_Y(d) = H_{\mathbb{Y}}(d)$.

(b), (c) They follow from (a).

(d) By Lemma 2.85 one has $I(\overline{\mathbb{Y}}) = I(\mathbb{Y})$. Clearly $I(Y)^h \subset I(\mathbb{Y})$. To show the reverse inclusion take f in $I(\mathbb{Y})$ homogeneous of degree d. By factoring out u we may assume that at least of the monomials of f does not contains u. Then, by the proof of (a), there is $g \in I(Y)_{\leq d}$ such that $g^h = g^{\mathfrak{h}} = f$. Thus f is in $I(Y)^h$. ♠

Let $\succ$ be the GRevLex order on the monomials of $S[u]$, where $u = t_{s+1}$ is a new variable this order extends the GRevLex on the monomials of S.

PROPOSITION 2.89. *Let $Y \subset \mathbb{A}^s_K$ be a set and let $\overline{\phi(Y)} \subset \mathbb{P}^s_K$ be its projective closure. If $f_1, \ldots, f_r$ is a Gröbner basis of $I(Y)$, then*

$$I(\overline{\phi(Y)}) = I(Y)^h = (f_1^h, \ldots, f_r^h),$$

and the height of $I(Y)$ in S is equal to the height of $I(\overline{\phi(Y)})$ in $S[u]$.

PROOF. By Proposition 2.88 one has that $I(\overline{\phi(Y)}) = I(Y)^h$, and thanks to Lemma 2.46 one has $I(Y)^h = (f_1^h, \ldots, f_r^h)$ and $\operatorname{ht} I(Y) = \operatorname{ht} I(\overline{\phi(Y)})$. ♠

THEOREM 2.90 (Projective Hilbert Nullstellensatz). *Let K be an algebraically closed field and let I be a graded ideal of S. If the projective variety $V(I)$ is not empty, then*

$$I(V(I)) = \sqrt{I}.$$

PROOF. It follows from Theorem 2.83. ♠

Let $\mathbb{Y} = V(I)$ be a projective variety. The *dimension* of $\mathbb{Y}$, denoted $\dim(\mathbb{Y})$, is the degree of the Hilbert polynomial of $S/I(\mathbb{Y})$, i.e., $\dim(\mathbb{Y}) = \dim(S/I(\mathbb{Y})) - 1$. If $Y = V(I)$ is an affine variety, the *dimension* of Y is the degree of the affine Hilbert polynomial of $S/I(Y)$, that is, $\dim(Y) = \dim(S/I(Y))$.

THEOREM 2.91. (The Dimension Theorem) *Let K be an algebraically closed field and let $I \subsetneq S$ be an ideal. If $\mathbb{Y} = V(I)$ is a projective variety in $\mathbb{P}^{s-1}$ and I is graded (resp. $Y = V(I)$ is an affine variety in $\mathbb{A}^s$), then* $\dim(\mathbb{Y}) = \dim(S/I) - 1$ *(resp.* $\dim(Y) = \dim(S/I)$*).*

PROOF. It follows from Theorems 2.90 and 2.83, respectively. ♠

LEMMA 2.92. *Let $\mathbb{Y}$ be a finite subset of $\mathbb{P}^{s-1}$, let $[\alpha]$ be a point in $\mathbb{Y}$, with $\alpha = (\alpha_1, \ldots, \alpha_s)$ and $\alpha_k \neq 0$ for some k, and let $I_{[\alpha]}$ be the vanishing ideal of $[\alpha]$. Then $I_{[\alpha]}$ is a prime ideal of height $s-1$,*

$$I_{[\alpha]} = (\{\alpha_k t_i - \alpha_i t_k | \, k \neq i \in \{1, \ldots, s\}), \ \deg(S/I_{[\alpha]}) = 1,$$

and $I(\mathbb{Y}) = \bigcap_{[Q]\in\mathbb{Y}} I_{[Q]}$ is the primary decomposition of $I(\mathbb{Y})$.

A similar statement holds for affine sets in affine spaces.

LEMMA 2.93. *Let Y be a finite subset of $\mathbb{A}^s$, let α be a point in Y, with $\alpha = (\alpha_1, \ldots, \alpha_s)$, and let I_α be the vanishing ideal of α. Then I_α is a prime ideal of height s,*

$$I_\alpha = (t_1 - \alpha_1, \ldots, t_s - \alpha_s), \ \deg(S/I_\alpha) = 1,$$

and $I(Y) = \bigcap_{Q\in Y} I_Q$ is the primary decomposition of $I(Y)$.

LEMMA 2.94. *If $\mathbb{Y} \subset \mathbb{P}^{s-1}$ is a finite set, then $\deg(S/I(\mathbb{Y})) = |\mathbb{Y}|$.*

PROOF. For $[P] \in \mathbb{Y}$, let $I_{[P]}$ be its vanishing ideal. Since $I(\mathbb{Y}) = \cap_{[P]\in\mathbb{Y}} I_{[P]}$ and since $\deg(S/I_{[P]}) = 1$ (see Lemma 4.5), the lemma follows from the additivity of the degree (see Proposition 4.2). ♠

PROPOSITION 2.95. (**[GKR93]**) *If $\mathbb{Y} \subset \mathbb{P}^{s-1}$ is a finite set, then*

$$1 = H_{\mathbb{Y}}(0) < H_{\mathbb{Y}}(1) < \cdots < H_{\mathbb{Y}}(r-1) < H_{\mathbb{Y}}(d) = |\mathbb{Y}|$$

for $d \geq r = \operatorname{reg}(S/I(\mathbb{Y}))$.

PROOF. As $S/I(\mathbb{Y})$ is Cohen–Macaulay of dimension 1, by Theorem 1.115, its Hilbert polynomial has degree 0. Hence, by Lemma 2.94, $H_{\mathbb{Y}}(d) = |\mathbb{Y}|$ for $d \gg 0$. Consequently the result follows readily from Theorem 2.73. ♠

LEMMA 2.96. *If $\mathbb{Y} \subset \mathbb{P}^{s-1}$ and $\dim(S/I(\mathbb{Y})) = 1$, then we have $|\mathbb{Y}| < \infty$ and $\deg(S/I(\mathbb{Y})) = |\mathbb{Y}|$.*

PROOF. The Hilbert polynomial of $S/I(\mathbb{Y})$ has degree 0. If $H_{\mathbb{Y}}$ denotes the Hilbert function of $S/I(\mathbb{Y})$, one has that $H_{\mathbb{Y}}(d) = a_0$ for $d \gg 0$. If $|\mathbb{Y}| > a_0$, pick $[P_1], \ldots, [P_{a_0+1}]$ distinct points in $\mathbb{Y}$ and set $I = \cap_{i=1}^{a_0+1} I_{[P_i]}$, where $I_{[P_i]}$ is the vanishing ideal of $[P_i]$. Then $\dim(S/I) = 1$ and $\deg(S/I) = a_0 + 1$ (see Proposition 4.2). Hence, by Lemma 2.94, $H_I(d) = a_0 + 1$ for $d \gg 0$. From the exact sequence

$$0 \to I/I(\mathbb{Y}) \to S/I(\mathbb{Y}) \to S/I \to 0$$

we get that $a_0 = \dim_K(I/I(\mathbb{Y}))_d + (a_0 + 1)$ for $d \gg 0$, a contradiction. Thus $|\mathbb{Y}| \leq a_0$ and by Lemma 2.94 one has equality. ♠

LEMMA 2.97. *Let I be a graded ideal of a polynomial ring S over a field K. Then the radical of I is also graded.*

THEOREM 2.98. *Let $I \subset S$ be an ideal. The following hold.*

(a): *If* $\dim(S/I) = 0$, *then* $|V(I)| \leq \dim_K(S/\mathrm{rad}(I)) \leq \dim_K(S/I) < \infty$.
(b): *If I is graded,* $\dim(S/I) = 1$, *and* $V(I) \subset \mathbb{P}^{s-1}$ *is the zero set of I, then*

$$|V(I)| \leq \deg(S/\mathrm{rad}(I)) \leq \deg(S/I).$$

PROOF. (a) By Lemma 1.56 and Theorem 1.59, one has $\dim_K(S/I) < \infty$. The second inequality is easy to show because there is an exact sequence of finite dimensional K-vector spaces:

$$0 \to \mathrm{rad}(I)/I \to S/I \to S/\mathrm{rad}(I) \to 0.$$

We may assume that I is a radical ideal because $V(I) = V(\mathrm{rad}(I))$. Then the irredundant primary decomposition of I has the form:

$$I = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r,$$

where $\mathfrak{m}_i$ is a maximal ideal of S for $i = 1, \ldots, r$. Consequently, one has

$$V(I) = V(\mathfrak{m}_1) \cup \cdots \cup V(\mathfrak{m}_r). \tag{2.3.4}$$

Notice that for each i either $V(\mathfrak{m}_i) = \emptyset$ or $V(\mathfrak{m}_i) = \{a\}$ for some $a \in \mathbb{A}^s$. Indeed if $V(\mathfrak{m}_i) \neq \emptyset$, pick $a \in V(\mathfrak{m}_i)$ with $a = (a_1, \ldots, a_s)$, then

$$\mathfrak{m}_i \subset (t_1 - a_1, \ldots, t_s - a_s) \;\Rightarrow\; \mathfrak{m}_i = (t_1 - a_1, \ldots, t_s - a_s).$$

Thus $V(\mathfrak{m}_i) = \{a\}$. Hence, by Eq. (2.3.4), $|V(I)| \leq r$. By additivity of the degree (see Proposition 4.2) we get

$$\dim_K(S/I) = \deg(S/I) = \sum_{i=1}^{r} \deg(S/\mathfrak{m}_i) = \sum_{i=1}^{r} \dim_K(S/\mathfrak{m}_i) \geq r.$$

Consequently $\dim_K(S/I) \geq r \geq |V(I)|$.

(b) Set $J = \mathrm{rad}(I)$. By Lemma 2.97, J is a graded ideal. There is an exact sequence of graded rings:

$$0 \to J/I \to S/I \to S/J \to 0.$$

As I and J are graded ideals of dimension 1, the Hilbert functions $H_I(d)$ and $H_J(d)$ of I and J are constant for $d \gg 0$. Therefore, from the exact sequence above, we get

$$\deg(S/I) = H_I(d) \geq H_J((d) = \deg(S/J) \;\text{ for }\; d \gg 0.$$

Thus $\deg(S/J) \leq \deg(S/I)$. We may assume that I is a radical ideal because $V(I) = V(\operatorname{rad}(I))$. Thanks to Lemma 1.100, the irredundant primary decomposition of I has the form:

$$I = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r,$$

where $\mathfrak{p}_i$ is a graded prime ideal of height $s-1$ for all i. Hence, one has

$$V(I) = V(\mathfrak{p}_1) \cup \cdots \cup V(\mathfrak{p}_r). \tag{2.3.5}$$

Notice that for each i either $V(\mathfrak{p}_i) = \emptyset$ or $V(\mathfrak{p}_i) = \{[a]\}$ for some $[a] \in \mathbb{P}^{s-1}$. Indeed if $V(\mathfrak{p}_i) \neq \emptyset$, pick $[a] \in V(\mathfrak{p}_i)$ with $a = (a_1, \ldots, a_s)$ and $a_j \neq 0$ for some j, for simplicity assume $j = 1$, then

$$\mathfrak{p}_i \subset I_{[a]} = (a_2 t_1 - t_2, a_3 t_1 - t_3 \ldots, a_s t_1 - t_s) \;\Rightarrow\; \mathfrak{p}_i = I_{[a]}.$$

Thus $V(\mathfrak{p}_i) = \{[a]\}$. Hence, by Eq. (2.3.5), $|V(I)| \leq r$. By additivity of the degree (see Proposition 4.2) we get

$$\deg(S/I) = \sum_{i=1}^{r} \deg(S/\mathfrak{p}_i) \geq r.$$

Consequently $\deg(S/I) \geq r \geq |V(I)|$. ♠

LEMMA 2.99. *Let K be an algebraically closed field and let $I \subsetneq S$ be an ideal. The following hold.*

(a) $V(I) \neq \emptyset$.
(b) *If I is graded and* $\dim(S/I) \geq 1$, *then* $V(I) \neq \{0\}$.

PROOF. (a) Pick a maximal ideal $\mathfrak{m} \subset S$ containing I. By Theorem 2.81 there is $a = (a_1, \ldots, a_s) \in K^s$ such that $\mathfrak{m} = (t_1 - a_1, \ldots, t_s - a_s)$. Thus $V(I)$ is not empty because $a \in V(I)$.

(b) Consider the maximal irrelevant ideal $\mathfrak{m} = (t_1, \ldots, t_s)$. Clearly $I \subset \mathfrak{m}$ because I is graded. Then V_I, the affine variety defined by I, contains the vector 0. If $V_I = \{0\}$, by Theorem 2.83, we get that $\operatorname{rad}(I) = \mathfrak{m}$, a contradiction. Thus there is $0 \neq a \in V_I$. Hence $[a] \in V(I)$. ♠

COROLLARY 2.100. *Let K be an algebraically closed field and let $I \subset S$ be an ideal. The following hold.*

(a) *If* $\dim(S/I) = 0$, *then* $|V(I)| = \dim_K(S/\operatorname{rad}(I)) < \infty$.
(b) *If I is graded and* $\dim(S/I) = 1$, *then* $|V(I)| = \deg(S/\operatorname{rad}(I))$.

PROOF. It follows from the proof of Theorem 2.98 using Lemma 2.99. ♠

2.4. The footprint of an ideal

Let $\prec$ be a monomial order on S and let $(0) \neq I \subset S$ be an ideal.

DEFINITION 2.101. A monomial t^a is a *standard monomial* of S/I, with respect to $\prec$, if t^a is not the leading monomial of any polynomial in I. The set of standard monomials, denoted $\Delta_\prec(I)$, is called the *footprint* of S/I.

The image of $\Delta_\prec(I)$, under the canonical map $S \mapsto S/I$, $x \mapsto \overline{x}$, is a K-basis for S/I (see Proposition 2.31). In particular if I is graded, then $H_I(d)$ is the number of standard monomials of degree d.

LEMMA 2.102. **[Car13**, p. 2] *Let $I \subset S$ be an ideal generated by $\mathcal{G} = \{g_1, \ldots, g_r\}$, then*

$$\Delta_\prec(I) \subset \Delta_\prec(\text{in}_\prec(g_1), \ldots, \text{in}_\prec(g_r)),$$

with equality if $\mathcal{G}$ is a Gröbner basis.

PROOF. Take t^a in $\Delta_\prec(I)$. If $t^a \notin \Delta_\prec(\text{in}_\prec(g_1), \ldots, \text{in}_\prec(g_r))$, then $t^a = t^c\,\text{in}_\prec(g_i)$ for some i and some t^c. Thus $t^a = \text{in}_\prec(t^c g_i)$, with $t^c g_i$ in I, a contradiction. The second statement holds by the definition of a Gröbner basis. ♠

LEMMA 2.103. *Let $\mathcal{G} = \{g_1, \ldots, g_r\}$ be a Gröbner basis of I. If for some i, the variable t_i does not divides $\text{in}_\prec(g_j)$ for all j, then t_i is a regular element on S/I.*

PROOF. Assume that $t_i f \in I$. By the division algorithm we can write $f = g + h$, where $g \in I$ and h is 0 or a standard polynomial. It suffices to show that $h = 0$. If $h \neq 0$, then $t_i \text{in}_\prec(h) \in \text{in}_\prec(I)$. Since $t_i h \in I$, there are g_k and f such that $\text{in}_\prec(t_i h) = t_i \text{in}_\prec(h) = f\text{in}_\prec(g_k)$. Hence, using our hypothesis on t_i, we get that $\text{in}_\prec(h)$ is a multiple of $\text{in}_\prec(g_k)$, a contradiction. ♠

The element f is called a *zero-divisor* of S/I if there is $\overline{0} \neq \overline{a} \in S/I$ such that $f\overline{a} = \overline{0}$, and f is called *regular* on S/I otherwise.

This lemma tells us that if t_i is a zero-divisor of S/I for all i, then any variable t_i must occur in an initial monomial $\text{in}_\prec(g_j)$ for some j.

LEMMA 2.104. *Let $\prec$ be a monomial order, let $I \subset S$ be an ideal, and let f be a polynomial of S of positive degree. If $\text{in}_\prec(f)$ is regular on $S/\text{in}_\prec(I)$, then f is regular on S/I.*

PROOF. Let g be a polynomial of S such that $gf \in I$. It suffices to show that $g \in I$. By the division algorithm (see Theorem 2.24) we may assume that $g = 0$ or that g is a standard polynomial of S/I. If $g \neq 0$, then $\text{in}_\prec(g)\text{in}_\prec(f)$ is in $\text{in}_\prec(I)$ and consequently $\text{in}_\prec(g)$ is in $\text{in}_\prec(I)$, a contradiction. ♠

2.5. Computing zeros of polynomials

In this section we give a degree formula to compute the number of zeros that a homogeneous polynomial has in any given finite set of points in a projective space over any field.

PROPOSITION 2.105. *Let $I \subset S$ be an ideal, let $\prec$ be a monomial order on S, let $\Delta_\prec(I)$ be the set of standard monomials of I, and let X be a finite subset of $\mathbb{A}^s_K$. The following hold.*

(a) *If $|\Delta_\prec(I)| < \infty$, then $|V(I)| \leq |\Delta_\prec(I)|$.*
(b) $|X| = |V(I(X))| = |\Delta_\prec(I(X))| = \deg S/I(X) = \dim_K S/I(X)$.

PROOF. By Proposition 2.31, one has the equality $|\Delta_\prec(I)| = \dim_K(S/I)$. Hence, by Lemma 1.56, S/I is an Artinian ring. Thus the result follows by recalling that an Artinian ring has dimension zero (see Theorem 1.59) and applying Theorem 2.98 and Proposition 2.95. ♠

LEMMA 2.106. *If $I \subset S$ is an ideal and $\mathcal{G} = \{g_1, \ldots, g_r\}$ is a Gröbner basis of I, then $\Delta_\prec(I)$ is the set of all monomial of S that are not a multiple of any of the leading monomials of $g_1, \ldots, g_r$.*

PROOF. It follows from the definition of a Gröbner basis. ♠

LEMMA 2.107. *Let $I \subset S$ be an ideal generated by $\mathcal{G} = \{g_1, \ldots, g_r\}$, then*

$$\Delta_\prec(I) \subset \Delta_\prec(\text{in}(g_1), \ldots, \text{in}(g_r)).$$

PROOF. Take t^a in $\Delta_\prec(I)$. If $t^a \notin \Delta_\prec(\text{in}(g_1), \ldots, \text{in}(g_r))$, then t^a is a multiple of $\text{in}(g_i)$ for some i and consequently t^a is a multiple of a monomial in the initial ideal of I, a contradiction. ♠

An ideal $I \subset S$ is called *unmixed* if all its associated primes have the same height and I is called *radical* if I is equal to its radical. The radical of I is denoted by $\text{rad}(I)$.

LEMMA 2.108. *Let $I \subset S$ be a radical unmixed graded ideal. If $f \in S$ is homogeneous, $(I\colon f) \neq I$, and $\mathcal{A}$ is the set of all associated primes of S/I that contain f, then $\text{ht}(I) = \text{ht}(I, f)$ and*

$$\deg S/(I, f) = \sum_{\mathfrak{p} \in \mathcal{A}} \deg S/\mathfrak{p}.$$

PROOF. As f is a zero-divisor of S/I and I is unmixed, there is an associated prime ideal $\mathfrak{p}$ of S/I of height $\text{ht}(I)$ such that $f \in \mathfrak{p}$. Thus $I \subset (I, f) \subset \mathfrak{p}$, and consequently $\text{ht}(I) = \text{ht}(I, f)$. Therefore the set of associated primes of (I, f) of height equal to $\text{ht}(I)$ is not empty and is equal to $\mathcal{A}$. There is an irredundant primary decomposition

$$(I, f) = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r \cap \mathfrak{q}'_{r+1} \cap \cdots \cap \mathfrak{q}'_t, \tag{2.5.1}$$

where $\operatorname{rad}(\mathfrak{q}_i) = \mathfrak{p}_i$, $\mathcal{A} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$, and $\operatorname{ht}(\mathfrak{q}_i') > \operatorname{ht}(I)$ for $i > r$. We may assume that the associated primes of S/I are $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$. Since I is a radical ideal, we get that $I = \cap_{i=1}^m \mathfrak{p}_i$. Next we show the following equality:

$$\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_m = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r \cap \mathfrak{q}_{r+1}' \cap \cdots \cap \mathfrak{q}_t' \cap \mathfrak{p}_{r+1} \cap \cdots \cap \mathfrak{p}_m. \tag{2.5.2}$$

The inclusion "$\supset$" is clear because $\mathfrak{q}_i \subset \mathfrak{p}_i$ for $i = 1, \ldots, r$. The equality "$\subset$" follows by noticing that the right hand side of Eq. (4.2.2) is equal to $(I, f) \cap \mathfrak{p}_{r+1} \cap \cdots \cap \mathfrak{p}_m$, and consequently it contains $I = \cap_{i=1}^m \mathfrak{p}_i$. Notice that $\operatorname{rad}(\mathfrak{q}_j') = \mathfrak{p}_j' \not\subset \mathfrak{p}_i$ for all i, j and $\mathfrak{p}_j \not\subset \mathfrak{p}_i$ for $i \neq j$. Hence localizing Eq. (4.2.2) at the prime ideal $\mathfrak{p}_i$ for $i = 1, \ldots, r$, we get that $\mathfrak{p}_i = I_{\mathfrak{p}_i} \cap S = (\mathfrak{q}_i)_{\mathfrak{p}_i} \cap S = \mathfrak{q}_i$ for $i = 1, \ldots, r$. Using Eq. (4.2.1) and the additivity of the degree the required equality follows. ♠

Given a subset $\mathbb{X} \subset \mathbb{P}^{s-1}$ define $I(\mathbb{X})$, the *vanishing ideal* of $\mathbb{X}$, as the ideal generated by the homogeneous polynomials in S that vanish at all points of $\mathbb{X}$, and given a graded ideal $I \subset S$ define its *zero set* w.r.t $\mathbb{X}$ as

$$V_{\mathbb{X}}(I) = \{[\alpha] \in \mathbb{X} |\, f(\alpha) = 0,\ \forall f \in I \text{ homogeneous}\}.$$

In particular, if $f \in S$ is homogeneous, the zero set $V_{\mathbb{X}}(f)$ of f is the set of all $[\alpha] \in \mathbb{X}$ such that $f(\alpha) = 0$, that is $V_{\mathbb{X}}(f)$ is the set of zeros of f in $\mathbb{X}$.

THEOREM 2.109. *Let $\mathbb{X}$ be a finite subset of $\mathbb{P}^{s-1}$ over a field K and let $I(\mathbb{X}) \subset S$ be its graded vanishing ideal. If $0 \neq f \in S$ is homogeneous, then the number of zeros of f in $\mathbb{X}$ is given by*

$$|V_{\mathbb{X}}(f)| = \begin{cases} \deg S/(I(\mathbb{X}), f) & \text{if } (I(\mathbb{X}) \colon f) \neq I(\mathbb{X}), \\ 0 & \text{if } (I(\mathbb{X}) \colon f) = I(\mathbb{X}). \end{cases}$$

PROOF. Let $[P_1], \ldots, [P_m]$ be the points of $\mathbb{X}$ with $m = |\mathbb{X}|$ and let $[P]$ be a point in $\mathbb{X}$, with $P = (\alpha_1, \ldots, \alpha_s)$ and $\alpha_k \neq 0$ for some k. Then the vanishing ideal $I_{[P]}$ of $[P]$ is a prime ideal of height $s - 1$,

$$I_{[P]} = (\{\alpha_k t_i - \alpha_i t_k |\, k \neq i \in \{1, \ldots, s\}),\ \deg(S/I_{[P]}) = 1,$$

and $I(\mathbb{X}) = \bigcap_{i=1}^m I_{[P_i]}$ is a primary decomposition (see Lemma 4.5). In particular $I(\mathbb{X})$ is an unmixed radical ideal of dimension 1.

Assume that $(I(\mathbb{X}) \colon f) \neq I(\mathbb{X})$. Let $\mathcal{A}$ be the set of all $I_{[P_i]}$ that contain the polynomial f. Then $f(P_i) = 0$ if and only if $I_{[P_i]}$ is in $\mathcal{A}$. Hence, by Lemma 4.9, we get

$$|V_{\mathbb{X}}(f)| = \sum_{[P_i] \in V_{\mathbb{X}}(f)} \deg S/I_{[P_i]} = \sum_{f \in I_{[P_i]}} \deg S/I_{[P_i]} = \deg S/(I(\mathbb{X}), f).$$

If $(I(\mathbb{X})\colon f) = I(\mathbb{X})$, then f is a regular element of $S/I(\mathbb{X})$. This means that f is not in any of the associated primes of $I(\mathbb{X})$, that is, $f \notin I_{[P_i]}$ for all i. Thus $V_{\mathbb{X}}(f) = \emptyset$ and $|V_{\mathbb{X}}(f)| = 0$. ♠

The next result will be used to bound the number of zeros of polynomials over finite fields (see Corollary 4.15) and to study the general properties of the minimum distance function of a graded ideal.

LEMMA 2.110. **[MBPV17]** *Let $I \subset S$ be an unmixed graded ideal and let $\prec$ be a monomial order. If $f \in S$ is homogeneous and $(I\colon f) \neq I$, then*

(i) $\deg S/(I,f) \leq \deg S/(\mathrm{in}_\prec(I), \mathrm{in}_\prec(f)) \leq \deg S/I$,
(ii) $\deg S/I = \deg S/(I\colon f) + \deg S/(I,f)$ *if* $f \notin I$, *and*
(iii) $\deg(S/(I,f)) < \deg(S/I)$ *if* $f \notin I$.

PROOF. (i) To simplify notation we set $J = (I,f)$ and $L = (\mathrm{in}_\prec(I), \mathrm{in}_\prec(f))$. First we show that S/J and S/L have dimension equal to $\dim S/I$. As f is a zero-divisor of S/I and I is unmixed, there is an associated prime ideal $\mathfrak{p}$ of S/I such that $f \in \mathfrak{p}$ and $\dim S/I = \dim S/\mathfrak{p}$. Since $I \subset J \subset \mathfrak{p}$, we get that $\dim S/J$ is $\dim S/I$. Since S/I and $S/\mathrm{in}_\prec(I)$ have the same Hilbert function, and so does $S/\mathfrak{p}$ and $S/\mathrm{in}_\prec(\mathfrak{p})$, we obtain

$$\dim S/\mathrm{in}_\prec(I) = \dim S/I = \dim S/\mathfrak{p} = \dim S/\mathrm{in}_\prec(\mathfrak{p}).$$

Hence, taking heights in the inclusions $\mathrm{in}_\prec(I) \subset L \subset \mathrm{in}_\prec(\mathfrak{p})$, we obtain $\mathrm{ht}(I) = \mathrm{ht}(L)$.

Pick a Gröbner basis $\mathcal{G} = \{g_1, \ldots, g_r\}$ of I. Then J is generated by $\mathcal{G} \cup \{f\}$ and by Lemma 2.102 one has the inclusions

$$\Delta_\prec(J) = \Delta_\prec(I,f) \subset \Delta_\prec(\mathrm{in}_\prec(g_1), \ldots, \mathrm{in}_\prec(g_r), \mathrm{in}_\prec(f)) =$$
$$\Delta_\prec(\mathrm{in}_\prec(I), \mathrm{in}_\prec(f)) = \Delta_\prec(L) \subset \Delta_\prec(\mathrm{in}_\prec(g_1), \ldots, \mathrm{in}_\prec(g_r)) = \Delta_\prec(I).$$

Thus $\Delta_\prec(J) \subset \Delta_\prec(L) \subset \Delta_\prec(I)$. Recall that $H_I(d)$, the Hilbert function of I at d, is the number of standard monomials of degree d. Hence $H_J(d) \leq H_L(d) \leq H_I(d)$ for $d \geq 0$. If $\dim(S/I)$ is equal to 0, then

$$\deg S/J = \sum_{d\geq 0} H_J(d) \leq \deg S/L = \sum_{d\geq 0} H_L(d) \leq \deg S/I = \sum_{d\geq 0} H_I(d).$$

Assume now that $\dim(S/I) \geq 1$. By the Hilbert theorem, H_J, H_L, H_I are polynomial functions of degree equal to $k = \dim(S/I) - 1$. Thus

$$k! \lim_{d\to\infty} H_J(d)/d^k \leq k! \lim_{d\to\infty} H_L(d)/d^k \leq k! \lim_{d\to\infty} H_I(d)/d^k,$$

that is $\deg S/J \leq \deg S/L \leq \deg S/I$.

If I is an unmixed radical ideal and $f \notin I$, then there is at least one minimal prime that does not contains f. Hence, by Lemma 4.9, it follows that $\deg(S/(I,f)) < \deg(S/I)$.

(ii) Using that I is unmixed, it is not hard to see that S/I, $S/(I\colon f)$, and $S/(I,f)$ have the same dimension. There is an exact sequence

$$0 \longrightarrow S/(I\colon f)[-d] \xrightarrow{f} S/I \longrightarrow S/(I,f) \longrightarrow 0.$$

Hence, by the additivity of Hilbert functions, we get

$$H_I(i) = H_{(I\colon f)}(i-d) + H_{(I,f)}(i) \text{ for } i \geq 0. \tag{2.5.3}$$

If $\dim S/I = 0$, then using Eq. (2.5.3) one has

$$\sum_{i\geq 0} H_I(i) = \sum_{i\geq 0} H_{(I\colon f)}(i) + \sum_{i\geq 0} H_{(I,f)}(i).$$

Therefore, using the definition of degree, the required equality follows. If $k = \dim S/I - 1$ and $k \geq 1$, by the Hilbert theorem, H_I, $H_{(I,f)}$, and $H_{(I\colon f)}$ are polynomial functions of degree k. Then dividing Eq. (2.5.3) by i^k and taking limits as i goes to infinity, the required equality follows.

(iii) This part follows at once from part (ii). ♠

REMARK 2.111. Let $I \subset S$ be an unmixed graded ideal of dimension 1. If $f \in S_d$, then $(I\colon f) = I$ if and only if $\dim(S/(I,f)) = 0$. In this case $\deg(S/(I,f))$ could be greater than $\deg(S/I)$.

COROLLARY 2.112. *Let $\mathbb{X}$ be a finite subset of a projective space $\mathbb{P}^{s-1}$ over a field K, let $I(\mathbb{X}) \subset S$ be its graded vanishing ideal, and let $\prec$ be a monomial order. If $0 \neq f \in S$ is homogeneous and $(I(\mathbb{X})\colon f) \neq I(\mathbb{X})$, then*

$$|V_{\mathbb{X}}(f)| = \deg S/(I(\mathbb{X}),f) \leq \deg S/(\mathrm{in}_{\prec}(I(\mathbb{X})), \mathrm{in}_{\prec}(f)) \leq \deg S/I(\mathbb{X}).$$

PROOF. It follows from Theorem 4.10 and Lemma 4.14. ♠

The next result gives a sufficient conditions for an ideal of dimension zero to be radical.

LEMMA 2.113. (Seidenberg's Lemma [**BW93**]) *Let $I \subset S$ be an ideal of dimensional zero. If I contains a univariate polynomial $f_i \in K[t_i]$ with $\gcd(f_i, f_i') = 1$ for $i = 1, \ldots, s$, then I is an intersection of finitely many maximal ideals. In particular, I is radical.*

LEMMA 2.114. *Let $I \subsetneq S$ be an ideal. If I is an intersection of a finite number of maximal ideals. Then any ideal containing I is a radical ideal.*

PROOF. Let J be an ideal containing I. The ideal I has a minimal primary decomposition $I = \cap_{i=1}^{m} \mathfrak{m}_i$, where $\mathfrak{m}_i$ is a maximal ideal for all i. Clearly $\mathrm{ht}(I) = \mathrm{ht}(J) = s$.

Therefore the set $\mathrm{Ass}(S/J)$ of associated primes of S/J is a subset of $\mathrm{Ass}(S/I)$. Hence we may assume that $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ are the associated primes of S/J. There is a minimal primary decomposition

$$J = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r,$$

where $\mathrm{rad}(\mathfrak{q}_i) = \mathfrak{m}_i$ for $i = 1, \ldots, r$. Therefore

$$I = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_m = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r \cap \mathfrak{m}_{r+1} \cap \cdots \cap \mathfrak{m}_m.$$

Hence localizing this equality at the prime ideal $\mathfrak{m}_i$ for $i = 1, \ldots, r$, we get that $\mathfrak{m}_i = I_{\mathfrak{m}_i} \cap S = (\mathfrak{q}_i)_{\mathfrak{m}_i} \cap S = \mathfrak{q}_i$ for $i = 1, \ldots, r$. Thus J is the intersection of $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ and J is a radical ideal. ♠

COROLLARY 2.115. *Let X be a finite subset of an affine space $\mathbb{A}^s$ over a field K. Then any ideal containing $I(X)$ is a radical ideal.*

PROOF. It follows from Lemmas 2.93 and 2.114. ♠

THEOREM 2.116. *Let X be a finite subset of an affine space $\mathbb{A}^s$ over a field K and let $I(X) \subset S$ be its vanishing ideal. If $0 \neq F \in S$, then the number of zeros of F in X is given by*

$$|V_X(F)| = \begin{cases} \deg S/(I(X), F) & \text{if } (I(X)\colon F) \neq I(X), \\ 0 & \text{if } (I(X)\colon F) = I(X). \end{cases}$$

PROOF. Let $P_1, \ldots, P_m$ be the points of X with $m = |X|$ and let P be a point in X, with $P = (\alpha_1, \ldots, \alpha_s)$ and $\alpha_k \neq 0$ for some k. Then the vanishing ideal I_P of P is a maximal ideal of height s,

$$I_P = (t_1 - \alpha_1, \ldots, t_s - \alpha_s),\ \deg(S/I_P) = 1, \text{ and}$$

$I(X) = \bigcap_{P \in X} I_Q$ is a primary decomposition of $I(X)$ (see Lemma 2.93). In particular $I(X)$ is an unmixed radical ideal of dimension 0.

Assume that $(I(X)\colon F) \neq I(X)$. Let $\mathcal{A}$ be the set of all I_{P_i} that contain the polynomial F. Then $F(P_i) = 0$ if and only if I_{P_i} is in $\mathcal{A}$. Hence, by Lemma 2.114, we get

$$|V_X(F)| = \sum_{P_i \in V_X(F)} \deg S/I_{P_i} = \deg S/(I(X), F).$$

If $(I(X)\colon F) = I(X)$, then F is a regular element of $S/I(X)$. This means that F is not in any of the associated primes of $I(X)$, that is, $F \notin I_{P_i}$ for all i. Thus $V_X(F) = \emptyset$ and $|V_X(F)| = 0$. ♠

Let us illustrate the use of Theorem 2.116.

EXAMPLE 2.117. Let $V_X(F)$ be the curve in $X = \mathbb{A}^2_K$ defined by the polynomial $F = x^4 + y^4 - 2$ over the finite field $K = \mathbb{F}_5$. Using *Macaulay*2 **[GSa]** with the procedure below we obtain that F has 16 zeros in X. Notice that $I(X)$ is equal to $(x^5 - x, y^5 - y)$.

```
q=5
S=ZZ/q[x,y];
F=x^4 + y^4 - 2
Ix=ideal(x^q-x,y^q-y)
quotient(Ix,F)==Ix
J=ideal(Ix,F)
degree J
```

EXAMPLE 2.118. Let $V_X(F)$ be the curve in $X = \mathbb{A}^2_K$ defined by the polynomial $F = x^3 + y^6 - 3$ over the finite field $K = \mathbb{F}_7$. Using *Macaulay*2 **[GSa]** with the procedure below we obtain that F has no zeros. Notice that $I(X)$ is equal to $(x^7 - x, y^7 - y)$.

```
q=7
R=GF(q)[x,y];
F=x^3+y^6-3
Ix=ideal(x^q-x,y^q-y)
J=ideal(Ix,F)
quotient(Ix,F)==Ix
degree J
```

Next we illustrate the use of Theorem 4.10.

EXAMPLE 2.119. Let $V_X(F)$ be the variety in $X = \mathbb{P}^2$ defined by the polynomial

$$F = t_1^3 + t_2^3 + t_3^3 - 3t_1t_2t_3 - 3t_1^2t_2 - 3t_2^2t_3 - 3t_1t_3^2$$

over the finite field $K = \mathbb{F}_13$. Using *Macaulay*2 **[GSa]** with the procedure below we obtain that F has no zeros in $\mathbb{P}^2$.

```
q=13
R=GF(q)[t1,t2,t3];
F=ideal(t1^3+t2^3+t3^3-3*t1*t2*t3-3*t1^2*t2-3*t2^2*t3-3*t1*t3^2)
Ix=ideal(t1^q*t2-t1*t2^q,t1^q*t3-t1*t3^q,t2^q*t3-t2*t3^q)
J=ideal(Ix,F)
quotient(Ix,F)==Ix
degree J
```

CHAPTER 3

Reed–Muller-Type Codes

In this chapter we study the families of projective and affine Reed-Muller-type codes and their connection to vanishing ideals and Hilbert functions. Also, we show a finite version of Hilbert Nullstellensatz.

3.1. Projective Reed–Muller-type codes

Let $S = K[t_1, \ldots, t_s]$ be a polynomial ring over a finite field $K = \mathbb{F}_q$ with the standard grading $S = \oplus_{d=0}^{\infty} S_d$ and let $\mathbb{Y}$ be a subset of $\mathbb{P}^{s-1}$. Let $P_1, \ldots, P_m$ be a set of representatives for the points of $\mathbb{Y}$ with $m = |\mathbb{Y}|$. Fix a degree $d \geq 1$. For each i there is $f_i \in S_d$ such that $f_i(P_i) \neq 0$. Indeed suppose $P_i = [(a_1, \ldots, a_s)]$, there is at least one j in $\{1, \ldots, s\}$ such that $a_j \neq 0$. Setting $f_i(t_1, \ldots, t_s) = t_j^d$ one has that $f_i \in S_d$ and $f_i(P_i) \neq 0$. There is a K-linear map:

$$\text{ev}_d \colon S_d = K[t_1, \ldots, t_s]_d \to K^{|\mathbb{Y}|}, \quad f \mapsto \left(\frac{f(P_1)}{f_1(P_1)}, \ldots, \frac{f(P_m)}{f_m(P_m)} \right). \tag{3.1.1}$$

The map ev_d is called an *evaluation map*. The image of S_d under ev_d, denoted by $C_{\mathbb{Y}}(d)$, is called a *projective Reed–Muller-type code* of degree d over $\mathbb{Y}$ **[DRTR01, GSRTR02]**. It is also called an *evaluation code* associated to $\mathbb{Y}$ **[GLS05]**.

By a *linear code* we mean a linear subspace of K^m for some m and for some finite field K. Projective Reed–Muller-type codes are a special type of linear codes.

DEFINITION 3.1. Let $0 \neq v \in C_{\mathbb{Y}}(d)$. The *Hamming weight* of v, denoted by $\|v\|$ or by $\omega(v)$, is the number of non-zero entries of v. The *minimum distance* of $C_{\mathbb{Y}}(d)$, denoted by $\delta_{\mathbb{Y}}(d)$ or $\delta(C_{\mathbb{Y}}(d))$, is defined as

$$\delta_{\mathbb{Y}}(d) := \min\{\|v\|) \colon 0 \neq v \in C)\}.$$

DEFINITION 3.2. The *basic parameters* of the linear code $C_{\mathbb{Y}}(d)$ are: its *length* $|\mathbb{Y}|$, *dimension* $\dim_K C_{\mathbb{Y}}(d)$, and *minimum distance* $\delta_{\mathbb{Y}}(d)$.

If $\mathbb{Y} = \mathbb{P}^{s-1}$, $C_{\mathbb{Y}}(d)$ is the *classical projective Reed–Muller code*, and formulas for its basic parameters are given in **[Sor91**, Theorem 1].

DEFINITION 3.3. The set $\mathbb{T} = \{[(x_1, \ldots, x_s)] \in \mathbb{P}^{s-1} | \, x_i \in K^* \text{ for all } i\}$ is called a *projective torus* in $\mathbb{P}^{s-1}$, and the set $T = (K^*)^s$ is called an *affine torus* in $\mathbb{A}^s$, where $K^* = K \setminus \{0\}$.

If $\mathbb{T}$ is a projective torus in $\mathbb{P}^{s-1}$, $C_{\mathbb{T}}(d)$ is the *generalized projective Reed–Solomon code*, and formulas for its basic parameters are given in [**SPV11**, Theorem 3.5].
If $\mathbb{X}$ is the image of a cartesian product of subsets of K, under the morphism $K^{s-1} \to \mathbb{P}^{s-1}$, $x \to [x, 1]$, then $C_{\mathbb{X}}(d)$ is an *affine cartesian code* and formulas for its basic parameters were given in [**GT13, LRMV14**].

LEMMA 3.4. (a) *The map* ev_d *is well-defined, i.e., it is independent of the set of representatives that we choose for the points of* $\mathbb{X}$. (b) *The basic parameters of the Reed–Muller-type code* $C_{\mathbb{X}}(d)$ *are independent of* $f_1, \ldots, f_m$.

PROOF. (a): If $P'_1, \ldots, P'_m$ is another set of representatives, there are $\lambda_1, \ldots, \lambda_m$ in K^* such that $P'_i = \lambda_i P_i$ for all i. Thus, $f(P'_i)/f_i(P'_i) = f(P_i)/f_i(P_i)$ for $f \in S_d$ and $1 \leq i \leq m$.

(b): Let $f'_1, \ldots, f'_m$ be homogeneous polynomials of S of degree d such that $f'_i(P_i) \neq 0$ for $i = 1, \ldots, m$, and let

$$\mathrm{ev}'_d \colon S_d \to K^{|\mathbb{X}|}, \quad f \mapsto \left(\frac{f(P_1)}{f'_1(P_1)}, \ldots, \frac{f(P_m)}{f'_m(P_m)} \right)$$

be the evaluation map relative to $f'_1, \ldots, f'_m$. Then note that $\ker(\mathrm{ev}_d) = \ker(\mathrm{ev}'_d)$ and $\|\mathrm{ev}_d(f)\| = \|\mathrm{ev}'_d(f)\|$ for $f \in S_d$. It follows that the basic parameters of $\mathrm{ev}_d(S_d)$ and $\mathrm{ev}'_d(S_d)$ are the same. ♠

LEMMA 3.5. (Singleton bound) *Let* K *be a field and let* $V \subset K^s$ *be a vector subspace. Then*

$$\delta_V \leq s - \dim_K(V) + 1,$$

where $\delta_V = \min\{\|\alpha\| \, | \, \alpha \in V \setminus \{0\}\}$.

PROOF. Pick $\alpha = (\alpha_1, \ldots, \alpha_s)$ with $\delta_V = \|\alpha\|$. Consider the subspace W of K^s generated by $e_1, \ldots, e_{\delta_V - 1}$. Notice that $W \cap V = (0)$. Then

$$s \geq \dim_K(V + W) = \dim_K(V) + \dim_K(W) + \dim_K(V \cap W).$$

Therefore $s \geq \dim_K(V) + \delta_V - 1$, as required. ♠

The following summarizes the well-known relation between projective Reed–Muller-type codes and the theory of Hilbert functions. If $\mathbb{Y}$ is a subset of $\mathbb{P}^{s-1}$, we denote the Hilbert function $S/I(\mathbb{Y})$ by $H_{\mathbb{Y}}$.

PROPOSITION 3.6. ([**GSRTR02, RMSV11**]) *The following hold.*

(i) $H_{\mathbb{Y}}(d) = \dim_K C_{\mathbb{Y}}(d)$ *for* $d \geq 0$.

(ii) $\deg(S/I(\mathbb{Y})) = |\mathbb{Y}|$.
(iii) $\delta_{\mathbb{Y}}(d) = 1$ *for* $d \geq \operatorname{reg}(S/I(\mathbb{Y}))$.
(iv) $S/I(\mathbb{Y})$ *is a reduced Cohen–Macaulay graded ring of dimension* 1.
(v) $C_{\mathbb{Y}}(d) \neq (0)$ *for* $d \geq 1$.
(vi) (*Singleton bound*) $1 \leq \delta_{\mathbb{X}}(d) \leq |\mathbb{X}| - H_{\mathbb{X}}(d) + 1$.

PROOF. (i): The kernel of the evaluation map ev_d, defined in Eq. (3.1.1), is precisely $I(\mathbb{Y})_d$. Hence there is an isomorphism of K-vector spaces between $S_d/I(\mathbb{Y})_d$ and $C_{\mathbb{Y}}(d)$. Thus $H_{\mathbb{Y}}(d)$ is equal to $\dim_K C_{\mathbb{Y}}(d)$.

(ii): This follows readily from Proposition 2.95.

(iii): For $d \geq \operatorname{reg}(S/I(\mathbb{Y})))$, one has that $H_{\mathbb{Y}}(d) = |\mathbb{Y}|$. Thus, by part (i), we get that $C_{\mathbb{Y}}(d)$ is equal to $K^{|\mathbb{Y}|}$. Consequently $\delta_{\mathbb{Y}}(d) = 1$.

(iv): By Lemma 4.5, the primary decomposition of $I(\mathbb{Y})$ is

$$I(\mathbb{Y}) = \bigcap_{[Q]\in\mathbb{Y}} I_{[Q]}, \tag{3.1.2}$$

where $I_{[Q]}$ is a prime ideal of height $s-1$ for any $[Q] \in \mathbb{Y}$. Hence the height of $I(\mathbb{Y})$ is $s-1$ and the dimension of $S/I(\mathbb{Y})$ is 1. Hence $\operatorname{depth}(S/I(\mathbb{Y})) \leq 1$ (see Lemma 1.80). To complete the proof notice that, by Eq. (3.1.2), the maximal ideal $\mathfrak{m} = (t_1, \ldots, t_s)$ is not an associated prime of $I(\mathbb{Y})$; that is $\operatorname{depth}(S/I(\mathbb{Y})) > 0$ and $S/I(\mathbb{Y})$ is Cohen–Macaulay.

(v), (vi): Part (v) follows readily from Proposition 2.95 and part (vi) follows from Lemma 3.5. ♠

Degree and regularity via Hilbert series. The degree and the regularity of $S/I(\mathbb{Y})$ can be read off from its Hilbert series. Indeed, the Hilbert series can be written as

$$F_{\mathbb{Y}}(t) := \sum_{i=0}^{\infty} H_{\mathbb{Y}}(i)t^i = \sum_{i=0}^{\infty} \dim_K(S/I(\mathbb{Y}))_i t^i = \frac{h_0 + h_1 t + \cdots + h_r t^r}{1-t},$$

where $h_0, \ldots, h_r$ are positive integers; see **[Sta78]**. This follows from the fact that $I(\mathbb{Y})$ is a Cohen-Macaulay ideal of height $s-1$. The number r is the regularity of $S/I(\mathbb{Y})$ and $h_0 + \cdots + h_r$ is the degree of $S/I(\mathbb{Y})$.

3.2. Regularity and minimum distance

LEMMA 3.7. *Let* $\mathbb{Y} = \{[\alpha], [\beta]\}$ *be a subset of* $\mathbb{P}^{s-1}$ *with two elements. The following hold.*

(i) $\operatorname{reg} S/I(\mathbb{Y}) = 1$.
(ii) *There is* $h \in S_1$, *a form of degree* 1, *such that* $h(\alpha) \neq 0$ *and* $h(\beta) = 0$.
(iii) *For each* $d \geq 1$, *there is* $f \in S_d$, *a form of degree* d, *such that* $f(\alpha) \neq 0$ *and* $f(\beta) = 0$.

(iv) *If* $\mathbb{X}$ *is a subset of* $\mathbb{P}^{s-1}$ *with at least two elements and* $d \geq 1$*, then there is* $f \in S_d$ *such* $f \notin I(\mathbb{X})$ *and* $(I(\mathbb{X}) \colon f) \neq I(\mathbb{X})$.

PROOF. (i): As $H_{\mathbb{Y}}(0) = 1$ and $|\mathbb{Y}| = 2$, by Proposition 2.95, we get that $H_{\mathbb{Y}}(1) = |\mathbb{Y}| = 2$. Thus $S/I(\mathbb{Y})$ has regularity equal to 1.

(ii): Consider the evaluation map

$$\mathrm{ev}_1 \colon S_1 \longrightarrow K^2, \quad f \mapsto (f(\alpha)/f_1(\alpha), f(\beta)/f_2(\beta)).$$

By part (i) this map is onto. Thus $(1,0)$ is in the image of ev_1 and the result follows.

(iii): It follows from part (ii) by setting $f = h^d$.

(iv): By part (iii), there are distinct $[\alpha], [\beta]$ in $\mathbb{X}$ and $f \in S_d$ such that $f(\alpha) \neq 0, f(\beta) = 0$. Then $f \notin I(\mathbb{X})$. Notice that $f(\beta) = 0$ if and only if $f \in I_{[\beta]}$. Therefore, by Theorem 4.3 and Lemma 4.5, we have that f is a zero-divisor of $S/I(\mathbb{X})$, thus $(I(\mathbb{X}) \colon f) \neq I(\mathbb{X})$. ♠

The next result was shown in [**RMSV11**, Proposition 5.2] for some special type of Reed–Muller-type codes (cf. [**Toh09**, Proposition 2.1]).

PROPOSITION 3.8. *There is an integer* $r \geq 0$ *such that*

$$|\mathbb{X}| = \delta_{\mathbb{X}}(0) > \delta_{\mathbb{X}}(1) > \cdots > \delta_{\mathbb{X}}(d) = \delta_{\mathbb{X}}(r) = 1 \text{ for } d \geq r.$$

PROOF. Assume that $\delta_{\mathbb{X}}(d) > 1$, it suffices to show that $\delta_{\mathbb{X}}(d) > \delta_{\mathbb{X}}(d+1)$. Pick $g \in S_d$ such that $g \notin I(\mathbb{X})$ and

$$|V_{\mathbb{X}}(g)| = \max\{|V_{\mathbb{X}}(f)| \colon \mathrm{ev}_d(f) \neq 0; f \in S_d\}.$$

Then $\delta_{\mathbb{X}}(d) = |\mathbb{X}| - |V_{\mathbb{X}}(g)| \geq 2$. Thus there are distinct points $[\alpha], [\beta]$ in $\mathbb{X}$ such that $g(\alpha) \neq 0$ and $g(\beta) \neq 0$. By Lemma 3.7, there is a linear form $h \in S_1$ such that $h(\alpha) \neq 0$ and $h(\beta) = 0$. Hence the polynomial hg is not in $I(\mathbb{X})$, has degree $d+1$, and has at least $|V_{\mathbb{X}}(g)| + 1$ zeros. Thus $\delta_{\mathbb{X}}(d) > \delta_{\mathbb{X}}(d+1)$, as required. ♠

The *regularity* of $S/I(\mathbb{X})$, denoted $\mathrm{reg}(S/I(\mathbb{X}))$, is the least integer $r \geq 0$ such that $H_{\mathbb{X}}(d)$ is equal to $h_{I(\mathbb{X})}(d)$ for $d \geq r$. As is seen below, the knowledge of the regularity of $S/I(\mathbb{X})$ is important for applications to coding theory. According to [**GKR93**] and Proposition 3.8, there are integers $r \geq 0$ and $r_1 \geq 0$ such that

$$1 = H_{\mathbb{X}}(0) < H_{\mathbb{X}}(1) < \cdots < H_{\mathbb{X}}(r-1) < H_{\mathbb{X}}(d) = |\mathbb{X}|$$

for $d \geq r = \mathrm{reg}(S/I(\mathbb{X}))$, and

$$|\mathbb{X}| = \delta_{\mathbb{X}}(0) > \delta_{\mathbb{X}}(1) > \cdots > \delta_{\mathbb{X}}(r_1 - 1) > \delta_{\mathbb{X}}(r_1) = \delta_{\mathbb{X}}(d) = 1 \text{ for } d \geq r_1,$$

respectively. The integer r_1 is called the *regularity* of $\delta_{\mathbb{X}}$ and is denoted $\operatorname{reg}(\delta_{\mathbb{X}})$. In general $r_1 \leq r$ (see the discussion below). Using the methods of **[RMSV11, TV15]**, the regularity of $S/I(\mathbb{X})$ can be effectively computed when $\mathbb{X}$ is parameterized by monomials, but r_1 is very difficult to compute.

The Hilbert function and the minimum distance are related by the Singleton bound:

$$1 \leq \delta_{\mathbb{X}}(d) \leq |\mathbb{X}| - H_{\mathbb{X}}(d) + 1.$$

In particular, if $d \geq \operatorname{reg}(S/I(\mathbb{X})) \geq 1$, then $\delta_{\mathbb{X}}(d) = 1$. The converse is not true. Thus, potentially good Reed–Muller-type codes $C_{\mathbb{X}}(d)$ can occur only if $1 \leq d < \operatorname{reg}(S/I(\mathbb{X}))$. There are some families where $d \geq \operatorname{reg}(S/I(\mathbb{X})) \geq 1$ if and only if $\delta_{\mathbb{X}}(d) = 1$ **[LRMV14, SPV11, Sor91]**, but we do not know of any set $\mathbb{X}$ parameterized by monomials where this fails. If $\mathbb{X}$ is parameterized by monomials we say that $C_{\mathbb{X}}(d)$ is a *projective parameterized code* **[RMSV11, TV15]**.

Conjeture. If $\mathbb{X} \subset \mathbb{P}^{s-1}$ is parameterized by monomials and $X = \mathbb{T} \cap \mathbb{X}$, where $\mathbb{T}$ is a projective torus, then we have that $\operatorname{reg}(S/I(\mathbb{X})) = \operatorname{reg}(\delta_{\mathbb{X}})$ and $\operatorname{reg}(S/I(X)) = \operatorname{reg}(\delta_X)$.

3.3. Affine Reed–Muller-type codes

Let $K = \mathbb{F}_q$ be a finite field, let Y be a subset of $\mathbb{A}^s$, and let $\mathbb{Y}$ be the projective closure of Y. As Y is finite, its projective closure is:

$$\mathbb{Y} = \{[(\alpha, 1)] \,|\, \alpha \in Y\} \subset \mathbb{P}^s.$$

Let $S = K[t_1, \ldots, t_s]$ be a polynomial ring, let $P_1, \ldots, P_m$ be the points of Y, and let $S_{\leq d}$ be the K-vector space of all polynomials of S of degree at most d. The *evaluation map*

$$\operatorname{ev}_d^a \colon S_{\leq d} \longrightarrow K^{|Y|}, \quad f \mapsto (f(P_1), \ldots, f(P_m)),$$

defines a linear map of K-vector spaces. The image of ev_d^a, denoted by $C_Y(d)$, defines a *linear code*. We call $C_Y(d)$ the *affine Reed–Muller-type code* of degree d on Y **[TV13]**. If Y is a subset of $\mathbb{A}^s$, we denote the affine Hilbert function of $S/I(Y)$ by H_Y^a.

The regularity of $S[u]/I(\mathbb{Y})$ is important for applications to coding theory as the next result shows.

LEMMA 3.9. (a) $H_Y^a(d) = H_{\mathbb{Y}}(d)$ *for* $d \geq 0$.
(b) $\dim_K(C_Y(d)) = H_{\mathbb{Y}}(d)$ *and length of* $C_Y(d)$ *is* $\deg(S[u]/I(\mathbb{Y}))$.
(c) $\delta_Y(d) := \delta(C_Y(d)) = 1$ *for* $d \geq \operatorname{reg} S[u]/I(\mathbb{Y})$.

PROOF. (a): It follows at once from Proposition 2.88.

(b): The kernel of ev_d^a is $I(Y)_{\leq d}$. Thus $S_{\leq d}/I(Y)_{\leq d} \simeq C_Y(d)$. Therefore $H_Y^a(d) = \dim_K C_Y(d)$. Thus, by (a), the required equalities follows.

(c): For $d \geq \operatorname{reg} S[u]/I(\mathbb{Y})$ the linear code $C_Y(d)$ coincides with $K^{|Y|}$ and has, accordingly, minimum distance equal to 1. ♠

PROPOSITION 3.10. *The affine Reed–Muller-type code $C_Y(d)$ has the same basic parameters that the projective Reed–Muller-type code $C_{\mathbb{Y}}(d)$.*

PROOF. We set $Q_i = (P_i, 1)$ for $i = 1, \ldots, m$, where $P_1, \ldots, P_m$ are the points of Y. Thanks to Lemma 3.4 we may take $Q_1, \ldots, Q_m$ as the set of representatives of $\mathbb{Y}$ and assume that $C_{\mathbb{Y}}(d)$ is the image of the linear map

$$\mathrm{ev}_d \colon S[u]_d \to K^{|\mathbb{Y}|}, \quad f \mapsto (f(Q_i)/f_i(Q_i))_{i=1}^m,$$

where $f_i(t_1, \ldots, t_n, u) = u^d$ for $i = 1, \ldots, m$ and u is a new variable. Thus it suffices to show that $C_Y(d) = C_{\mathbb{Y}}(d)$ for $d \geq 1$. Since

$$S[u]_d/I(\mathbb{Y})_d \simeq C_{\mathbb{Y}}(d) \text{ and } S_{\leq d}/I(Y)_{\leq d} \simeq C_Y(d),$$

by Lemma 3.9, we get that the linear codes $C_Y(d)$ and $C_{\mathbb{Y}}(d)$ have the same dimension, and the same length. Thus, it suffices to show the inclusion "$\supset$". Any point of $C_{\mathbb{Y}}(d)$ has the form $W = (f(P_i, 1))_{i=1}^m$ with $f \in S[u]_d$. If $\widetilde{f}$ is the polynomial $f(t_1, \ldots, t_n, 1)$, then $\widetilde{f}$ is in $S_{\leq d}$ and $f(P_i, 1) = \widetilde{f}(P_i)$ for all i. Thus, W is in $C_Y(d)$, as required. ♠

Affine variety codes. Let X be a finite subset of an affine space $\mathbb{A}_K^s$ over a field K and let $I(X)$ be its vanishing ideal. The coordinate ring

$$S/I(X) = K[t_1, \ldots, t_s]/I(X)$$

of the affine variety X is an Artinian ring, because it has Krull dimension zero, and $\dim_K(S/I(X)) = \deg S/I(X) = |X|$ (see Lemma 3.9). Thus we have an isomorphism of K-vector spaces

$$\phi \colon S/I(X) \to \mathbb{A}^m, \ \overline{f} \mapsto (f(P_1), \ldots, f(P_m)),$$

where $X = \{P_1, \ldots, P_m\}$ and $m = |X|$. If $K = \mathbb{F}_q$ is a finite field and $X = \mathbb{A}^s$, then $I(X) = (t_1^q - t_1, \ldots, t_s^q - t_s)$.

DEFINITION 3.11 (**[FL98]**). Let $K = \mathbb{F}_q$ be a finite field and let L be a K-linear subspace of $S/I(X)$. The *affine variety code*, denoted by $C(I(X), L)$, is the image of L under the evaluation map ϕ.

Affine variety codes are a natural generalization of affine Reed–Muller-type codes. The decoding of affine variety codes using Gröbner basis was studied in **[FL98]**. The images

in $S/I(X)$ of the set of standard monomials of $I(X)$ with respect to a monomial order $\prec$ form a K-basis of $S/I(X)$. This is why it is natural to use Gröbner basis to study affine variety codes.

CHAPTER 4

Generalized Minimum Distance Functions

We explore the r-th generalized minimum distance function (gmd function for short) and the corresponding generalized footprint function of a graded ideal in a polynomial ring over a field. If $\mathbb{X}$ is a set of projective points over a finite field and $I(\mathbb{X})$ is its vanishing ideal, we show that the gmd function and the Vasconcelos function of $I(\mathbb{X})$ are equal to the r-th generalized Hamming weight of the corresponding Reed-Muller-type code $C_{\mathbb{X}}(d)$. We show that the r-th generalized footprint function of $I(\mathbb{X})$ is a lower bound for the r-th generalized Hamming weight of $C_{\mathbb{X}}(d)$. As an application to coding theory we show an explicit formula and a combinatorial formula for the second generalized Hamming weight of an affine cartesian code.

4.1. Generalized Hamming weights and commutative algebra

In this section we recall some of the results that will be needed throughout this chapter and introduce some more notation. All results of this section are well-known.

Generalized Hamming weights. Let $K = \mathbb{F}_q$ be a finite field and let C be a $[m, k]$ *linear code* of *length* m and *dimension* k.

The r-th *generalized Hamming weight* of C, denoted $\delta_r(C)$, is the size of the smallest support of an r-dimensional subcode, that is,

$$\delta_r(C) := \min\{|\chi(D)| : \ D \text{ is a linear subcode of } C \text{ with } \dim_K(D) = r\}.$$

The *weight hierarchy* of C is the sequence $(\delta_1(C), \ldots, \delta_k(C))$ and $\delta_1(C)$ is called the *minimum distance* of C and is denoted by $\delta(C)$. According to **[Wei91**, Theorem 1, Corollary 1] the weight hierarchy is an increasing sequence

$$1 \leq \delta_1(C) < \delta_2(C) < \cdots < \delta_r(C) \leq m,$$

and $\delta_r(C) \leq m - k + r$ for $r = 1, \ldots, k$. For $r = 1$ this is the Singleton bound for the minimum distance. Notice that $\delta_r(C) \geq r$.

Recall that the *support* $\chi(\beta)$ of a vector $\beta \in K^m$ is $\chi(K\beta)$, that is, $\chi(\beta)$ is the set of non-zero entries of β.

LEMMA 4.1. *Let D be a subcode of C of dimension $r \geq 1$. If $\beta_1, \ldots, \beta_r$ is a K-basis for D with $\beta_i = (\beta_{i,1}, \ldots, \beta_{i,m})$ for $i = 1, \ldots, r$, then $\chi(D) = \cup_{i=1}^{r} \chi(\beta_i)$ and the number of elements of $\chi(D)$ is the number of non-zero columns of the matrix:*

$$\begin{bmatrix} \beta_{1,1} & \cdots & \beta_{1,i} & \cdots & \beta_{1,m} \\ \beta_{2,1} & \cdots & \beta_{2,i} & \cdots & \beta_{2,m} \\ \vdots & \cdots & \vdots & \cdots & \vdots \\ \beta_{r,1} & \cdots & \beta_{r,i} & \cdots & \beta_{r,m} \end{bmatrix}.$$

Commutative algebra. Let $S = K[t_1, \ldots, t_s] = \oplus_{d=0}^{\infty} S_d$ be a polynomial ring over a field K with the standard grading and let $I \neq (0)$ be a graded ideal of S of Krull dimension k. The *Hilbert function* of S/I is:

$$H_I(d) := \dim_K(S_d/I_d), \quad d = 0, 1, 2, \ldots,$$

where $I_d = I \cap S_d$. By a theorem of Hilbert [**Sta78**, p. 58], there is a unique polynomial $h_I(x) \in \mathbb{Q}[x]$ of degree $k-1$ such that $H_I(d) = h_I(d)$ for $d \gg 0$. The degree of the zero polynomial is -1.

The *degree* or *multiplicity* of S/I is the positive integer

$$\deg(S/I) := \begin{cases} (k-1)! \lim_{d\to\infty} H_I(d)/d^{k-1} & \text{if } k \geq 1, \\ \dim_K(S/I) & \text{if } k = 0. \end{cases}$$

We will use the following multi-index notation: for $a = (a_1, \ldots, a_s) \in \mathbb{N}^s$, set $t^a := t_1^{a_1} \cdots t_s^{a_s}$. The multiplicative group of the field K is denoted by K^*. As usual $\operatorname{ht}(I)$ will denote the height of the ideal I. By the dimension of I (resp. S/I) we mean the Krull dimension of S/I. The Krull dimension of S/I is denoted by $\dim(S/I)$.

One of the most useful and well-known facts about the degree is its additivity:

PROPOSITION 4.2. (Additivity of the degree [**OPVV14**, Proposition 2.5]) *If I is an ideal of S and $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$ is an irredundant primary decomposition, then*

$$\deg(S/I) = \sum_{\operatorname{ht}(\mathfrak{q}_i)=\operatorname{ht}(I)} \deg(S/\mathfrak{q}_i).$$

If $F \subset S$, the *quotient ideal* of I with respect to (F) is given by $(I\colon (F))$. An element f is called a *zero-divisor* of S/I if there is $\overline{0} \neq \overline{a} \in S/I$ such that $f\overline{a} = \overline{0}$, and f is called *regular* on S/I if f is not a zero-divisor. Thus f is a zero-divisor if and only if $(I\colon f) \neq I$. An associated prime of I is a prime ideal $\mathfrak{p}$ of S of the form $\mathfrak{p} = (I\colon f)$ for some f in S.

THEOREM 4.3. [**Vil15**, Lemma 2.1.19, Corollary 2.1.30] *If I is an ideal of S and $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$ is an irredundant primary decomposition with $\operatorname{rad}(\mathfrak{q}_i) = \mathfrak{p}_i$, then the set of zero-divisors $\mathcal{Z}(S/I)$ of S/I is equal to $\bigcup_{i=1}^{m} \mathfrak{p}_i$, and $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ are the associated primes of I.*

DEFINITION 4.4. The *regularity* of S/I, denoted $\operatorname{reg}(S/I)$, is the least integer $r \geq 0$ such that $H_I(d)$ is equal to $h_I(d)$ for $d \geq r$.

The footprint of an ideal. Let $\prec$ be a monomial order on S and let $(0) \neq I \subset S$ be an ideal. A monomial t^a is called a *standard monomial* of S/I, with respect to $\prec$, if t^a is not the leading monomial of any polynomial in I. The set of standard monomials, denoted $\Delta_\prec(I)$, is called the *footprint* of S/I. The image of the standard polynomials of degree d, under the canonical map $S \mapsto S/I$, $x \mapsto \overline{x}$, is equal to S_d/I_d, and the image of $\Delta_\prec(I)$ is a basis of S/I as a K-vector space (see [**Vil15**, Proposition 3.3.13]). In particular, if I is graded, then $H_I(d)$ is the number of standard monomials of degree d.

A subset $\mathcal{G} = \{g_1, \ldots, g_r\}$ of I is called a *Gröbner basis* of I if

$$\operatorname{in}_\prec(I) = (\operatorname{in}_\prec(g_1), \ldots, \operatorname{in}_\prec(g_r)).$$

Vanishing ideal of a finite set. The *projective space* of dimension $s-1$ over the field K is denoted $\mathbb{P}^{s-1}$. It is usual to denote the equivalence class of α by $[\alpha]$.

For a given a subset $\mathbb{X} \subset \mathbb{P}^{s-1}$ define $I(\mathbb{X})$, the *vanishing ideal* of $\mathbb{X}$, as the ideal generated by the homogeneous polynomials in S that vanish at all points of $\mathbb{X}$, and given a graded ideal $I \subset S$ define its *zero set* relative to $\mathbb{X}$ as

$$V_{\mathbb{X}}(I) = \{[\alpha] \in \mathbb{X} |\, f(\alpha) = 0 \ \forall f \in I \text{ homogeneous}\}.$$

In particular, if $f \in S$ is homogeneous, the zero set $V_{\mathbb{X}}(f)$ of f is the set of all $[\alpha] \in \mathbb{X}$ such that $f(\alpha) = 0$, that is $V_{\mathbb{X}}(f)$ is the set of zeros of f in $\mathbb{X}$.

LEMMA 4.5. *Let $\mathbb{X}$ be a finite subset of $\mathbb{P}^{s-1}$, and consider $[\alpha]$ be a point in $\mathbb{X}$ with $\alpha = (\alpha_1, \ldots, \alpha_s)$ and $\alpha_k \neq 0$ for some k, and let $I_{[\alpha]}$ be the vanishing ideal of $[\alpha]$. Then $I_{[\alpha]}$ is a prime ideal,*

$$I_{[\alpha]} = (\{\alpha_k t_i - \alpha_i t_k |\, k \neq i \in \{1, \ldots, s\}),\ \deg(S/I_{[\alpha]}) = 1,$$

$\operatorname{ht}(I_{[\alpha]}) = s-1$, *and $I(\mathbb{X}) = \bigcap_{[\beta] \in \mathbb{X}} I_{[\beta]}$ is the primary decomposition of $I(\mathbb{X})$.*

DEFINITION 4.6. The set $\mathbb{T} = \{[(x_1, \ldots, x_s)] \in \mathbb{P}^{s-1} |\, x_i \in K^* \ \forall\, i\}$ is called a *projective torus*.

4.2. Computing the number of points of a variety

In this section we give a degree formula to compute the number of solutions of a system of homogeneous polynomials over any given finite set of points in a projective space over a field.

LEMMA 4.7. *Let $\mathbb{X}$ be a finite subset of $\mathbb{P}^{s-1}$ over a field K. If $F = \{f_1, \ldots, f_r\}$ is a set of homogeneous polynomials of $S \setminus \{0\}$, then*

$$V_{\mathbb{X}}(F) = \emptyset \quad \textit{if and only if} \quad (I(\mathbb{X})\colon (F)) = I(\mathbb{X})$$

.

PROOF. $\Rightarrow$) Assume that that $I(\mathbb{X}) \subsetneq (I(\mathbb{X})\colon (F))$. Pick a homogeneous polynomial g such that $gf_i \in I(\mathbb{X})$ for all i and $g \notin I(\mathbb{X})$. Then there is $[\alpha]$ in $\mathbb{X}$ such that $g(\alpha) \neq 0$. Thus $f_i(\alpha) = 0$ for all i, that is, $[\alpha] \in V_{\mathbb{X}}(F)$, a contradiction.

$\Leftarrow$) We can write $\mathbb{X} = \{[P_1], \ldots, [P_m]\}$ and $I(\mathbb{X}) = \cap_{i=1}^{m} \mathfrak{p}_i$, where $\mathfrak{p}_i$ is equal to $I_{[P_i]}$, the vanishing ideal of $[P_i]$. We proceed by contradiction assuming that $V_{\mathbb{X}}(F) \neq \emptyset$. Pick $[P_i]$ in $V_{\mathbb{X}}(F)$. For simplicity of notation assume that $i = 1$. Notice that $(\mathfrak{p}_1\colon (F)) = (1)$. Therefore

$$\bigcap_{i=1}^{m} \mathfrak{p}_i = I(\mathbb{X}) = (I(\mathbb{X})\colon (F)) = \bigcap_{i=1}^{m} (\mathfrak{p}_i\colon (F)) = \bigcap_{i=2}^{m} (\mathfrak{p}_i\colon (F)) \subset \mathfrak{p}_1.$$

Hence $\mathfrak{p}_i \subset (\mathfrak{p}_i\colon (F)) \subset \mathfrak{p}_1$ for some $i \geq 2$, see **[Vil15**, p. 74]. Thus $\mathfrak{p}_i = \mathfrak{p}_1$, a contradiction. ♠

An ideal $I \subset S$ is called *unmixed* if all its associated primes have the same height, and I is called *radical* if I is equal to its radical. The radical of I is denoted by $\operatorname{rad}(I)$.

LEMMA 4.8. *Let $\mathbb{X}$ be a finite subset of $\mathbb{P}^{s-1}$ over a field K and let $I(\mathbb{X}) \subset S$ be its vanishing ideal. If $F = \{f_1, \ldots, f_r\}$ is a set of homogeneous polynomials of $S \setminus \{0\}$, then*

$$|\mathbb{X} \setminus V_{\mathbb{X}}(F)| = \begin{cases} \deg S/(I(\mathbb{X})\colon (F)) & \textit{if } (I(\mathbb{X})\colon (F)) \neq I(\mathbb{X}), \\ \deg S/I(\mathbb{X}) & \textit{if } (I(\mathbb{X})\colon (F)) = I(\mathbb{X}). \end{cases}$$

PROOF. Let $[P_1], \ldots, [P_m]$ be the points of $\mathbb{X}$ with $m = |\mathbb{X}|$, and let $[P]$ be a point in $\mathbb{X}$ with $P = (\alpha_1, \ldots, \alpha_s)$ and $\alpha_k \neq 0$ for some k. Then the vanishing ideal $I_{[P]}$ of $[P]$ is a prime ideal of height $s - 1$,

$$I_{[P]} = (\{\alpha_k t_i - \alpha_i t_k |\, k \neq i \in \{1, \ldots, s\}), \ \deg(S/I_{[P]}) = 1,$$

and $I(\mathbb{X}) = \bigcap_{i=1}^{m} I_{[P_i]}$ is a primary decomposition (see Lemma 4.5).

Assume that $(I(\mathbb{X})\colon (F)) \neq I(\mathbb{X})$. We set $I = I(\mathbb{X})$ and $\mathfrak{p}_i = I_{[P_i]}$ for all $i = 1, \ldots, m$. Notice that $(\mathfrak{p}_j\colon f_i) = (1)$ if and only if $f_i \in \mathfrak{p}_j$ if and only if $f_i(P_j) = 0$. Then

$$(I\colon (F)) = \bigcap_{i=1}^{r} (I\colon f_i) = \left(\bigcap_{f_1(P_j)\neq 0} \mathfrak{p}_j\right) \bigcap \cdots \bigcap \left(\bigcap_{f_r(P_j)\neq 0} \mathfrak{p}_j\right) = \bigcap_{[P_j]\notin V_{\mathbb{X}}(F)} \mathfrak{p}_j.$$

Therefore, by the additivity of the degree of Proposition 4.2, we get that $\deg S/(I\colon (F))$ is equal to $|\mathbb{X} \setminus V_{\mathbb{X}}(F)|$. If $(I(\mathbb{X})\colon (F)) = I(\mathbb{X})$, then $V_{\mathbb{X}}(F) = \emptyset$ (see Lemma 4.7). Thus $|V_{\mathbb{X}}(F)| = 0$ and the required formula follows because $|\mathbb{X}| = \deg S/I(\mathbb{X})$. ♠

LEMMA 4.9. *Let $I \subset S$ be a radical unmixed graded ideal. If $F = \{f_1, \ldots, f_r\}$ is a set of homogeneous polynomials of $S \setminus \{0\}$, $(I\colon (F)) \neq I$, and $\mathcal{A}$ is the set of all associated primes of S/I that contain F, then* $\operatorname{ht}(I) = \operatorname{ht}(I, F)$ *and*

$$\deg(S/(I, F)) = \sum_{\mathfrak{p}\in\mathcal{A}} \deg(S/\mathfrak{p}).$$

PROOF. As $I \subsetneq (I\colon (F))$, there is $g \in S \setminus I$ such that $g(F) \subset I$. Hence the ideal (F) is contained in the set of zero-divisors of S/I. Thus, by Theorem 4.3 and since I is unmixed, (F) is contained in an associated prime ideal $\mathfrak{p}$ of S/I of height $\operatorname{ht}(I)$. Thus $I \subset (I, F) \subset \mathfrak{p}$, and consequently $\operatorname{ht}(I) = \operatorname{ht}(I, F)$. Therefore the set of associated primes of (I, F) of height equal to $\operatorname{ht}(I)$ is not empty and is equal to $\mathcal{A}$. There is an irredundant primary decomposition

$$(I, F) = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r \cap \mathfrak{q}'_{r+1} \cap \cdots \cap \mathfrak{q}'_t, \tag{4.2.1}$$

where $\operatorname{rad}(\mathfrak{q}_i) = \mathfrak{p}_i$, $\mathcal{A} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$, and $\operatorname{ht}(\mathfrak{q}'_i) > \operatorname{ht}(I)$ for $i > r$. We may assume that the associated primes of S/I are $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ with $r \leq m$. Since I is a radical ideal, we get that $I = \cap_{i=1}^{m} \mathfrak{p}_i$. Next we show the following equality:

$$\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_m = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r \cap \mathfrak{q}'_{r+1} \cap \cdots \cap \mathfrak{q}'_t \cap \mathfrak{p}_{r+1} \cap \cdots \cap \mathfrak{p}_m. \tag{4.2.2}$$

"$\supset$" is clear because $\mathfrak{q}_i \subset \mathfrak{p}_i$ for $i = 1, \ldots, r$. The inclusion "$\subset$" follows by noticing that the right hand side of Eq. (4.2.2) is equal to $(I, f) \cap \mathfrak{p}_{r+1} \cap \cdots \cap \mathfrak{p}_m$, and consequently it contains $I = \cap_{i=1}^{m} \mathfrak{p}_i$. Notice that $\operatorname{rad}(\mathfrak{q}'_j) = \mathfrak{p}'_j \not\subset \mathfrak{p}_i$ for all i, j and $\mathfrak{p}_j \not\subset \mathfrak{p}_i$ for $i \neq j$. Hence localizing Eq. (4.2.2) at the prime ideal $\mathfrak{p}_i$ for $i = 1, \ldots, r$, we get that $\mathfrak{p}_i = I_{\mathfrak{p}_i} \cap S = (\mathfrak{q}_i)_{\mathfrak{p}_i} \cap S = \mathfrak{q}_i$ for $i = 1, \ldots, r$. Using Eq. (4.2.1), together with the additivity of the degree of Proposition 4.2, the required equality follows. ♠

LEMMA 4.10. *Let $\mathbb{X}$ be a finite subset of $\mathbb{P}^{s-1}$ over a field K and let $I(\mathbb{X}) \subset S$ be its vanishing ideal. If $F = \{f_1, \ldots, f_r\}$ is a set of homogeneous polynomials of $S \setminus \{0\}$, then the number of*

points of $V_{\mathbb{X}}(F)$ is given by

$$|V_{\mathbb{X}}(F)| = \begin{cases} \deg S/(I(\mathbb{X}), F) & \text{if } (I(\mathbb{X})\colon (F)) \neq I(\mathbb{X}), \\ 0 & \text{if } (I(\mathbb{X})\colon (F)) = I(\mathbb{X}). \end{cases}$$

PROOF. Let $[P_1], \ldots, [P_m]$ be the points of $\mathbb{X}$ with $m = |\mathbb{X}|$. The vanishing ideal $I_{[P_i]}$ of $[P_i]$ is a prime ideal of height $s-1$, $\deg(S/I_{[P_i]}) = 1$, and $I(\mathbb{X}) = \bigcap_{i=1}^{m} I_{[P_i]}$ (see Lemma 4.5).

Assume that $(I(\mathbb{X})\colon (F)) \neq I(\mathbb{X})$. Let $\mathcal{A}$ be the set of all $I_{[P_i]}$ that contain the set F. Notice that $f_j \in I_{[P_i]}$ if and only if $f_j(P_i) = 0$. Then $[P_i]$ is in $V_{\mathbb{X}}(F)$ if and only if $F \subset I_{[P_i]}$. Thus $[P_i]$ is in $V_{\mathbb{X}}(F)$ if and only if $I_{[P_i]}$ is in $\mathcal{A}$. Hence, by Lemma 4.9, we get

$$|V_{\mathbb{X}}(F)| = \sum_{[P_i] \in V_{\mathbb{X}}(F)} \deg S/I_{[P_i]} = \sum_{F \subset I_{[P_i]}} \deg S/I_{[P_i]} = \deg S/(I(\mathbb{X}), F).$$

Assume that $(I(\mathbb{X})\colon F) = I(\mathbb{X})$. Then, by Lemma 4.7, $V_{\mathbb{X}}(f) = \emptyset$ and $|V_{\mathbb{X}}(f)| = 0$. ♠

PROPOSITION 4.11. *If $\mathbb{X}$ is a finite subset of $\mathbb{P}^{s-1}$, then*

$$\deg(S/I(\mathbb{X})) = \deg(S/(I(\mathbb{X}), F)) + \deg(S/(I(\mathbb{X})\colon (F))).$$

PROOF. It follows from Lemmas 4.8 and 4.10. ♠

THEOREM 4.12 (Finite Affine Hilbert Nullstellensatz). *Let $K = \mathbb{F}_q$ be a finite field and let $I \subset S$ be an ideal. Then*

$$I(V(I)) = I + (t_1^q - t_1, \ldots, t_s^q - t_s).$$

PROOF. We set $J = (t_1^q - t_1, \ldots, t_s^q - t_s)$. The inclusion $I + J \subset I(V(I))$ is clear because the elements of J vanish at all points of $\mathbb{A}_K^s$. Let $\mathbb{F}$ be the algebraic closure of $\mathbb{F}_q$ which is an algebraically closed field and let $B = \mathbb{F}[t_1, \ldots, t_s]$. As the roots of $t_i^q - t_i$ are exactly the elements of $\mathbb{F}_q$ one has $V_{\mathbb{F}}((I+J)B) = V(I+J)$, where $(I+J)B$ is the extension of $I + J$ to B. By Seidenberg's Lemma (see Lemma 2.113), we obtain that $(I+J)B$ is a radical ideal of dimension zero. Hence, by Hilbert Nullstellensatz (see Theorem 2.83), one has $I(V_{\mathbb{F}}((I+J)B)) = (I+J)B$. By this equality any element of $I(V(I+J))$ is in $(I+J)B \cap S = I + J$. To complete the proof notice that $V(I+J) = V(I)$. ♠

COROLLARY 4.13. *Let $K = \mathbb{F}_q$ be a finite field and let $I \subset S$ be an ideal. Then $V(I) = \emptyset$ if and only if $I + (t_1^q - t_1, \ldots, t_s^q - t_s) = S$.*

PROOF. It follows from the proof of Theorem 4.12. ♠

4.3. Generalized minimum distance function of a graded ideal

In this part we study the generalized minimum distance function of a graded ideal and show that it generalizes the generalized Hamming weight of a projective Reed-Muller-type code. To avoid repetitions, we continue to employ the notations and definitions used in the above sections.

LEMMA 4.14. *Let $I \subset S$ be an unmixed graded ideal and let $\prec$ be a monomial order. If F is a finite set of homogeneous polynomials of S and $(I\colon (F)) \neq I$, then*

$$\deg(S/(I,F)) \leq \deg(S/(\mathrm{in}_\prec(I), \mathrm{in}_\prec(F))) \leq \deg(S/I),$$

and $\deg(S/(I,F)) < \deg(S/I)$ *if I is an unmixed radical ideal and $(F) \not\subset I$.*

PROOF. To simplify notation we set $J = (I,F)$, $L = (\mathrm{in}_\prec(I), \mathrm{in}_\prec(F))$, and set $F = \{f_1, \ldots, f_r\}$. We denote the Krull dimension of S/I by $\dim(S/I)$. Recall that $\dim(S/I) = \dim(S) - \mathrm{ht}(I)$. First we show that S/J and S/L have Krull dimension equal to $\dim(S/I)$. As $I \subsetneq (I\colon F)$, all elements of F are zero divisors of S/I. Hence, as I is unmixed, there is an associated prime ideal $\mathfrak{p}$ of S/I such that $(F) \subset \mathfrak{p}$ and $\dim(S/I) = \dim(S/\mathfrak{p})$. Since $I \subset J \subset \mathfrak{p}$, we get that $\dim(S/J)$ is $\dim(S/I)$. Since S/I and $S/\mathrm{in}_\prec(I)$ have the same Hilbert function, and so does $S/\mathfrak{p}$ and $S/\mathrm{in}_\prec(\mathfrak{p})$, we obtain

$$\dim(S/\mathrm{in}_\prec(I)) = \dim(S/I) = \dim(S/\mathfrak{p}) = \dim(S/\mathrm{in}_\prec(\mathfrak{p})).$$

Hence, taking heights in the inclusions $\mathrm{in}_\prec(I) \subset L \subset \mathrm{in}_\prec(\mathfrak{p})$, we get $\mathrm{ht}(I) = \mathrm{ht}(L)$.

Pick a Gröbner basis $\mathcal{G} = \{g_1, \ldots, g_r\}$ of I. Then J is generated by $\mathcal{G} \cup F$ and by Lemma 2.102 one has the inclusions

$$\Delta_\prec(J) = \Delta_\prec(I,F) \subset \Delta_\prec(\mathrm{in}_\prec(g_1), \ldots, \mathrm{in}_\prec(g_r), \mathrm{in}_\prec(F)) =$$
$$\Delta_\prec(\mathrm{in}_\prec(I), \mathrm{in}_\prec(F)) = \Delta_\prec(L) \subset \Delta_\prec(\mathrm{in}_\prec(g_1), \ldots, \mathrm{in}_\prec(g_r)) = \Delta_\prec(I).$$

Thus $\Delta_\prec(J) \subset \Delta_\prec(L) \subset \Delta_\prec(I)$. Recall that $H_I(d)$, the Hilbert function of I at d, is the number of standard monomials of degree d. Hence $H_J(d) \leq H_L(d) \leq H_I(d)$ for $d \geq 0$. If $\dim(S/I)$ is equal to 0, then

$$\deg(S/J) = \sum_{d\geq 0} H_J(d) \leq \deg(S/L) = \sum_{d\geq 0} H_L(d) \leq \deg(S/I) = \sum_{d\geq 0} H_I(d).$$

Assume now that $\dim(S/I) \geq 1$. By a theorem of Hilbert [**Sta78**, p. 58], H_J, H_L, H_I are polynomial functions of degree equal to $k = \dim(S/I) - 1$ (see [**BH98**, Theorem 4.1.3]). Thus

$$k! \lim_{d\to\infty} H_J(d)/d^k \leq k! \lim_{d\to\infty} H_L(d)/d^k \leq k! \lim_{d\to\infty} H_I(d)/d^k,$$

that is, $\deg(S/J) \leq \deg(S/L) \leq \deg(S/I)$.

If I is an unmixed radical ideal and $(F) \not\subset I$, then there is at least one minimal prime that does not contains (F). Hence, by Lemma 4.9, it follows that $\deg(S/(I,F)) < \deg(S/I)$. ♠

COROLLARY 4.15. *Let $\mathbb{X}$ be a finite subset of $\mathbb{P}^{s-1}$, let $I(\mathbb{X}) \subset S$ be its vanishing ideal, and let $\prec$ be a monomial order. If F is a finite set of homogeneous polynomials of S and $(I(\mathbb{X})\colon (F)) \neq I(\mathbb{X})$, then*

$$|V_{\mathbb{X}}(F)| = \deg(S/(I(\mathbb{X}),F)) \leq \deg(S/(\mathrm{in}_{\prec}(I(\mathbb{X})),\mathrm{in}_{\prec}(F))) \leq \deg(S/I(\mathbb{X})),$$

and $\deg(S/(I(\mathbb{X}),F)) < \deg(S/I(\mathbb{X}))$ if $(F) \not\subset I(\mathbb{X})$.

PROOF. It follows from Lemmas 4.10 and 4.14. ♠

LEMMA 4.16. *Let $\mathbb{X} = \{[P_1],\ldots,[P_m]\}$ be a finite subset of $\mathbb{P}^{s-1}$ and let D be a linear subspace of $C_{\mathbb{X}}(d)$ of dimension $r \geq 1$. The following hold.*

(i) *There are $\overline{f}_1,\ldots,\overline{f}_r$ linearly independent elements of S_d/I_d such that*

$$D = \oplus_{i=1}^{r} K\beta_i,$$

where β_i is $(f_i(P_1),\ldots,f_i(P_m))$, and the support $\chi(D)$ of D is equal to $\cup_{i=1}^{r}\chi(\beta_i)$.

(ii) $|\chi(D)| = |\mathbb{X} \setminus V_{\mathbb{X}}(f_1,\ldots,f_r)|$.

(iii) $\delta_r(C_{\mathbb{X}}(d)) = \min\{|\mathbb{X} \setminus V_{\mathbb{X}}(F)| : F = \{f_i\}_{i=1}^{r} \subset S_d\}$ *where $\{\overline{f}_i\}_{i=1}^{r}$ are linearly independent over K.*

PROOF. (i): This part follows from Lemma 4.1 and using that the evaluation map ev_d induces an isomorphism between S_d/I_d and $C_{\mathbb{X}}(d)$.

(ii): Consider the matrix A with rows $\beta_1,\ldots,\beta_r$. Notice that the i-th column of A is not zero if and only if $[P_i]$ is in $\mathbb{X} \setminus V_{\mathbb{X}}(f_1,\ldots,f_r)$. It suffices to observe that the number of non-zero columns of A is $|\chi(D)|$ (see Lemma 4.1).

(iii): This follows from part (ii) and using the definition of the r-th generalized Hamming weight of $C_{\mathbb{X}}(d)$ (see Section 4.1). ♠

DEFINITION 4.17. If $I \subset S$ is a graded ideal, the *Vasconcelos function* of I is the function $\vartheta_I\colon \mathbb{N}_+ \times \mathbb{N}_+ \to \mathbb{N}$ given by

$$\vartheta_I(d,r) := \begin{cases} \min\{\deg(S/(I\colon (F)))|\, F \in \mathcal{F}_{d,r}\} & \text{if } \mathcal{F}_{d,r} \neq \emptyset, \\ \deg(S/I) & \text{if } \mathcal{F}_{d,r} = \emptyset. \end{cases}$$

THEOREM 4.18. *Let K be a field and let $\mathbb{X}$ be a finite subset of $\mathbb{P}^{s-1}$. If $|\mathbb{X}| \geq 2$ and $\delta_{\mathbb{X}}(d,r)$ is the r-th generalized Hamming weight of $C_{\mathbb{X}}(d)$, then*

$$\delta_{\mathbb{X}}(d,r) = \delta_{I(\mathbb{X})}(d,r) = \vartheta_I(d,r) \text{ for } d \geq 1 \text{ and } 1 \leq r \leq H_{I(\mathbb{X})}(d),$$

and $\delta_{\mathbb{X}}(d,r) = r$ for $d \geq \operatorname{reg}(S/I(\mathbb{X}))$.

PROOF. If $\mathcal{F}_{d,r} = \emptyset$, then using Lemmas 4.8, 4.10, and 4.16 we get that $\delta_{\mathbb{X}}(d,r)$, $\delta_{I(\mathbb{X})}(d,r)$, and $\vartheta_{I(\mathbb{X})}(d,r)$ are equal to $\deg(S/I(\mathbb{X})) = |\mathbb{X}|$. Assume that $\mathcal{F}_{d,r} \neq \emptyset$ and set $I = I(\mathbb{X})$. Using Lemma 4.16 and the formula for $V_{\mathbb{X}}(f)$ of Lemma 4.10, we obtain

$$\begin{aligned}
\delta_{\mathbb{X}}(d,r) &\overset{(4.16)}{=} \min\{|\mathbb{X} \setminus V_{\mathbb{X}}(F)| \colon F \in \mathcal{F}_{d,r}\} \\
&\overset{(4.10)}{=} |\mathbb{X}| - \max\{\deg(S/(I,F))|\, F \in \mathcal{F}_{d,r}\} \\
&= \deg(S/I) - \max\{\deg(S/(I,F))|\, F \in \mathcal{F}_{d,r}\} \\
&= \delta_I(d,r), \text{ and}
\end{aligned}$$

$$\begin{aligned}
\delta_{\mathbb{X}}(d,r) &\overset{(4.16)}{=} \min\{|\mathbb{X} \setminus V_{\mathbb{X}}(F)| \colon F \in \mathcal{F}_{d,r}\} \\
&\overset{(4.8)}{=} \min\{\deg(S/(I\colon (F)))|\, F \in \mathcal{F}_{d,r}\} \\
&= \vartheta_I(d,r).
\end{aligned}$$

In these equalities we used the fact that $\deg(S/I(\mathbb{X})) = |\mathbb{X}|$. As $H_I(d) = |\mathbb{X}|$ for $d \geq \operatorname{reg}(S/I)$, using the generalized Singleton bound for the generalized Hamming distance and the fact that the weight hierarchy is an increasing sequence we obtain that $\delta_{\mathbb{X}}(d,r) = r$ for $d \geq \operatorname{reg}(S/I(\mathbb{X}))$ (see **[Wei91**, Theorem 1, Corollary 1]). ♠

REMARK 4.19. $r \leq \delta_{\mathbb{X}}(d,r) \leq |\mathbb{X}|$ for $d \geq 1$ and $1 \leq r \leq H_{I(\mathbb{X})}(d)$. This follows from the fact that the weight hierarchy is an increasing sequence (see **[Wei91**, Theorem 1]).

LEMMA 4.20. *Let $\prec$ be a monomial order, let $I \subset S$ be an ideal, let $F = \{f_1, \ldots, f_r\}$ be a set of polynomial of S of positive degree, and let $\operatorname{in}_\prec(F) = \{\operatorname{in}_\prec(f_1), \ldots, \operatorname{in}_\prec(f_r)\}$ be the set of initial terms of F. If $(\operatorname{in}_\prec(I)\colon (\operatorname{in}_\prec(F))) = \operatorname{in}_\prec(I)$, then $(I\colon (F)) = I$.*

PROOF. Let g be a polynomial of $(I\colon (F))$, that is, $gf_i \in I$ for $i = 1, \ldots, r$. It suffices to show that $g \in I$. Pick a Gröbner basis $g_1, \ldots, g_n$ of I. Then, by the division algorithm **[CLO07**, Theorem 3, p. 63], we can write $g = \sum_{i=1}^n h_i g_i + h$, where $h = 0$ or h is a finite sum of monomials not in $\operatorname{in}_\prec(I) = (\operatorname{in}_\prec(g_1), \ldots, \operatorname{in}_\prec(g_n))$. We need only show that $h = 0$. If $h \neq 0$, then hf_i is in I and $\operatorname{in}_\prec(h)\operatorname{in}_\prec(f_i)$ is in the ideal $\operatorname{in}_\prec(I)$ for $i = 1, \ldots, r$. Hence

$\text{in}_\prec(h)$ is in $(\text{in}_\prec(I)\colon(\text{in}_\prec(F)))$. Therefore, by hypothesis, $\text{in}_\prec(h)$ is in the ideal $\text{in}_\prec(I)$, a contradiction. ♠

Given integers $d, r \geq 1$, we define $\mathcal{M}_{\prec,d,r}$ to be the set of all subsets M of $\Delta_\prec(I)_d = \Delta_\prec(I) \cap S_d$ with r distinct elements such that $(\text{in}_\prec(I)\colon(M)) \neq \text{in}_\prec(I)$.

DEFINITION 4.21. The *generalized footprint function* of I, denoted fp_I, is the function $\text{fp}_I\colon \mathbb{N}_+ \times \mathbb{N}_+ \to \mathbb{Z}$ given by

$$\begin{cases} \deg(S/I) - \max\{\deg(S/(\text{in}_\prec(I), M)) \mid M \in \mathcal{M}_{\prec,d,r}\} & \text{if } \mathcal{M}_{\prec,d,r} \neq \emptyset, \\ \deg(S/I) & \text{if } \mathcal{M}_{\prec,d,r} = \emptyset. \end{cases}$$

Let $\mathcal{F}_{\prec,d,r}$ be the set consisting of all subsets $F = \{f_1, \ldots, f_r\}$ of S_d such that $(I\colon(F)) \neq I$, f_i is a standard polynomial for all i, $\overline{f}_1, \ldots, \overline{f}_r$ are linearly independent over the field K, and $\text{in}_\prec(f_1), \ldots, \text{in}_\prec(f_r)$ are distinct monomials.

PROPOSITION 4.22. *The generalized minimum distance function of I is given by*

$$\delta_I(d,r) = \begin{cases} \deg(S/I) - \max\{\deg(S/(I,F)) \mid F \in \mathcal{F}_{\prec,d,r}\} & \text{if } \mathcal{F}_{\prec,d,r} \neq \emptyset, \\ \deg(S/I) & \text{if } \mathcal{F}_{\prec,d,r} = \emptyset. \end{cases}$$

PROOF. Take $F = \{f_1, \ldots, f_r\}$ in $\mathcal{F}_{d,r}$. By the division algorithm any f_i can be written as $f_i = p_i + h_i$, where p_i is in I_d and h_i is a K-linear combination of standard monomials of degree d. Setting $H = \{h_1, \ldots, h_r\}$, notice that $(I\colon(F)) = (I\colon(H))$, $(I,F) = (I,H)$, $\overline{f}_i = \overline{h}_i$ for $i = 1, \ldots, r$. Thus $H \in \mathcal{F}_{d,r}$, that is, we may assume that $f_1, \ldots, f_r$ are standard polynomials. Setting $KF = Kf_1 + \cdots + Kf_r$, we claim that there is a set $G = \{g_1, \ldots, g_r\}$ consisting of homogeneous standard polynomials of S/I of degree d such that $KF = KG$, $\text{in}_\prec(g_1), \ldots, \text{in}_\prec(g_r)$ distinct monomials, and $\text{in}_\prec(f_i) \succeq \text{in}_\prec(g_i)$ for all i. We proceed by induction on r. The case $r = 1$ is clear. Assume that $r > 1$. Permuting the f_i's if necessary we may assume that $\text{in}_\prec(f_1) \succeq \cdots \succeq \text{in}_\prec(f_r)$. If $\text{in}_\prec(f_1) \succ \text{in}_\prec(f_2)$, the claim follows applying the induction hypothesis to $f_2, \ldots, f_r$. If $\text{in}_\prec(f_1) = \text{in}_\prec(f_2)$, there is $k \geq 2$ such that $\text{in}_\prec(f_1) = \text{in}_\prec(f_i)$ for $i \leq k$ and $\text{in}_\prec(f_1) \succ \text{in}_\prec(f_i)$ for $i > k$. We set $h_i = f_1 - f_i$ for $i = 2, \ldots, k$ and $h_i = f_i$ for $i = k+1, \ldots, r$. Notice that $\text{in}_\prec(f_1) \succ h_i$ for $i \geq 2$ and that $h_2, \ldots, h_r$ are standard monomials of degree d which are linearly independent over K. Hence the claim follows applying the induction hypothesis to $H = \{h_2, \ldots, h_r\}$. The required expression for $\delta_I(d,r)$ follows readily using Theorem 4.18. ♠

THEOREM 4.23. *Let K be a field, let $\mathbb{X}$ be a finite subset of $\mathbb{P}^{s-1}$, and let $\prec$ be a monomial order. If $|\mathbb{X}| \geq 2$ and $\delta_{\mathbb{X}}(d,r)$ is the r-th generalized Hamming weight of $C_{\mathbb{X}}(d)$, then*

$$\text{fp}_{I(\mathbb{X})}(d,r) \leq \delta_{\mathbb{X}}(d,r) \text{ for } d \geq 1 \text{ and } 1 \leq r \leq H_{I(\mathbb{X})}(d).$$

PROOF. This follows from Theorem 4.18, Lemma 4.20, and Proposition 4.22. ♠

4.4. An integer inequality

For $a : a_1, \ldots, a_m$ and $b : b_1, \ldots, b_m$ sequences in $\mathbb{Z}^+ = \{1, 2, \ldots\}$ we define

$$\pi(a, b) := \prod_{i=1}^{m} a_i + \prod_{i=1}^{m} b_i - \prod_{i=1}^{m} \min(a_i, b_i).$$

Fix integers $d \geq 1$ and $1 \leq e_1 \leq \cdots \leq e_m$. Let $1 \leq a_i, b_i \leq e_i$, for $i = 1, \ldots, m$, be integers. Suppose $d = \sum a = \sum b$ and $a \neq b$. In this section we will prove the following inequality:

$$\pi(a, b) \geq \left(\sum_{i=1}^{m} a_i - \sum_{i=k+1}^{m} e_i - (k-2) \right) e_{k+1} \cdots e_m - e_{k+2} \cdots e_m$$

for $k = 1, \ldots, m-1$, where $e_{k+2} \cdots e_m = 1$ when $k = m-1$ (Proposition 4.28).

LEMMA 4.24. *Let $a_1, a_2, b_1, b_2 \in \mathbb{Z}^+$. Set $a_1' = \min(a_1, a_2)$ and $a_2' = \max(a_1, a_2)$. Then*

$$\min(a_1, b_1) \min(a_2, b_2) \leq \min(a_1', b_1') \min(a_2', b_2').$$

PROOF. It is an easy case-by-case verification of 24 possible cases. ♠

LEMMA 4.25. *Let $a : a_1, \ldots, a_m$ and $b : b_1, \ldots, b_m$ be sequences in $\mathbb{Z}^+$. Suppose:*

(i) $r < s$, $a_r > a_s$. *Set* $a_r' = a_s$, $a_s' = a_r$, $a_i' = a_i$ *for* $i \neq r, s$; *and* $b_r' = \min(b_r, b_s)$, $b_s' = \max(b_r, b_s)$, $b_i' = b_i$ *for* $i \neq r, s$. *Then* $\pi(a, b) \geq \pi(a', b')$.

(ii) $r < s$, $b_r = a_r \leq a_s < b_s$. *Set* $a_r' = a_r - 1$, $a_s' = a_s + 1$, $a_i' = a_i$ *for* $i \neq r, s$. *Then* $\pi(a, b) \geq \pi(a', b)$.

(iii) $r < s$, $b_r < a_r \leq a_s$. *Set* $a_r' = a_r - 1$, $a_s' = a_s + 1$, $a_i' = a_i$ *for* $i \neq r, s$. *Then* $\pi(a, b) \geq \pi(a', b)$.

(iv) $r < s$, $a_r < a_s$, $b_r = a_s, b_s = a_r$, $b_i = a_i$ *for* $i \neq r, s$, $h := a_s - a_r \geq 2$. *Set* $b_r' = a_r + 1$, $b_s' = a_s - 1$, $b_i' = a_i$ *for* $i \neq r, s$. *Then* $\pi(a, b) \geq \pi(a, b')$.

PROOF.

$$\begin{aligned}(i)\ \ \pi(a, b) - \pi(a', b') &= \prod a_i + \prod b_i - \prod a_i' - \prod b_i' + \prod \min(a_i', b_i') - \prod \min(a_i, b_i) \\ &= \left(\min(a_r', b_r') \min(a_s', b_s') - \min(a_r, b_r) \min(a_s, b_s)\right) \prod_{i \neq r,s} \min(a_i, b_i) \geq 0. \ \ (\textit{Lemma } 4.24)\end{aligned}$$

$$
\begin{aligned}
(ii)\ \ \pi(a,b)-\pi(a',b) &= \prod a_i - \prod a_i' + \prod \min(a_i', b_i) - \prod \min(a_i, b_i) \\
&= (a_r a_s - (a_r-1)(a_s+1)) \prod_{i\neq r,s} a_i \\
&\quad + (\min(a_r', b_r)\min(a_s', b_s) - \min(a_r, b_r)\min(a_s, b_s)) \prod_{i\neq r,s} \min(a_i, b_i) \\
&= (a_s - a_r + 1) \prod_{i\neq r,s} a_i + ((a_r-1)(a_s+1) - a_r a_s) \prod_{i\neq r,s} \min(a_i, b_i) \\
&= (a_s - a_r + 1) \left(\prod_{i\neq r,s} a_i - \prod_{i\neq r,s} \min(a_i, b_i) \right) \geq 0.
\end{aligned}
$$

$$
\begin{aligned}
(iii)\ \ \pi(a,b)-\pi(a',b) &= \prod a_i - \prod a_i' + \prod \min(a_i', b_i) - \prod \min(a_i, b_i) \\
&= (a_r a_s - (a_r-1)(a_s+1)) \prod_{i\neq r,s} a_i \\
&\quad + (\min(a_r', b_r)\min(a_s', b_s) - \min(a_r, b_r)\min(a_s, b_s)) \prod_{i\neq r,s} \min(a_i, b_i) \\
&= (a_s - a_r + 1) \prod_{i\neq r,s} a_i + b_r(\min(a_s+1, b_s) - \min(a_s, b_s)) \prod_{i\neq r,s} \min(a_i, b_i) \geq 0.
\end{aligned}
$$

For the last inequality note that $\min(a_s+1, b_s) - \min(a_s, b_s) = 0$ or 1.

$$
\begin{aligned}
(iv)\ \ \pi(a,b)-\pi(a,b') &= \prod b_i - \prod b_i' + \prod \min(a_i, b_i') - \prod \min(a_i, b_i) \\
&= (a_r a_s - (a_r+1)(a_s-1) + a_r(a_s-1) - a_r^2) \prod_{i\neq r,s} a_i \\
&= (a_r-1)(h-1) \prod_{i\neq r,s} a_i \geq 0.
\end{aligned}
$$

♠

LEMMA 4.26. *If $a_1, \ldots, a_r$ are positive integers, then*

$$a_1 \cdots a_r \geq (a_1 + \cdots + a_r) - (r-1).$$

PROOF. It follows by induction on r. ♠

LEMMA 4.27. *Let $1 \leq e_1 \leq \cdots \leq e_m$ and $1 \leq a_i, b_i \leq e_i$, for $i = 1, \ldots, m$ be integers. Suppose $a_i = b_i = 1$ for $i < r$, $a_i = b_i = e_i$ for $i > r+1 := s$, $1 \leq a_i, b_i \leq e_i$ for $i = r, s$, with $a_r + a_s = b_r + b_s$ and $(a_r, a_s) \neq (b_r, b_s)$. If $b_r \leq a_s$ and $b_s = a_s - 1$, then*

$$\pi(a,b) \geq \left(\sum_{i=1}^{m} a_i - \sum_{i=k+1}^{m} e_i - (k-2) \right) e_{k+1} \cdots e_m - e_{k+2} \cdots e_m \tag{4.4.1}$$

for $i = 1, \ldots, m-1$, where $e_{k+2} \cdots e_m = 1$ when $k = m-1$.

PROOF. Set $\sigma = \sum_{i=1}^{m} a_i - \sum_{i=k+1}^{m} e_i - (k-2)$. Since $b_s(b_r - a_r) = a_s - 1$, one has the equality

$$\pi(a,b) = (a_r a_s + b_r b_s - a_r b_s) \prod_{i=r+2}^{m} e_i = (a_r a_s + a_s - 1) \prod_{i=r+2}^{m} e_i. \tag{4.4.2}$$

Case $k+1 < r$: The integer σ can be rewritten as

$$\sigma = k + (1 - e_{k+1}) + \cdots + (1 - e_{r-1}) + (a_r - e_r) + (a_s - e_s) - (k-2).$$

Since $a_r < b_r \leq e_r$, it holds that $a_r - e_r \leq -1$, and hence $\sigma \leq 1$. If $\sigma \leq 0$, Eq. (4.4.1) trivially follows (because the left hand side is positive and the right hand side would be negative). So we may assume $\sigma = 1$. This assumption implies that $e_{k+1} = 1$ because $a_r < b_r \leq e_r$. Then the right hand side of Eq. (4.4.1) is

$$(\sigma) e_{k+1} \cdots e_m - e_{k+2} \cdots e_m = (e_{k+1} - 1) e_{k+2} \cdots e_r = 0.$$

Case $k+1 = r$: The integer σ can be rewritten as

$$\sigma = k + (a_r - e_r) + (a_s - e_s) - (k-2).$$

By the same reason as above, we may assume $\sigma = 1$. This assumption implies $a_r = e_r - 1$ and $a_s = e_s$. Then, by Eq. (4.4.2), we obtain that Eq. (4.4.1) is equivalent to

$$(e_r e_s - 1) \prod_{i=r+2}^{m} e_i \geq (\sigma)\, e_r \cdots e_m - e_{r+1} \cdots e_m,$$

which reduces to $e_r e_s - 1 \geq (1)\, e_r e_s - e_s$, or equivalently, $e_s \geq 1$.

Case $k+1 = r+1$: We can rewrite σ as

$$\sigma = (k-1) + a_r + (a_s - e_s) - (k-2) = a_r + (a_s - e_s) + 1.$$

Then, using Eq. (4.4.2), we obtain that Eq. (4.4.1) is equivalent to

$$(a_r a_s + a_s - 1) \prod_{i=r+2}^{m} e_i \geq (\sigma)\, e_{r+1} \cdots e_m - e_{r+2} \cdots e_m,$$

which reduces to $a_r a_s + a_s \geq (a_r + a_s - e_s + 1)\, e_s$, or equivalently,

$$(e_s - a_s)(e_s - a_r - 1) \geq 0.$$

Case $k+1 > r+1$: One can rewrite σ as

$$\sigma = (r-1) + a_r + \cdots + a_k - (k-2).$$

Then, using Eq. (4.4.2), we obtain that Eq. (4.4.1) reduces to

$$(a_r a_s + a_s - 1)e_{r+2} \cdots e_{k+1} \geq (\sigma)\, e_{k+1} - 1.$$

But, as $a_s \geq 2$, using Lemma 4.26, we get

$$\begin{aligned}(a_r a_s + a_s - 1)e_{r+2} \cdots e_k &\geq (a_r a_s + a_s - 1) + e_{r+2} + \cdots + e_k - (k - r - 1) \\ &\geq (a_r + a_s) + a_{r+2} + \cdots + a_k + r - k + 1 = \sigma.\end{aligned}$$

So, multiplying by e_{k+1}, the required inequality follows. ♠

PROPOSITION 4.28. *Let $d \geq 1$ and $1 \leq e_1 \leq \cdots \leq e_m$ be integers. Suppose $1 \leq a_i \leq e_i$ and $1 \leq b_i \leq e_i$, for $i = 1, \ldots, m$, are integers such that $d = \sum a = \sum b$ and $a \neq b$. Then*

$$\pi(a, b) \geq \left(\sum_{i=1}^{m} a_i - \sum_{i=k+1}^{m} e_i - (k-2) \right) e_{k+1} \cdots e_m - e_{k+2} \cdots e_m$$

for $k = 1, \ldots, m-1$, where $e_{k+2} \cdots e_m = 1$ when $k = m - 1$.

PROOF. Apply to (a, b) any of the four "operations" described in Lemma 4.25, and let (a', b') be the new obtained pair. These operations should be applied in such a way that $1 \leq a'_i, b'_i \leq e_i$ for $i = 1, \ldots, m$ and $a' \neq b'$; this is called a *valid* operation. One can order the set of all pairs (a, b) that satisfy the hypothesis of the proposition using the GRevLex order defined by $(a, b) \succ (a', b')$ if and only if the last non-zero entry of $(a, b) - (a', b')$ is negative. Note that by construction $d = \sum a'_i = \sum b'_i = \sum a_i$. Repeat this step as many times as possible (which is a finite number because the result (a', b') of any valid operation applied to (a, b) satisfies $(a, b) \succ (a', b')$). Permitting an abuse of notation, let a and b be the resulting sequences at the end of that process. We will show that these a and b satisfy the hypothesis of Lemma 4.27.

Set $r = \min(i : a_i \neq b_i)$. By symmetry we may assume $a_r < b_r$. Pick the first $s > r$ such that $a_s > b_s$ (the case $a_r > b_r$ and $a_s < b_s$ can be shown similarly).

Claim (a): For $p < r$, $a_p = 1$. Assume $a_p > 1$. If $a_p > a_r$, we can apply Lemma $4.25(i)[p, r]$, which is assumed not possible; (this last notation means that we are applying Lemma $4.25(i)$ with the indexes p and r). Otherwise apply Lemma $4.25(ii)[p, r]$. So $a_p = b_p = 1$ for $p < r$.

Claim (b): $s = r + 1$. Assume $r < p < s$. For a contradiction it suffices to show that we can apply a valid operation to a, b. By the choice of s, $a_p \leq b_p$. Assume that $b_r > b_p$, we apply Lemma $4.25(i)[r, p]$. If $b_p > b_s$, apply Lemma $4.25(i)[p, s]$. Hence $b_r \leq b_p \leq b_s$. Note that $b_p \geq 2$ since $a_r < b_r \leq b_p$. If $a_p = b_p$, we can apply Lemma $4.25(ii)[p, s]$. If $a_p < b_p$, we can apply Lemma $4.25(iii)[p, s]$ because $a_p < b_p \leq b_s < a_s$.

Claim (c): For $p > s$, $a_p = b_p = e_p$. If $b_p < a_p$, applying Claim (b) to r and p we get a contradiction. Thus we may assume $b_p \geq a_p$. It suffices to show that $a_p = e_p$. If $a_s > a_p$, then by Lemma 4.25$(i)[s,p]$ one can apply a valid operation to a, b, a contradiction. Thus $a_s \leq a_p$. If $a_p < e_p$, then $b_s < a_s \leq a_p < e_p$, and by Lemma 4.25$(iii)[s,p]$ we can apply a valid operation to a, b, a contradiction. Hence $a_p = e_p$.

Claim (d): $b_r \leq a_s$ and $b_s = a_s - 1$. By the previous claims one has the equalities $s = r + 1$ and $a_r + a_s = b_r + b_s$. If $a_s < b_r$. Then $b_s < a_s < b_r$, and by Lemma 4.25$(i)[r,s]$ we can apply a valid operation to a, b, a contradiction. Hence $a_s \geq b_r$. Suppose $a_s = b_r$, then $a_r = b_s$. If $a_s - a_r \geq 2$, by Lemma 4.25$(iv)[r,s]$ we apply a valid operation to a, b, a contradiction. Hence, $a_s - b_s = a_s - a_r = 1$. Assume $a_s > b_r$. If $b_r > b_s$, then $a_s > b_r > b_s$, and we can use Lemma 4.25$(i)[r,s]$ to apply a valid operation to a, b, a contradiction. Hence $b_r \leq b_s$. In the case that $a_s - b_s = b_r - a_r \geq 2$, then $a_r < b_r \leq b_s < a_s$, and by Lemma 4.25$(iii)[r,s]$ we can apply a valid operation to a, b, a contradiction. So, in this other case, also $a_s - b_s = 1$. In conclusion, we have that $b_r \leq a_s$ and $b_s = a_s - 1$, as claimed.

From Claims (a)–(d), we obtain that a, b satisfy the hypothesis of Lemma 4.27. Hence the required inequality follows from Lemmas 4.25 and 4.27. ♠

LEMMA 4.29. *Let* $1 \leq d_1 \leq \cdots \leq d_m$, $0 \leq \alpha_i, \beta_i \leq d_i - 1$ *for* $i = 1, \ldots, m$, $m \geq 2$, *be integers such that* $\sum_{i=1}^m \alpha_i = \sum_{i=1}^m \beta_i$ *and* $(\alpha_1, \ldots, \alpha_m) \neq (\beta_1, \ldots, \beta_m)$. *Then*

$$\prod_{i=1}^{m}(d_i - \alpha_i) + \prod_{i=1}^{m}(d_i - \beta_i) - \prod_{i=1}^{m}\min\{d_i - \alpha_i, d_i - \beta_i\} \geq \left(\sum_{i=1}^{k+1}(d_i - \alpha_i) - (k-1) - \sum_{i=k+2}^{m}\alpha_i\right) d_{k+2}\cdots d_m - d_{k+3}\cdots d_m \tag{4.4.3}$$

for $k = 0, \ldots, m-2$, *where* $d_{k+3}\cdots d_m = 1$ *if* $k = m-2$.

PROOF. Making the substitutions $k = k - 1$, $d_i - \alpha_i = a_i$, $d_i - \beta_i = b_i$, and $d_i = e_i$, the inequality follows at once from Proposition 4.28. ♠

4.5. Second generalized Hamming weight

Let $A_1, \ldots, A_{s-1}$ be subsets of $\mathbb{F}_q$ and let $\mathbb{X}$ be the projective cartesian set

$$\mathbb{X} := [A_1 \times \cdots \times A_{s-1} \times \{1\}] \subset \mathbb{P}^{s-1},$$

where $d_i = |A_i|$ for all $i = 1, \ldots, s-1$ and $2 \leq d_1 \leq \cdots \leq d_{s-1}$.
The Reed–Muller-type code $C_{\mathbb{X}}(d)$ is called an *affine cartesian code* **[LRMV14]**. If $\mathbb{X}^* =$

$A_1 \times \cdots \times A_{s-1}$, then $C_{\mathbb{X}}(d) = C_{\mathbb{X}^*}(d)$ (see **[LRMV14]**). We suppose that $d = \sum_{i=1}^{k}(d_i - 1) + \ell$, where $0 \leq k \leq s-2$ and $1 \leq \ell \leq d_{k+1} - 1$. To prove the inequality "$\leq$" in Theorem 4.32 we need the following Lemma.

LEMMA 4.30. *We can find two linearly independent polynomials F and $G \in S_{\leq d}$ such that $|V_{\mathbb{X}^*}(F) \cap V_{\mathbb{X}^*}(G)|$ is given by*

$$\begin{cases} d_1 \cdots d_{s-1} - (d_{k+1} - \ell + 1)d_{k+2} \cdots d_{s-1} + d_{k+3} \cdots d_{s-1} & \text{if } k < s-3, \\ d_1 \cdots d_{s-1} - (d_{k+1} - \ell + 1)d_{k+2} \cdots d_{s-1} + 1 & \text{if } k = s-3, \\ d_1 \cdots d_{s-1} - d_{s-1} + \ell - 1 & \text{if } k = s-2. \end{cases}$$

PROOF. Case (I): $k \leq s-3$. Similarly to **[LRMV14]** we take $A_i = \{\beta_{i,1}, \ldots, \beta_{i,d_i}\}$, for $i = 1, \ldots, s-1$. Also, for $i = 1, \ldots, k$, let

$$f_i := (\beta_{i,1} - t_i)(\beta_{i,2} - t_i) \cdots (\beta_{i,d_{i-1}} - t_i),$$
$$g := (\beta_{k+1,1} - t_{k+1})(\beta_{k+1,2} - t_{k+1}) \cdots (\beta_{k+1,\ell-1} - t_{k+1}).$$

Setting $h_1 := \beta_{k+1,\ell} - t_{k+1}$ and $h_2 := \beta_{k+2,\ell} - t_{k+2}$. Set $F := f_1 \cdots f_k \cdot g \cdot h_1$ and $G := f_1 \cdots f_k \cdot g \cdot h_2$. Notice that $\deg F = \deg G = \sum_{i=1}^{k}(d_i - 1) + \ell = d$ and that they are linearly independent over $\mathbb{F}_q$. Let

$$V_1 := (A_1 \times \cdots \times A_{s-1}) \setminus (V_{\mathbb{X}^*}(F) \cap V_{\mathbb{X}^*}(G)),$$
$$V_2 := \{\beta_{1,d_1}\} \times \cdots \times \{\beta_{k,d_k}\} \times \{\beta_{k+1,i}\}_{i=\ell}^{d_{k+1}} \times A_{k+2} \times \cdots \times A_{s-1}.$$

It is easy to see that $V_1 \subset V_2$ and $(V_2 \setminus V_1) \cap (V_{\mathbb{X}^*}(F) \cap V_{\mathbb{X}^*}(G)) = V_3$, where V_3 is given by

$$\begin{cases} \{\beta_{1,d_1}\} \times \cdots \times \{\beta_{k,d_k}\} \times \{\beta_{k+1,\ell}\} \times \{\beta_{k+2,\ell}\} \times A_{k+3} \times \cdots \times A_{s-1} & \text{if } k < s-3, \\ \{\beta_{1,d_1}\} \times \cdots \times \{\beta_{k,d_k}\} \times \{\beta_{k+1,\ell}\} \times \{\beta_{k+2,\ell}\} & \text{if } k = s-3. \end{cases}$$

Therefore

$$|V_1| = |V_2| - |V_3| = \begin{cases} (d_{k+1} - \ell + 1)d_{k+2} \cdots d_{s-1} - d_{k+3} \cdots d_{s-1} & \text{if } k < s-3, \\ (d_{k+1} - \ell + 1)d_{k+2} \cdots d_{s-1} - 1 & \text{if } k = s-3, \end{cases}$$

and the claim follows because $|V_{\mathbb{X}^*}(F) \cap V_{\mathbb{X}^*}(G)| = d_1 \cdots d_{s-1} - |V_1|$.

Case (II): $k = s-2$. As $\ell \leq d_{k+1} - 1$ then $\ell + 1 \leq d_{k+1}$. We define h_3 as $\beta_{k+1,\ell+1} - t_{k+1}$, and F, f_i, g, h_1 as in Case (I). Let $G' := f_1 \cdots f_k \cdot g \cdot h_3$. If

$$V_1' := (A_1 \times \cdots \times A_{s-1}) \setminus (V_{\mathbb{X}^*}(F) \cap V_{\mathbb{X}^*}(G')),$$
$$V_2' := \{\beta_{1,d_1}\} \times \cdots \times \{\beta_{k,d_k}\} \times \{\beta_{k+1,i}\}_{i=\ell}^{d_{k+1}},$$

then (because h_1 and h_3 do not have common zeros) $V_1' = V_2'$ and thus

$$|V_1'| = d_{k+1} - \ell + 1 = d_{s-1} - \ell + 1.$$

The result follows because $|V_{\mathbb{X}^*}(F) \cap V_{\mathbb{X}^*}(G')| = d_1 \cdots d_{s-1} - |V_1'|$. ♠

LEMMA 4.31. **[MBPV16**, Lemma 3.3] *Let $L \subset S$ be the ideal $(t_1^{d_1}, \ldots, t_{s-1}^{d_{s-1}})$, where $d_1, \ldots, d_{s-1}$ are in $\mathbb{N}_+$. If $t^a = t_1^{a_1} \cdots t_s^{a_s}$, $a_j \geq 1$ for some $1 \leq j \leq s-1$, and $a_i \leq d_i - 1$ for $i \leq s-1$, then*

$$\deg(S/(L, t^a)) = \deg(S/(L, t_1^{a_1} \cdots t_{s-1}^{a_{s-1}})) = d_1 \cdots d_{s-1} - \prod_{i=1}^{s-1}(d_i - a_i).$$

We come to one of our applications to coding theory.

THEOREM 4.32. *Let A_i, $i = 1, \ldots, s-1$, be subsets of $\mathbb{F}_q$ and let $\mathbb{X} \subset \mathbb{P}^{s-1}$ be the projective cartesian set given by $\mathbb{X} = [A_1 \times \cdots \times A_{s-1} \times \{1\}]$. If $d_i = |A_i|$ for $i = 1, \ldots, s-1$ and $2 \leq d_1 \leq \cdots \leq d_{s-1}$, then*

$$\delta_{\mathbb{X}}(d, 2) = \begin{cases} (d_{k+1} - \ell + 1)\, d_{k+2} \cdots d_{s-1} - d_{k+3} \cdots d_{s-1} & \text{if } k < s-3, \\ (d_{k+1} - \ell + 1)\, d_{k+2} \cdots d_{s-1} - 1 & \text{if } k = s-3, \\ d_{s-1} - \ell + 1 & \text{if } k = s-2, \\ 2 & \text{if } d \geq \sum_{i=1}^{s-1} (d_i - 1), \end{cases}$$

where $0 \leq k \leq s-2$, $d = \sum_{i=1}^{k} (d_i - 1) + \ell$ and $1 \leq \ell \leq d_{k+1} - 1$.

PROOF. We set $n = s-1$, $I = I(\mathbb{X})$, and $L = (t_1^{d_1}, \ldots, t_n^{d_n})$. By **[Wei91**, Theorem 1, Corollary 1], we get $\delta_{\mathbb{X}}(d, 2) = 2$ for $d \geq \sum_{i=1}^{s-1}(d_i - 1)$. Thus we may assume $d < \sum_{i=1}^{s-1}(d_i - 1)$. First we show the inequality "$\geq$". Let $\prec$ be a graded monomial order with $t_1 \succ \cdots \succ t_s$. The initial ideal $\mathrm{in}_{\prec}(I)$ of I is equal to $L = (t_1^{d_1}, \ldots, t_n^{d_n})$; see **[LRMV14]**. Let $F = \{t^a, t^b\}$ be an element of $\mathcal{M}_{\prec,d,2}$, that is, $t^a = t_1^{a_1} \cdots t_s^{a_s}$, $t^b = t_1^{b_1} \cdots t_s^{b_s}$, $d = \sum_{i=1}^{s} a_i = \sum_{i=1}^{s} b_i$, $a \neq b$, $a_i \leq d_i - 1$ and $b_i \leq d_i - 1$ for $i = 1, \ldots, n$, and $(L\colon (F)) \neq L$. In particular, from the last condition it follows readily that $a_i \neq 0$ and $b_j \neq 0$ for some $1 \leq i, j \leq n$. There are exact sequences of graded S-modules

$$0 \to (S/((L, t^a)\colon t^b))[-|b|] \xrightarrow{t^b} S/(L, t^a) \to S/(L, t^a, t^b) \to 0,$$
$$0 \to (S/((L, t^b)\colon t^a))[-|a|] \xrightarrow{t^a} S/(L, t^b) \to S/(L, t^a, t^b) \to 0,$$

where $|a| = \sum_{i=1}^{s} a_i$. From the equalities

$$((L, t^a)\colon t^b) = (L\colon t^b) + (t^a\colon t^b) = (t_1^{d_1 - b_1}, \ldots, t_n^{d_n - b_n}, \textstyle\prod_{i=1}^{s} t_i^{\max\{a_i, b_i\} - b_i}),$$
$$((L, t^b)\colon t^a) = (L\colon t^a) + (t^b\colon t^a) = (t_1^{d_1 - a_1}, \ldots, t_n^{d_n - a_n}, \textstyle\prod_{i=1}^{s} t_i^{\max\{a_i, b_i\} - a_i}),$$

it follows that either $((L, t^a) : t^b)$ or $((L, t^b) : t^a)$ is contained in $(t_1, \ldots, t_n)$. Hence at least one of these ideals has height n. Therefore, setting

$$P(a,b) = \prod_{i=1}^{n}(d_i - a_i) + \prod_{i=1}^{n}(d_i - b_i) - \prod_{i=1}^{n}\min\{d_i - a_i, d_i - b_i\},$$

and using Lemma 4.31 it is not hard to see that the degree of $S/(L, t^a, t^b)$ is

$$\deg(S/(L, t^a, t^b)) = \prod_{i=1}^{n} d_i - P(a,b),$$

and the second generalized footprint function of I is

$$\mathrm{fp}_I(d,2) = \min\left\{P(a,b) | \, \{t^a, t^b\} \in \mathcal{M}_{\prec,d,2}\right\}. \tag{4.5.1}$$

Making the substitution $-\ell = \sum_{i=1}^{k}(d_i - 1) - \sum_{i=1}^{s} a_i$ and using the fact that $\mathrm{fp}_{I(\mathbb{X})}(d,r)$ is less than or equal to $\delta_{\mathbb{X}}(d,r)$ (see Theorem 4.23) it suffices to show the inequalities

$$P(a,b) \geq \left(\sum_{i=1}^{k+1}(d_i - a_i) - (k-1) - a_s - \sum_{i=k+2}^{n} a_i\right) d_{k+2}\cdots d_n - d_{k+3}\cdots d_n, \tag{4.5.2}$$

for $\{t^a, t^b\} \in \mathcal{M}_{\prec,d,2}$ if $0 \leq k \leq s-3$, where $d_{k+3}\cdots d_n = 1$ if $k = s-3$, and

$$P(a,b) \geq \sum_{i=1}^{s-1}(d_i - a_i) - (s-3) - a_s, \tag{4.5.3}$$

for $\{t^a, t^b\} \in \mathcal{M}_{\prec,d,2}$ if $k = s-2$. As $(a_1, \ldots, a_n)$ is not equal to $(b_1, \ldots, b_n)$, one has that either $\prod_{i=1}^{n} d_i - \prod_{i=1}^{n}(d_i - a_i) \geq 1$ or $\prod_{i=1}^{n} d_i - \prod_{i=1}^{n}(d_i - b_i) \geq 1$. If $a_s \geq 1$ or $b_s \geq 1$ (resp. $a_s = b_s = 0$), the inequality of Eq. (4.5.2) follows at once from [**MBPV17**, Proposition 5.7] (resp. Lemma 4.29). If $a_s \geq 1$ or $b_s \geq 1$ (resp. $a_s = b_s = 0$), the inequality of Eq. (4.5.3) follows at once from [**MBPV17**, Proposition 5.7] (resp. Lemma 4.26(a)). This completes the proof of the inequality "$\geq$".

The inequality "$\leq$" follows directly from Lemma 4.30. ♠

Another of our applications to coding theory is the following purely combinatorial formula for the second generalized Hamming weight of an affine cartesian code which is quite different from the corresponding formula of [**BD17**, Theorem 5.4].

THEOREM 4.33. *Let $\mathcal{P}_d$ be the set of all pairs (a,b), a, b in $\mathbb{N}^s$, $a = (a_1, \ldots, a_s)$, $b = (b_1, \ldots, b_s)$, such that $a \neq b$, $d = \sum_{i=1}^{s} a_i = \sum_{i=1}^{s} b_i$, $1 \leq a_i, b_i \leq d_i - 1$ for $i = 1, \ldots, n$, $n := s-1$, $a_i \neq 0$ and $b_j \neq 0$ for some $1 \leq i, j \leq n$. If we consider $\mathbb{X} = [A_1 \times \cdots \times A_n \times \{1\}] \subset \mathbb{P}^n$,*

with $A_i \subset \mathbb{F}_q$, $d_i = |A_i|$, *and* $2 \leq d_1 \leq \cdots \leq d_n$, *then*

$$\mathrm{fp}_{I(\mathbb{X})}(d,2) = \delta_{\mathbb{X}}(d,2) = \min\{P(a,b)|\,(a,b) \in \mathcal{P}_d\} \;\; \textit{for} \;\; d \leq \textstyle\sum_{i=1}^{n}(d_i-1),$$

where $P(a,b) = \prod_{i=1}^{n}(d_i - a_i) + \prod_{i=1}^{n}(d_i - b_i) - \prod_{i=1}^{n}\min\{d_i - a_i, d_i - b_i\}$.

PROOF. Let $\psi(d)$ be the formula for $\delta_{\mathbb{X}}(d,2)$ given in Theorem 4.32. Then using Eqs. (4.5.2) and Eqs. (4.5.3) one has $\psi(d) \leq \mathrm{fp}_{I(\mathbb{X})}(d,2)$. By Theorem 4.23 one has $\mathrm{fp}_{I(\mathbb{X})}(d,r) \leq \delta_{\mathbb{X}}(d,r)$, and by Lemma 4.30 one has $\delta_{\mathbb{X}}(d,r) \leq \psi(d)$. Therefore

$$\psi(d) \leq \mathrm{fp}_{I(\mathbb{X})}(d,2) \leq \delta_{\mathbb{X}}(d,r) \leq \psi(d).$$

Thus we have equality everywhere and the result follows from Eq. (4.5.1). ♠

4.6. Generalized Hamming weights of affine cartesian codes

There is a nice combinatorial formula for the r-th generalized Hamming weight of an affine cartesian code [**BD17**, Theorem 5.4]. Using this combinatorial formula we give an explicit formula to compute the r-th generalized Hamming weight for a family of cartesian codes.

THEOREM 4.34. *Let* $\mathbb{X} := [A_1 \times \cdots \times A_{s-1} \times \{1\}]$ *be a subset of* $\mathbb{P}^{s-1}$, *where* $A_i \subset \mathbb{F}_q$ *and* $d_i = |A_i|$ *for* $i = 1, \ldots, s-1$. *If* $2 \leq d_1 \leq \cdots \leq d_{s-1}$, *then*

$$\delta_{\mathbb{X}}(d,r) = \begin{cases} d_{k+r+1}\cdots d_{s-1}[(d_{k+1}-\ell+1)d_{k+2}\cdots d_{k+r}-1] & \textit{if} \;\; k < s-r-1, \\ \\ (d_{k+1}-\ell+1)d_{k+2}\cdots d_{s-1}-1 & \textit{if} \;\; k = s-r-1, \end{cases} \tag{4.6.1}$$

where we set $d_i \cdots d_j = 1$ *if* $i > j$ *or* $i < 1$, *and* $r \geq 1$, $k \geq 0$, ℓ *are integers such that* $d = \sum_{i=1}^{k}(d_i - 1) + \ell$, *and* $1 \leq \ell \leq d_{k+1} - 1$.

PROOF. Setting $n = s-1$, $R = K[t_1, \ldots, t_n]$ a polynomial ring with coefficients in K, and $L = (t_1^{d_1}, \ldots, t_n^{d_n})$, we order the set $M_{\leq d} := \Delta_{\prec}(L) \cap R_{\leq d}$ of all standard monomials of R/L of degree at most d with the lexicographic order (lex order for short), that is, $t^a \succ t^b$ if and only if the first non-zero entry of $a - b$ is positive. For $r > 1$ and $0 \leq k \leq n - r$, the r-th monomial $t_1^{b_{r,1}} \cdots t_n^{b_{r,n}}$ of $M_{\leq d}$ in decreasing lex order is

$$t_1^{d_1-1} \cdots t_k^{d_k-1} t_{k+1}^{\ell-1} t_{k+r}$$

and the r-th monomial $t_1^{a_{r,1}} \cdots t_n^{a_{r,n}}$ of $M_{\geq c_0-d} := \Delta_{\prec}(L) \cap R_{\geq c_0-d}$ in ascending lex order, where $c_0 = \sum_{i=1}^{n}(d_i - 1)$, is

$$t_{k+1}^{d_{k+1}-\ell} t_{k+2}^{d_{k+2}-1} \cdots t_{k+r-1}^{d_{k+r-1}-1} t_{k+r}^{d_{k+r}-2} t_{k+r+1}^{d_{k+r+1}-1} \cdots t_n^{d_n-1}.$$

Case (I): $0 \leq k < n-r$. The case $r = 1$ was proved in [**LRMV14**, Theorem 3.8]. Thus we may also assume $r \geq 2$. Therefore, applying [**BD17**, Theorem 5.4], we obtain that $\delta_{\mathbb{X}}(d,r)$ is given by

$$\begin{aligned}
1+\sum_{i=1}^{n} a_{r,i} \prod_{j=i+1}^{n} d_j &= 1+(d_{k+1}-\ell)d_{k+2}\cdots d_n + \sum_{i=k+2, i\neq k+r}^{n} (d_i-1)\prod_{j=i+1}^{n} d_j \\
&+ (d_{k+r}-2)d_{k+r+1}\cdots d_n \\
&= (d_{k+1}-\ell)d_{k+2}\cdots d_n + \left(1+\sum_{i=k+2}^{n}(d_i-1)\prod_{j=i+1}^{n} d_j\right) - d_{k+r+1}\cdots d_n \\
&= (d_{k+1}-\ell)d_{k+2}\cdots d_n + (d_{k+2}\cdots d_n) - d_{k+r+1}\cdots d_n \\
&= (d_{k+1}-\ell+1)d_{k+2}\cdots d_n - d_{k+r+1}\cdots d_n \\
&= d_{k+r+1}\cdots d_n[(d_{k+1}-\ell+1)d_{k+2}\cdots d_{k+r}-1].
\end{aligned}$$

Case (II): $k = n-r$. In this case the r-th monomial $t_1^{a_{r,1}}\cdots t_n^{a_{r,n}}$ of $M_{\geq c_0-d}$ in ascending lex order is

$$t_{k+1}^{d_{k+1}-\ell} t_{k+2}^{d_{k+2}-1}\cdots t_{k+r-1}^{d_{k+r-1}-1} t_{k+r}^{d_{k+r}-2} t_{k+r+1}^{d_{k+r+1}-1}\cdots t_n^{d_n-1}.$$

Therefore, applying [**BD17**, Theorem 5.4], we obtain that $\delta_{\mathbb{X}}(d,r)$ is given by

$$\begin{aligned}
1+\sum_{i=1}^{n} a_{r,i} \prod_{j=i+1}^{n} d_j &= 1+(d_{k+1}-\ell)d_{k+2}\cdots d_n + \sum_{i=k+2}^{n-1}(d_i-1)\prod_{j=i+1}^{n} d_j + (d_n-2) \\
&= (d_{k+1}-\ell)d_{k+2}\cdots d_n + \left(1+\sum_{i=k+2}^{n}(d_i-1)\prod_{j=i+1}^{n} d_j\right) - 1 \\
&= (d_{k+1}-\ell)d_{k+2}\cdots d_n + (d_{k+2}\cdots d_n) - 1 = (d_{k+1}-\ell+1)d_{k+2}\cdots d_n - 1.
\end{aligned}$$

♠

COROLLARY 4.35. *Let $\mathbb{T}$ be a projective torus in $\mathbb{P}^{s-1}$ and let $\delta_{\mathbb{T}}(d,r)$ be the r-th generalized Hamming weight of $C_{\mathbb{T}}(d)$. Then*

$$\delta_{\mathbb{T}}(d,r) = \left[(q-1)^{r-1}(q-\ell)-1\right](q-1)^{s-k-r-1}$$

for $1 \leq r \leq s-k-1$, $1 \leq r \leq H_{\mathbb{T}}(d)$, where $d = k(q-2)+\ell$, $0 \leq k \leq s-2$, $1 \leq \ell \leq q-2$.

CHAPTER 5

Cohen-Macaulay vertex-weighted digraphs

We give an effective characterization of the Cohen–Macaulay vertex-weighted oriented trees and forests. For transitive weighted oriented graphs we show that Alexander duality holds. It is shown that edge ideals of weighted acyclic tournaments are Cohen–Macaulay and satisfy Alexander duality. For a monomial ideal with no embedded primes we classify the normality of its symbolic Rees algebra in terms of the normality of its primary components.

5.1. Irreducible decompositions and symbolic powers

In this section we study irreducible representations of monomial ideals and various aspects of symbolic Rees algebras of monomial ideals. Here we continue to employ the notation and definitions used in the introduction of this thesis.

Recall that an ideal L of a Noetherian ring R is called *irreducible* if L cannot be written as an intersection of two proper ideals of R that properly contain L. Let $R = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K. Up to permutation of variables the irreducible monomial ideals of R are of the form

$$(x_1^{a_1}, \ldots, x_r^{a_r}),$$

where $a_1, \ldots, a_r$ are positive integers. According to Theorem 2.17 any monomial ideal I of R has a *unique* irreducible decomposition:

$$I = I_1 \cap \cdots \cap I_m,$$

where $I_1, \ldots, I_m$ are irreducible monomial ideals and $I \neq \cap_{i \neq j} I_i$ for $j = 1, \ldots, m$, that is, this decomposition is irredundant. The ideals $I_1, \ldots, I_m$ are called the *irreducible components* of I.

By [**Vil15**, Proposition 6.1.7] a monomial ideal $\mathfrak{I}$ is a primary ideal if and only if, after permutation of the variables, it has the form:

$$\mathfrak{I} = (x_1^{a_1}, \ldots, x_r^{a_r}, x^{b_1}, \ldots, x^{b_s}), \tag{5.1.1}$$

where $a_i \geq 1$ and $\cup_{i=1}^{s} \operatorname{supp}(x^{b_i}) \subset \{x_1, \ldots, x_r\}$. Thus if $\mathfrak{I}$ is a monomial primary ideal, then $\mathfrak{I}^k$ is a primary ideal for $k \geq 1$. Since irreducible ideals are primary, the irreducible

decomposition of I is a primary decomposition of I. Notice that the irreducible decomposition of I is not necessarily a minimal primary decomposition, that is, I_i and I_j could have the same radical for $i \neq j$. If I is a squarefree monomial ideal, its irreducible decomposition is minimal. For edge ideals of weighted oriented graphs one also has that their irreducible decompositions are minimal [**PRT17**].

DEFINITION 5.1. An irreducible monomial ideal $L \subset R$ is called a *minimal irreducible* ideal of I if $I \subset L$ and for any irreducible monomial ideal L' such that $I \subset L' \subset L$ one has that $L = L'$.

PROPOSITION 5.2. *If $I = I_1 \cap \cdots \cap I_m$ is the irreducible decomposition of a monomial ideal I, then $I_1, \ldots, I_m$ are the minimal irreducible monomial ideals of I.*

PROOF. Let L be an irreducible ideal that contains I. Then $I_i \subset L$ for some i. Indeed if $I_i \not\subset L$ for all i, for each i pick $x_{j_i}^{a_{j_i}}$ in $I_i \setminus L$. Since $I \subset L$, setting $x^a = \operatorname{lcm}\{x_{j_i}^{a_{j_i}}\}_{i=1}^m$ and writing $L = (x_{k_1}^{c_{k_1}}, \ldots, x_{k_\ell}^{c_{k_\ell}})$, it follows that x^a is in I and $x_{j_i}^{a_{j_i}}$ is a multiple of $x_{k_t}^{c_{k_t}}$ for some $1 \leq i \leq m$ and $1 \leq t \leq \ell$. Thus $x_{j_i}^{a_{j_i}}$ is in L, a contradiction. Therefore if L is minimal one has $L = I_i$ for some i. To complete the proof notice that I_i is a minimal irreducible monomial ideal of I for all i. This follows from the first part of the proof using that $I = I_1 \cap \cdots \cap I_m$ is an irredundant decomposition. ♠

The unique minimal set of generators of a monomial ideal I, consisting of monomials, is denoted by $G(I)$. The next result tells us that in certain cases we may have a sort of Alexander duality obtained by switching the roles of minimal generators and irreducible components [**Vil15**, Theorem 6.3.39] (see Example 5.46 and Theorem 5.43).

LEMMA 5.3. *Let I be a monomial ideal of R, and suppose that $G(I) = \{x^{v_1}, \ldots, x^{v_r}\}$ where $v_i = (v_{i1}, \ldots, v_{in})$ for $i = 1, \ldots, r$, and let $I = I_1 \cap \cdots \cap I_m$ be its irreducible decomposition. Then*

$$V := \{x_j^{v_{ij}} \,|\, v_{ij} \geq 1\} = G(I_1) \cup \cdots \cup G(I_m).$$

PROOF. "$\subset$" Take $x_j^{v_{ij}}$ in V, without loss of generality we can assume that $i = 1$ and $j = 1$. We proceed by contradiction assuming that $x_1^{v_{11}}$ is not in $\cup_{i=1}^m G(I_i)$. Setting $M = x_1^{v_{11}-1} x_2^{v_{12}} \cdots x_n^{v_{1n}}$, notice that M is in I. Indeed for any I_j not containing $x_2^{v_{12}} \cdots x_n^{v_{1n}}$, one has that $x_1^{v_{11}}$ is in I_j because x^{v_1} is in I. Thus there is $x_1^{c_j}$ in $G(I_j)$ such that $v_{11} > c_j \geq 1$ because $x_1^{v_{11}}$ is not in $G(I_j)$. Thus M is in I_j. This proves that M is in I, a contradiction to the minimality of $G(I)$ because this monomial that strictly divides one of the elements of $G(I)$ cannot be in I. Thus $x_1^{v_{11}}$ is in $\cup_{i=1}^m G(I_i)$, as required.

"$\supset$" Take $x_j^{a_j}$ in $G(I_i)$ for some i, j, without loss of generality we may assume that $i = j = 1$ and $G(I_1) = \{x_1^{a_1}, \ldots, x_\ell^{a_\ell}\}$. We proceed by contradiction assuming that $x_1^{a_1} \notin V$. Setting $L = (x_1^{a_1+1}, x_2^{a_2}, \ldots, x_\ell^{a_\ell})$, notice that $I \subset L$. Indeed take any monomial x^{v_k} in $G(I)$ which is not in $(x_2^{a_2}, \ldots, x_\ell^{a_\ell})$. Then x^{v_k} is a multiple of $x_1^{a_1}$ because $I \subset I_1$. Hence $v_{k1} > a_1$ because $x_1^{a_1} \notin V$. Thus x^{v_k} is in L. This proves that $I \subset L \subsetneq I_1$, a contradiction to the fact that I_1 is a minimal irreducible monomial ideal of I (see Proposition 5.2). ♠

Let $I \subset R$ be a monomial ideal. The *Alexander dual* of I, denoted $I^\vee$, is the ideal of R generated by all monomials x^a, with $a = (a_1, \ldots, a_n)$, such that $\{x_i^{a_i} | \, a_i \geq 1\}$ is equal to $G(L)$ for some minimal irreducible ideal L of I. The *dual* of I, denoted I^*, is the intersection of all ideals $(\{x_i^{a_i} | \, a_i \geq 1\})$ such that $x^a \in G(I)$. Thus one has

$$I^\vee = \left(\prod_{f \in G(I_1)} f, \ \ldots, \ \prod_{f \in G(I_m)} f \right) \ \text{ and } \ I^* = \bigcap_{x^a \in G(I)} (\{x_i^{a_i} | \, a_i \geq 1\}),$$

where $I_1, \ldots, I_m$ are the irreducible components of I. If $I^* = I^\vee$, we say that *Alexander duality* holds for I. There are other related ways introduced by Ezra Miller **[EGSS01, Mil98, Mil00, MS04]** to define the Alexander dual of a monomial ideal. It is well known that $I^* = I^\vee$ for squarefree monomial ideals **[Vil15**, Theorem 6.3.39].

DEFINITION 5.4. Let I be an ideal of a ring R and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be the minimal primes of I. Given an integer $k \geq 1$, we define the k-th *symbolic power* of I to be the ideal

$$I^{(k)} := \bigcap_{i=1}^{r} \mathfrak{q}_i = \bigcap_{i=1}^{r} (I^k R_{\mathfrak{p}_i} \cap R),$$

where $\mathfrak{q}_i$ is the $\mathfrak{p}_i$-primary component of I^k.

In other words, one has $I^{(k)} = S^{-1} I^k \cap R$, where $S = R \setminus \cup_{i=1}^{r} \mathfrak{p}_i$. An alternative notion of symbolic power can be introduced using the whole set of associated primes of I instead (see, e.g., **[CEHH13, DDSG$^+$15]**):

$$I^{\langle k \rangle} = \bigcap_{\mathfrak{p} \in \operatorname{Ass}(R/I)} (I^k R_{\mathfrak{p}} \cap R) = \bigcap_{\mathfrak{p} \in \operatorname{maxAss}(R/I)} (I^k R_{\mathfrak{p}} \cap R),$$

where $\operatorname{maxAss}(R/I)$ is the set of associated primes which are maximal with respect to inclusion **[CEHH13**, Lemmas 3.1 and 3.2]. Clearly $I^k \subset I^{\langle k \rangle} \subset I^{(k)}$. If I has no embedded primes, e.g. for radical ideals such as squarefree monomial ideals, the two last definitions of symbolic powers coincide. An interesting problem is to give necessary and sufficient conditions for the equality "$I^k = I^{(k)}$ for $k \geq 1$".

For prime ideals the k-th symbolic powers and the k-th usual powers are not always equal. Thus the next lemma does not hold in general but the proof below shows that it will hold for an ideal I in Noetherian ring R under the assumption that $\mathfrak{I}_i^k = \mathfrak{I}_i^{(k)}$ for $i = 1, \ldots, r$. The next lemma is well known for radical monomial ideals [**Vil01**, Propositions 3.3.24 and 7.3.14].

LEMMA 5.5. *Let $I \subset R$ be a monomial ideal and let $I = \mathfrak{I}_1 \cap \cdots \cap \mathfrak{I}_r \cap \cdots \cap \mathfrak{I}_m$ be an irredundant minimal primary decomposition of I, where $\mathfrak{I}_1, \ldots, \mathfrak{I}_r$ are the primary components associated to the minimal primes of I. Then*

$$I^{(k)} = \mathfrak{I}_1^k \cap \cdots \cap \mathfrak{I}_r^k \text{ for } k \geq 1.$$

PROOF. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be the minimal primes of I. By [**Vil15**, Proposition 6.1.7] any power of $\mathfrak{I}_i$ is again a $\mathfrak{p}_i$-primary ideal (see Eq. (5.1.1) at the beginning of this section). Thus $\mathfrak{I}_i^k = \mathfrak{I}_i^{(k)}$ for any i, k. Fixing integers $k \geq 1$ and $1 \leq i \leq r$, let

$$I^k = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r \cap \cdots \cap \mathfrak{q}_s$$

be a primary decomposition of I^k, where $\mathfrak{q}_j$ is $\mathfrak{p}_j$-primary for $j \leq r$. Localizing at $\mathfrak{p}_i$ yields $I^k R_{\mathfrak{p}_i} = \mathfrak{q}_i R_{\mathfrak{p}_i}$ and from $I = \mathfrak{I}_1 \cap \cdots \cap \mathfrak{I}_r \cap \cdots \cap \mathfrak{I}_m$ one obtains:

$$I^k R_{\mathfrak{p}_i} = (I R_{\mathfrak{p}_i})^k = (\mathfrak{I}_i R_{\mathfrak{p}_i})^k = \mathfrak{I}_i^k R_{\mathfrak{p}_i}.$$

Thus $\mathfrak{I}_i^k R_{\mathfrak{p}_i} = \mathfrak{q}_i R_{\mathfrak{p}_i}$ and contracting to R one has $\mathfrak{I}_i^{(k)} = \mathfrak{q}_i$. Therefore

$$I^{(k)} = \mathfrak{I}_1^{(k)} \cap \cdots \cap \mathfrak{I}_r^{(k)} = \mathfrak{I}_1^k \cap \cdots \cap \mathfrak{I}_r^k.$$

♠

It was pointed out to us by Ngô Viêt Trung that Lemma 5.5 is a consequence of [**HHT07**, Lemma 3.1]. This lemma also follows from [**CEHH13**, Proposition 3.6].

REMARK 5.6. To compute the k-th symbolic power $I^{(k)}$ of a monomial ideal I one can use the following procedure for *Macaulay*2 [**GSa**].

```
SPG=(I,k)->intersect(for n from 0 to #minimalPrimes(I)-1
list localize(I^k,(minimalPrimes(I))#n))
```

EXAMPLE 5.7. Let I be the ideal $(x_2x_3, x_4x_5, x_3x_4, x_2x_5, x_1^2x_3, x_1x_2^2)$. Using the procedure of Remark 5.6 we obtain $I^{(2)} = I^2 + (x_1x_2^2x_5, x_1x_2^2x_3)$.

REMARK 5.8. If one uses $\operatorname{Ass}(R/I)$ to define the symbolic powers of a monomial ideal I, the following function for *Macaulay*2 [**GSa**] can be used to compute $I^{\langle k \rangle}$.

```
SPA=(I,k)->intersect(for n from 0 to #associatedPrimes(I)-1
list localize(I^k,(associatedPrimes(I))#n))
```

EXAMPLE 5.9. Let I be the ideal $(x_1x_2^2, x_3x_1^2, x_2x_3^2)$. Using the procedures of Remarks 5.6 and 5.8, we obtain

$$I^{(1)} = I + (x_1x_2x_3) \text{ and } I^{\langle 1\rangle} = I.$$

REMARK 5.10. The following formula is useful to study the symbolic powers $I^{\langle k\rangle}$ of a monomial ideal I [**CEHH13**, Proposition 3.6]:

$$I^kR_{\mathfrak{p}} \cap R = (IR_{\mathfrak{p}} \cap R)^k \text{ for } \mathfrak{p} \in \operatorname{Ass}(R/I) \text{ and } k \geq 1.$$

DEFINITION 5.11. An ideal I of a ring R is called *normally torsion-free* if $\operatorname{Ass}(R/I^k)$ is contained in $\operatorname{Ass}(R/I)$ for all $k \geq 1$.

REMARK 5.12. Let I be an ideal of a ring R. If I has no embedded primes, then I is normally torsion-free if and only if $I^k = I^{(k)}$ for all $k \geq 1$.

LEMMA 5.13. [**SZ**, Lemma 5, Appendix 6] *Let $I \subset R$ be an ideal generated by a regular sequence. Then I^k is unmixed for $k \geq 1$. In particular $I^k = I^{(k)}$ for $k \geq 1$.*

One can also compute the symbolic powers of vanishing ideals of finite sets of reduced projective points using Lemma 5.5 because these ideals are intersections of finitely many prime ideals that are complete intersections. It is well known that complete intersections are normally torsion-free (Lemma 5.24).

REMARK 5.14. (Jonathan O'Rourke) If I is a radical ideal of R and all associated primes of I are normally torsion-free, then the k-th symbolic power of I can be computed using the following procedure for *Macaulay*2 [**GSa**].

```
SP1 = (I,k) ->  (temp = primaryDecomposition I;
temp2 = ((temp_0)^k); for i from 1 to #temp-1 do(temp2 =
intersect(temp2,(temp_i)^k)); return temp2)
```

EXAMPLE 5.15. Let $\mathbb{X}$ be the set $\{[e_1], [e_2], [e_3], [e_4], [(1,1,1,1)]\}$ of 5 points in general linear position in $\mathbb{P}^3$, over the field $\mathbb{Q}$, where e_i is the i-th unit vector, and let $I = I(\mathbb{X})$ be its vanishing ideal. Using *Macaulay*2 [**GSa**] and Remark 5.14 we obtain

$$I = (x_2x_4 - x_3x_4, x_1x_4 - x_3x_4, x_2x_3 - x_3x_4, x_1x_3 - x_3x_4, x_1x_2 - x_3x_4),$$

$I^2 = I^{(2)}$, $I^3 \neq I^{(3)}$ and I is a Gorenstein ideal. This example (in greater generality) has been used in [**NSZN16**, proof of Proposition 4.1 and Remark 4.2(2)].

PROPOSITION 5.16. **[HHT07]** *If $I \subset R$ is a monomial ideal, then the symbolic Rees algebra $R_s(I)$ of I is a finitely generated K-algebra.*

PROOF. It follows at once from Lemma 5.5 and [**HHT07**, Corollary 1.3]. ♠

To compute the generators of the symbolic Rees algebra of a monomial ideal one can use the procedure given in the proof of [**HHT07**, Theorem 1.1]. Another method will be presented in this section that works when the primary components are normal.

REMARK 5.17. The symbolic Rees algebra of a monomial ideal I is finitely generated if one uses the associated primes of I to define symbolic powers. This follows from [**HHT07**, Corollary 1.3] and the following formula [**CEHH13**, Theorem 3.7]:

$$I^{\langle k\rangle} = \bigcap_{\mathfrak{p}\in \operatorname{maxAss}(R/I)} (IR_{\mathfrak{p}} \cap R)^k \text{ for } k \geq 1.$$

COROLLARY 5.18. *If I is a monomial ideal, then $R_s(I)$ is Noetherian and there is an integer $k \geq 1$ such that $[I^{(k)}]^i = I^{(ik)}$ for $i \geq 1$.*

PROOF. It follows at once from [**GN94**, p. 80, Lemma 2.1] or by a direct argument using Proposition 5.16. ♠

For convenience of notation in what follows we will often assume that monomial ideals have no embedded primes but some of the results can be stated and proved for general monomial ideals.

PROPOSITION 5.19. *Let $I \subset R$ be a monomial ideal without embedded primes and let $I = \cap_{i=1}^{r} \mathfrak{I}_i$ be its minimal irredundant primary decomposition. Then $R_s(I)$ is normal if and only if $R[\mathfrak{I}_i t]$ is normal for all i.*

PROOF. $\Rightarrow$) Since $R_s(I)$ is Noetherian and normal it is a Krull domain by a theorem of Mori and Nagata [**Mat80**, p. 296]. Therefore, by [**ST88**, Lemma 2.5], we get that $R_{\mathfrak{p}_i}[I_{\mathfrak{p}_i} t] = R_{\mathfrak{p}_i}[(\mathfrak{I}_i)_{\mathfrak{p}_i} t]$ is normal. Let $\mathfrak{p}_i$ be the radical of $\mathfrak{I}_i$. Any power of $\mathfrak{I}_i$ is a $\mathfrak{p}_i$-primary ideal. This follows from [**Vil15**, Proposition 6.1.7] (see Eq. (5.1.1) at the beginning of this section). Hence it is seen that $R_{\mathfrak{p}_i}[(\mathfrak{I}_i)_{\mathfrak{p}_i} t] \cap R[t] = R[\mathfrak{I}_i t]$. As $R[t]$ is normal it follows that $R[\mathfrak{I}_i t]$ is normal.

$\Leftarrow$) By Lemma 5.5 one has $\cap_{i=1}^{r} R[\mathfrak{I}_i t] = R_s(I)$. As $R[\mathfrak{I}_i t]$ and $R_s(I)$ have the same field of quotients it follows that $R_s(I)$ is normal. ♠

In general, even for monomial ideals without embedded primes, normally torsion-free ideals may not be normal. For instance $I = (x_1^2, x_2^2)$ is normally torsion-free and is not normal. As a consequence of Proposition 5.19 one recovers the following well known result.

COROLLARY 5.20. *Let I be a squarefree monomial ideal. Then $R_s(I)$ is normal and $R[It]$ is normal if I is normally torsion-free.*

Let I be a monomial ideal and let $G(I) = \{x^{v_1}, \ldots, x^{v_m}\}$ be its minimal set of generators. We set

$$\mathcal{A}_I = \{e_1, \ldots, e_n, (v_1, 1), \ldots, (v_m, 1)\},$$

where $e_1, \ldots, e_n$ belong to $\mathbb{Z}^{n+1}$, and denote by $\mathbb{R}_+(I)$ or $\mathbb{R}_+\mathcal{A}_I$ (resp. $\mathbb{N}\mathcal{A}_I$) the cone (resp. semigroup) generated by $\mathcal{A}_I$. The integral closure of $R[It]$ is given by $\overline{R[It]} = K[\mathbb{R}_+(I) \cap \mathbb{Z}^{n+1}]$. Recall that a finite set $\mathcal{H}$ is called a *Hilbert basis* if $\mathbb{N}\mathcal{H} = \mathbb{R}_+\mathcal{H} \cap \mathbb{Z}^{n+1}$, and that $R[It]$ is normal if and only if $\mathcal{A}_I$ is a Hilbert basis **[Vil15**, Proposition 14.2.3].

Let $C \subset \mathbb{R}^{n+1}$ be a rational polyhedral cone. A finite set $\mathcal{H}$ is called a Hilbert basis of C if $C = \mathbb{R}_+\mathcal{H}$ and $\mathcal{H}$ is a Hilbert basis. A Hilbert basis of C is minimal if it does not strictly contain any other Hilbert basis of C. For pointed cones there is unique minimal Hilbert basis **[Vil15**, Theorem 1.3.9].

If the primary components of a monomial ideal are normal, the next result gives a simple procedure to compute its symbolic Rees algebra using Hilbert bases.

PROPOSITION 5.21. *Let I be a monomial ideal without embedded primes and let $I = \cap_{i=1}^r \mathfrak{I}_i$ be its minimal irredundant primary decomposition. If $R[\mathfrak{I}_i t]$ is normal for all i and $\mathcal{H}$ is the Hilbert basis of the polyhedral cone $\cap_{i=1}^r \mathbb{R}_+(\mathfrak{I}_i)$, then $R_s(I)$ is $K[\mathbb{N}\mathcal{H}]$, the semigroup ring of $\mathbb{N}\mathcal{H}$.*

PROOF. As $R[\mathfrak{I}_i t] = K[\mathbb{N}\mathcal{A}_{\mathfrak{I}_i}]$ is normal for $i = 1, \ldots, r$, the semigroup $\mathbb{N}\mathcal{A}_{\mathfrak{I}_i}$ is equal to $\mathbb{R}_+(\mathfrak{I}_i) \cap \mathbb{Z}^{n+1}$ for $i = 1, \ldots, r$. Hence, by Lemma 5.5, we get

$$\begin{aligned} R_s(I) &= \cap_{i=1}^r R[\mathfrak{I}_i t] = \cap_{i=1}^r K[\mathbb{N}\mathcal{A}_{\mathfrak{I}_i}] = K[\cap_{i=1}^r \mathbb{N}\mathcal{A}_{\mathfrak{I}_i}] \\ &= K[\mathbb{R}_+(\mathfrak{I}_1) \cap \cdots \cap \mathbb{R}_+(\mathfrak{I}_r) \cap \mathbb{Z}^{n+1}] = K[\mathbb{N}\mathcal{H}]. \end{aligned}$$

♠

DEFINITION 5.22. The rational polyhedral cone $\cap_{i=1}^r \mathbb{R}_+(\mathfrak{I}_i)$ is called the *Simis cone* of I and is denoted by $\mathrm{Cn}(I)$.

For squarefree monomial ideals the Simis cone was introduced in **[EVY05]**. In particular from Proposition 5.21 we recover **[EVY05**, Theorem 3.5].

EXAMPLE 5.23. The ideal $I = (x_2x_3,\ x_4x_5,\ x_3x_4,\ x_2x_5,\ x_1^2x_3,\ x_1x_2^2)$ satisfies the hypothesis of Proposition 5.21. Using *Normaliz* **[BIR$^+$]** we obtain that the minimal Hilbert basis of the Simis cone is:

```
18 Hilbert basis elements:
0 0 0 0 1 0     1 2 0 0 0 1
```

```
0 0 0 1 0 0      2 0 1 0 0 1
0 0 1 0 0 0      1 2 0 0 1 2
0 1 0 0 0 0      1 2 1 0 0 2
1 0 0 0 0 0      2 2 1 0 1 3
0 0 0 1 1 1      2 2 2 0 0 3
0 0 1 1 0 1      2 4 1 0 2 5
0 1 0 0 1 1      2 4 2 0 1 5
0 1 1 0 0 1      2 4 3 0 0 5
```

Hence $R_s(I)$ is generated by the monomials corresponding to these vectors.

Let I be an ideal of R. The equality "$I^k = I^{(k)}$ for $k \geq 1$" holds if and only if I has no embedded primes and is normally torsion-free (see Remark 5.12). We refer the reader to [**DDSG$^+$15**] for a recent survey on symbolic powers of ideals.

In [**GVV07**, Corollary 3.14] it is shown that a squarefree monomial ideal I is normally torsion-free if and only if the corresponding hypergraph satisfies the max-flow min-cut property.

LEMMA 5.24. [**SZ**, Lemma 5, Appendix 6] *Let $I \subset R$ be an ideal generated by a regular sequence. Then I^k is unmixed for $k \geq 1$. In particular $I^k = I^{(k)}$ for $k \geq 1$.*

The next result generalizes a result of Cowsik and Nori [**CN76**, p. 219].

THEOREM 5.25. [**Bro79**, (14) Corollary, p. 38] *Let $(R, \mathfrak{m})$ be a local Cohen–Macaulay ring, and let $I \subset R$ be an ideal of height $h > 0$. Assume that $IR_{\mathfrak{p}}$ is generated by h elements for each minimal prime $\mathfrak{p}$ of I. Then the following statements are equivalent:*

(*i*) *I^{k-1}/I^k is a Cohen-Macaulay module over R/I for infinitely many k.*
(*ii*) *R/I^k is a Cohen-Macaulay ring for infinitely many k.*
(*iii*) *I is generated by h elements (hence a complete intersection).*

REMARK 5.26. If $I \subset R$ is a complete intersection graded ideal of a polynomial ring R, then R/I^k is Cohen–Macaulay for $k \geq 1$ (see [**HU89**, Lemma 2.7] and [**Mat89**, 17.4, p. 139] for more general statements).

PROPOSITION 5.27. *Let $\mathbb{X}$ be a finite set of reduced points in a projective space $\mathbb{P}^{n-1}$ over a field K. Then $I(\mathbb{X})^k = I(\mathbb{X})^{(k)}$ for all $k \geq 1$ if and only if $I(\mathbb{X})$ is a complete intersection.*

PROOF. $\Rightarrow$): Assume that $I(\mathbb{X})^k = I(\mathbb{X})^{(k)}$ for all $k \geq 1$. We proceed by contradiction assuming that $I(\mathbb{X})$ is not a complete intersection. Then, by Theorem 5.25, $I(\mathbb{X})^k$ is not Cohen–Macaulay for some k. Hence the depth of $R/I(\mathbb{X})^k$ is 0 because $I(\mathbb{X})^k$

has dimension 1. Thus $\mathfrak{m}$ is an associated prime of $R/I(\mathbb{X})^k$, a contradiction because $\operatorname{Ass}(I(\mathbb{X})^k) = \operatorname{Ass}(I(\mathbb{X})^{(k)}) = \operatorname{Ass}(R/I(\mathbb{X}))$ and $I(\mathbb{X})$ is a radical Cohen–Macaulay ideal of height $n-1$.

$\Leftarrow$): This is a special case of a classical result (see Lemma 5.24 and Remark 5.26). ♠

Question: It seems to be an open question when the symbolic Rees algebra of the vanishing ideal of a finite set of (reduced) points in $\mathbb{P}^{n-1}$ is Noetherian. As pointed out to us by Ngô Viêt Trung, there are examples where this algebra is not finitely generated, the first one having been obtained by M. Nagata **[NM65, Nag59]** in his famous counter-example to Hilbert's 14th problem (see also **[Rob90**, p. 462]). According to Roberts **[Rob90**, p. 462], Nagata's example shows that the ideal of sixteen plane reduced points has a non-Noetherian symbolic algebra

COROLLARY 5.28. *Let $\mathbb{X}$ be a finite set of reduced points in $\mathbb{P}^{n-1}$ over a field K. If $I(\mathbb{X})$ is not a complete intersection, then $\operatorname{Ass}(R/I^k) = \operatorname{Ass}(R/I) \cup \{\mathfrak{m}\}$ for $k \gg 0$.*

PROOF. By Brodmann **[Bro79]** the sets $\operatorname{Ass}(R/I(\mathbb{X})^k)$ stabilize for large k. As $R/I(\mathbb{X})$ is one dimensional, for $k \gg 0$ either $\operatorname{Ass}(R/I^k) = \operatorname{Ass}(R/I) \cup \{\mathfrak{m}\}$ or $\operatorname{Ass}(R/I^k) = \operatorname{Ass}(R/I)$. Hence, by Theorem 5.25, the result follows. ♠

Question (Persistence of Associated Primes): Let $\mathbb{X}$ be a finite set of reduced points in $\mathbb{P}^{n-1}$ over a field K. Assume that $\mathfrak{m}$ is an associated prime of $R/I(\mathbb{X})^k$. Is $\mathfrak{m}$ an associated prime of $R/I(\mathbb{X})^{k+1}$?

Normal ideals of Noetherian rings have the persistence property of associated primes **[McA06**, Proposition 3.9].

REMARK 5.29. Assume that $\mathfrak{m}$ is an associated prime of I^k, where $I = I(\mathbb{X})$ and $k \geq 2$ is the first integer such that $I^k \neq I^{(k)}$. Then $\mathfrak{m} = (I^k \colon D)$, for some homogeneous polynomial D (necessarily $D \notin I^k$). Then

$$\mathfrak{m}D \subset I^k \Rightarrow \mathfrak{m}DI^\ell \subset I^{k+\ell} \Rightarrow \mathfrak{m} \subset (I^{k+\ell} \colon DI^\ell) \text{ for } \ell \in \mathbb{N}_+.$$

Thus, to show the equality $\mathfrak{m} = (I^{k+\ell} \colon DI^\ell)$, we need only show that there is some such D of degree $< k\operatorname{indeg}(I)$.

Problem: Give a classification of the normality of the vanishing ideal $I(\mathbb{X})$ of a finite set of reduced points $\mathbb{X}$ in a projective space over a field K.

If $I(\mathbb{X})$ is a complete intersection, then the Rees algebra $R[I(\mathbb{X})t]$ is normal. Indeed this follows from a result of **[SVV94]** after noticing that $I(\mathbb{X})$ is a radical ideal which is generically a complete intersection.

As an application we present a classification of the equality between ordinary and symbolic powers for a family of monomial ideals.

COROLLARY 5.30. *Let I be a monomial ideal without embedded primes and let $\mathfrak{I}_1, \ldots, \mathfrak{I}_r$ be its primary components. If $R[\mathfrak{I}_i t]$ is normal for all i, then $I^k = I^{(k)}$ for $k \geq 1$ if and only if $\mathrm{Cn}(I) = \mathbb{R}_+(I)$ and $R[It]$ is normal.*

PROOF. $\Rightarrow$) As $R_s(I) = R[It]$, by Proposition 5.21, $R[It]$ is normal. Therefore one has

$$K[\mathrm{Cn}(I) \cap \mathbb{Z}^{n+1}] = R_s(I) = R[It] = \overline{R[It]} = K[\mathbb{R}_+(I) \cap \mathbb{Z}^{n+1}].$$

Thus $\mathrm{Cn}(I) = \mathbb{R}_+(I)$.

$\Leftarrow$) By the proof of Proposition 5.21 one has $R_s(I) = K[\mathrm{Cn}(I) \cap \mathbb{Z}^{n+1}]$. Hence

$$R_s(I) = K[\mathrm{Cn}(I) \cap \mathbb{Z}^{n+1}] = K[\mathbb{R}_+(I) \cap \mathbb{Z}^{n+1}] = \overline{R[It]}.$$

As $R[It]$ is normal, we get $R_s(I) = R[It]$, that is, $I^k = I^{(k)}$ for $k \geq 1$. ♠

5.2. Cohen–Macaulay weighted oriented trees

In this section we show that edge ideals of transitive weighted oriented graphs satisfy Alexander duality. It turns out that edge ideals of weighted acyclic tournaments are Cohen–Macaulay and satisfy Alexander duality. Then we classify all Cohen–Macaulay weighted oriented forests. Here we continue to employ the notation and definitions used in section 5.1.

Let G be a graph with vertex set $V(G)$. A subset $C \subset V(G)$ is a *minimal vertex cover* of G if: (i) every edge of G is incident with at least one vertex in C, and (ii) there is no proper subset of C with the first property. If C satisfies condition (i) only, then C is called a *vertex cover* of G.

Let $\mathcal{D}$ be a weighted oriented graph with underlying graph G. Next we recall a combinatorial description of the irreducible decomposition of $I(\mathcal{D})$.

DEFINITION 5.31. **[PRT17]** Let C be a vertex cover of G. Consider the set $L_1(C)$ of all $x \in C$ such that there is $(x, y) \in E(\mathcal{D})$ with $y \notin C$, the set $L_3(C)$ of all $x \in C$ such that $N_G(x) \subset C$, and the set $L_2(C) = C \setminus (L_1(C) \cup L_3(C))$, where $N_G(x)$ is the *neighbor* set of x consisting of all $y \in V(G)$ such that $\{x, y\}$ is an edge of G. A vertex cover C of G is called a *strong vertex cover* of $\mathcal{D}$ if C is a minimal vertex cover of G or else for all $x \in L_3(C)$ there is $(y, x) \in E(\mathcal{D})$ such that $y \in L_2(C) \cup L_3(C)$ with $d(y) \geq 2$.

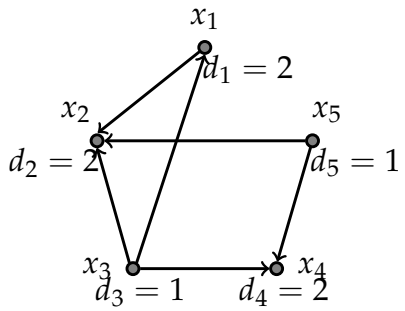


FIGURE 1. A Cohen–Macaulay digraph

THEOREM 5.32. **[PRT17]** *Let $\mathcal{D}$ be a weighted oriented graph. Then L is a minimal irreducible monomial ideal of $I(\mathcal{D})$ if and only if there is a strong vertex cover of $\mathcal{D}$ such that*

$$L = (L_1(C) \cup \{x_i^{d_i} | \, x_i \in L_2(C) \cup L_3(C)\}).$$

THEOREM 5.33. **[PRT17]** *If $\mathcal{D}$ is a weighted oriented graph and $\Upsilon(\mathcal{D})$ is the set of all strong vertex covers of $\mathcal{D}$, then the irreducible decomposition of $I(\mathcal{D})$ is*

$$I(\mathcal{D}) = \bigcap_{C \in \Upsilon(\mathcal{D})} I_C,$$

where $I_C = (L_1(C) \cup \{x_i^{d_i} | \, x_i \in L_2(C) \cup L_3(C)\})$.

PROOF. This follows at once from Proposition 5.2 and Theorem 5.32. ♠

COROLLARY 5.34. **[PRT17]** *Let $\mathcal{D}$ be a weighted oriented graph. Then $\mathfrak{p}$ is an associated prime of $I(\mathcal{D})$ if and only if $\mathfrak{p} = (C)$ for some strong vertex cover C of $\mathcal{D}$.*

EXAMPLE 5.35. Let K be the field of rational numbers and let $\mathcal{D}$ be the weighted digraph of Fig. 1 whose edge ideal is $I = (x_1^2x_3, \, x_1x_2^2, \, x_3x_2^2, \, x_3x_4^2, \, x_4^2x_5, \, x_2^2x_5)$. By Theorem 5.33, the irreducible decomposition of I is

$$I = (x_1^2, \, x_2^2, \, x_4^2) \cap (x_1, \, x_3, \, x_5) \cap (x_2^2, \, x_3, \, x_4^2) \cap (x_2^2, \, x_3, \, x_5).$$

Using *Macaulay*2 **[GSa]**, we get that I is a Cohen–Macaulay ideal whose Rees algebra is Cohen-Macaulay and whose integral closure is

$$\overline{I} = I + (x_1x_2x_3, \, x_1x_3x_4, \, x_2x_3x_4, \, x_2x_4x_5).$$

We note that the Cohen–Macaulayness of both I and its Rees algebra is destroyed (or recovered) by a single stroke of reversing the edge orientation of (x_5, x_2). This also destroys the unmixedness property of I.

In the summer of 2017 Antonio Campillo asked in a seminar at the University of Valladolid if there was anything special if we take an oriented graph $\mathcal{D}$ with underlying graph G and set d_i equal to $\deg_G(x_i)$ for $i = 1, \ldots, n$. It will turn out that in determining the Cohen–Macaulay property of $\mathcal{D}$ one can always make this canonical choice of weights.

LEMMA 5.36. *Let $I \subset R$ be a monomial ideal, let x_i be a variable and let $h_1, \ldots, h_r$ be the monomials of $G(I)$ where x_i occurs. If x_i occurs in h_j with exponent 1 for all j and m is a positive integer, then I is Cohen–Macaulay of height g if and only if*

$$((G(I) \setminus \{h_j\}_{j=1}^r) \cup \{x_i^m h_j\}_{j=1}^r)$$

is Cohen–Macaulay of height g.

PROOF. It follows at once from [**NPV14**, Lemmas 3.3 and 3.5]. ♠

It was pointed out to us by Ngô Viêt Trung that the next proposition follows from the fact that the map $x_i \to y_i^{d_i}$ (replacing x_i by $y_i^{d_i}$) defines a faithfully flat homomorphism from $K[X]$ to $K[Y]$.

PROPOSITION 5.37. *Let I be a squarefree monomial ideal and let $d_i = d(x_i)$ be a weighting of the variables. If G' is set of monomials obtained from $G(I)$ by replacing each x_i with $x_i^{d_i}$, then I is Cohen–Macaulay if and only if $I' = (G')$ is Cohen–Macaulay.*

PROOF. It follows applying Lemma 5.36 to each x_i. ♠

If a vertex x_i is a *sink* (i.e., has only arrows entering x_i), the next result shows that the Cohen-Macaulay property of $I(\mathcal{D})$ is independent of the weight of x_i.

COROLLARY 5.38. *If x_i is a sink of a weighted oriented graph $\mathcal{D}$ and $\mathcal{D}'$ is the digraph obtained from $\mathcal{D}$ by replacing d_i with $d_i = 1$. Then $I(\mathcal{D})$ is Cohen–Macaulay if and only if $I(\mathcal{D}')$ is Cohen–Macaulay.*

That is, to determine whether or not an oriented graph $\mathcal{D}$ is Cohen–Macaulay one may assume that all sources and sinks have weight 1. In particular if all vertices of $\mathcal{D}$ are either sources of sinks and G is its underlying graph, then $I(\mathcal{D})$ is Cohen–Macaulay if and only if $I(G)$ is Cohen–Macaulay.

Let I be a monomial ideal and let x_i be a fixed variable that occurs in $G(I)$. Let q be the maximum of the degrees in x_i of the monomials of $G(I)$ and let $\mathcal{B}_i$ be the set of all monomial of $G(I)$ of degree in x_i equal to q. For use below we set

$$\mathcal{A}_i := \{x^a | \ \deg_{x_i}(x^a) < q\} \cap G(I) = G(I) \setminus \mathcal{B}_i,$$

$p := \max\{\deg_{x_i}(x^a) |\, x^a \in \mathcal{A}_i\}$ and $L := (\{x^a/x_i |\, x^a \in \mathcal{B}_i\} \cup \mathcal{A}_i\})$.

The proof of the next result will be given in Chapter 6 (see Theorem 6.15)

THEOREM 5.39. **[MBMVV18]** *Let I be a monomial ideal. If $p \geq 1$, and $q - p \geq 2$, then*

$$\operatorname{depth}(R/I) = \operatorname{depth}(R/L).$$

The next corollary will be shown in Chapter 6 (see corollary 6.16)

COROLLARY 5.40. *Let $I = I(\mathcal{D})$ be the edge ideal of a vertex-weighted oriented graph with vertices $x_1, \ldots, x_n$ and let d_i be the weight of x_i. If $\mathcal{U}$ is the digraph obtained from $\mathcal{D}$ by assigning weight 2 to every vertex x_i with $d_i \geq 2$, then I is Cohen–Macaulay if and only if $I(\mathcal{U})$ is Cohen–Macaulay.*

LEMMA 5.41. **[Har**, Theorem 16.3(4), p. 200] *Let $\mathcal{D}$ be an oriented graph. Then $\mathcal{D}$ is acyclic, i.e., $\mathcal{D}$ has no oriented cycles, if and only if there is a linear ordering of the vertex set $V(\mathcal{D})$ such that all the edges of $\mathcal{D}$ are of the form (x_i, x_j) with $i < j$.*

A complete oriented graph is called a *tournament*. The next result shows that weighted acyclic tournaments are Cohen–Macaulay.

COROLLARY 5.42. *Let $\mathcal{D}$ be a weighted oriented graph. If the underlying graph G of $\mathcal{D}$ is a complete graph and $\mathcal{D}$ has no oriented cycles, then $I(\mathcal{D})$ is Cohen–Macaulay.*

PROOF. By Lemma 5.41, $\mathcal{D}$ has a source x_i for some i. Hence $\{x_1, \ldots, x_n\}$ is not a strong vertex cover of $\mathcal{D}$ because there is no arrow entering x_i. Thus, by Corollary 5.34, the maximal ideal $\mathfrak{m} = (x_1, \ldots, x_n)$ cannot be an associated prime of $I(\mathcal{D})$. Therefore $R/I(\mathcal{D})$ has depth at least 1. As $\dim(R/I(\mathcal{D})) = 1$, we get that $R/I(\mathcal{D})$ is Cohen–Macaulay. ♠

The next result gives an interesting family of digraphs whose edge ideals satisfy Alexander duality. Recall that a digraph $\mathcal{D}$ is called *transitive* if for any two edges (x_i, x_j), (x_j, x_k) in $E(\mathcal{D})$ with i, j, k distinct, we have that $(x_i, x_k) \in E(\mathcal{D})$. Acyclic tournaments are transitive and transitive oriented graphs are acyclic.

THEOREM 5.43. *If $\mathcal{D}$ is a transitive oriented graph and $I = I(\mathcal{D})$ is its edge ideal, then Alexander duality holds, that is, $I^* = I^\vee$.*

PROOF. "$\supset$" Take $x^a \in G(I^\vee)$. According to Theorem 5.33, there is a strong vertex cover C of $\mathcal{D}$ such that

$$x^a = \left(\prod_{x_k \in L_1} x_k\right)\left(\prod_{x_k \in L_2 \cup L_3} x_k^{d_k}\right), \tag{5.2.1}$$

where $L_i = L_i(C)$ with $i = 1, 2, 3$. Fix a monomial $x_i x_j^{d_j}$ in $G(I(\mathcal{D}))$, that is, $(x_i, x_j) \in E(\mathcal{D})$. It suffices to show that x^a is in the ideal $I_{i,j} := (\{x_i, x_j^{d_j}\})$. If $x_i \in C$, then by Eq. (5.2.1) the variable x_i occurs in x^a because C is equal to $L_1 \cup L_2 \cup L_3$. Hence x^a is a multiple of x_i and x^a is in $I_{i,j}$, as required. Thus we may assume that $x_i \notin C$. By Theorem 5.33 the ideal

$$I_C = (L_1 \cup \{x_k^{d_k} | \, x_k \in L_2 \cup L_3\})$$

is an irreducible component of $I(\mathcal{D})$ and $x_i x_j^{d_j} \in I_C$.

Case (I): $x_i x_j^{d_j} \in (L_1)$. Then $x_i x_j^{d_j} = x_k x^b$ for some $x_k \in L_1$. Hence, as $x_i \notin C$, we get $j = k$. Therefore, as $x_j \in L_1$, there is $x_\ell \notin C$ such that (x_j, x_ℓ) is in $E(\mathcal{D})$. Using that $\mathcal{D}$ is transitive gives $(x_i, x_\ell) \in E(\mathcal{D})$ and $x_i x_\ell^{d_\ell} \in I(\mathcal{D})$. In particular $x_i x_\ell^{d_\ell} \in I_C$, a contradiction because x_i and x_ℓ are not in C. Hence this case cannot occur.

Case (II): $x_i x_j^{d_j} \in (\{x_k^{d_k} | \, x_k \in L_2 \cup L_3\})$. Then we have that $x_i x_j^{d_j} = x_k^{d_k} x^b$ for some $x_k \in L_2 \cup L_3$. As $x_i \notin C$, we get $j = k$ and by Eq. (5.2.1) we obtain $x^a \in I_{i,j}$, as required.

"$\subset$": Take a minimal generator x^α of I^*. By Lemma 5.3, for each i either $\alpha_i = 1$ or $\alpha_i = d_i$. Consider the set $A = \{x_i | \, \alpha_i \geq 1\}$. We can write $A = A_1 \cup A_2$, where A_1 (resp. A_2) is the set of all x_i such that $\alpha_i = 1$ (resp. $\alpha_i = d_i \geq 2$). As (A) contains I, from the proof of Proposition 5.2, and using Theorem 5.33, there exists a strong vertex cover C of $\mathcal{D}$ contained in A such that the ideal

$$I_C = (L_1(C) \cup \{x_i^{d_i} | \, x_i \in L_2(C) \cup L_3(C)\})$$

is an irreducible component of $I(\mathcal{D})$. Thus it suffices to show that any monomial of $G(I_C)$ divides x^α because this would give $x^a \in I^\vee$.

Claim (I): If $x_k \in A_1$, then $d_k = 1$ or $x_k \in L_1(A)$. Assume that $d_k \geq 2$. Since x^α is a minimal generator of I^*, the monomial x^α / x_k is not in I^*. Then there is and edge (x_i, x_j) such that x^α / x_k is not in the ideal $I_{i,j} := (\{x_i, x_j^{d_j}\})$. As $x^\alpha \in I^*$ and $d_k \geq 2$, one has that x^α is in $I_{i,j}$ and $i = k$. Notice that x_j is not in A_2 because x^α / x_k is not in $I_{k,j}$. If x_j is not in A_1 the proof is complete because $x_k \in L_1(A)$. Assume that x_k is in A_1. Then $d_j \geq 2$ because x^α / x_k is not in $I_{k,j}$. Setting $k_1 = k$ and $k_2 = j$ and applying the previous argument to x^α / x_{k_2}, there is $x_{k_3} \notin A_2$ such that (x_{k_2}, x_{k_3}) is in $E(\mathcal{D})$. Since $\mathcal{D}$ is transitive, (x_{k_1}, x_{k_3}) is in $E(\mathcal{D})$. If x_{k_3} is not in A_1 the proof is complete. If x_{k_3} is in A_1, then $d_{k_3} \geq 2$ and we can continue using the previous argument. Suppose we have constructed $x_{k_1}, \ldots, x_{k_s}$ for some $s \leq r$ such that $x_{k_s} \notin A_2$, and $(x_{k_1}, x_{k_{s-1}})$ and $(x_{k_{s-1}}, x_{k_s})$ are in $E(\mathcal{D})$. Since $\mathcal{D}$ is transitive, (x_{k_1}, x_{k_s}) is in $E(\mathcal{D})$. If x_{k_s} is not in A_1 the proof is complete. If x_{k_s} is in A_1 and $s < r$, then $d_{k_s} \geq 2$ and we can continue the process. If x_{k_s} is in A_1 and $s = r$, that is, $A_1 = \{x_{k_1}, \ldots, x_{k_r}\}$, then applying the previous argument to x^α / x_{k_r} there is x_{r+1} not in A

such that (x_r, x_{r+1}) is in $E(\mathcal{D})$. Thus by transitivity (x_{k_1}, x_{r+1}) is in $E(\mathcal{D})$, that is, x_{k_1} is in $L_1(A)$.

Claim (II): If $x_k \in A_2$, then $x_k \in L_2(A)$. Since $x^\alpha \in G(I^*)$ and $\alpha_k = d_k \geq 2$, there is (x_i, x_k) in $E(\mathcal{D})$ such that x^α/x_k is not in $I_{i,k} = (\{x_i, x_k^{d_k}\})$. In particular x_i is not in A. To prove that x_k is in $L_2(A)$ it suffices to show that x_k is not in $L_1(A)$. If x_k is in $L_1(A)$, there is x_j not in A such that (x_k, x_j) is in $E(\mathcal{D})$. As $\mathcal{D}$ is transitive, we get that (x_i, x_j) is in $E(\mathcal{D})$ and $A \cap \{x_i, x_j\} = \emptyset$, a contradiction because (A) contains I.

Take a monomial $x_k^{a_k}$ of $G(I_C)$.

Case (A): $x_k \in L_1(C)$. Then $a_k = 1$. There is $(x_k, x_j) \in E(\mathcal{D})$ with $x_j \notin C$. Notice $x_k \in A_1$. Indeed if $x_k \in A_2$, then x_k is in $L_2(A)$ because of Claim (II). Then there is (x_i, x_k) in $E(\mathcal{D})$ with $x_i \notin A$. By transitivity $(x_i, x_j) \in E(\mathcal{D})$ and $\{x_i, x_j\} \cap C = \emptyset$, a contradiction because (C) contains I. Thus $x_k \in A_1$, that is, $\alpha_k = 1$. This proves that $x_k^{a_k}$ divides x^α.

Case (B): $x_k \in L_2(C)$. Then $x_k^{a_k} = x_k^{d_k}$. First assume $x_k \in A_1$. Then, by Claim (I), $d_k = 1$ or $x_k \in L_1(A)$. Clearly $x_k \notin L_1(A)$ because $L_1(A) \subset L_1(C)$ and x_k—being in $L_2(C)$—cannot be in $L_1(C)$. Thus $d_k = 1$ and $x_k^{d_k}$ divides x^α. Next assume $x_k \in A_2$. Then, by construction of A_2, $x_k^{d_k}$ divides x^α.

Case (C): $x_k \in L_3(C)$. Then $x_k^{a_k} = x_k^{d_k}$. First assume $x_k \in A_1$. Then, by Claim (I), $d_k = 1$ or $x_k \in L_1(A)$. Clearly $x_k \notin L_1(A)$ because $L_1(A) \subset L_1(C)$ and x_k—being in $L_3(C)$—cannot be in $L_1(C)$. Thus $d_k = 1$ and $x_k^{d_k}$ divides x^α. Next assume $x_k \in A_2$. Then, by construction of A_2, $x_k^{d_k}$ divides x^α. ♠

COROLLARY 5.44. *If $\mathcal{D}$ is a weighted acyclic tournament, then $I(\mathcal{D})^* = I(\mathcal{D})^\vee$, that is, Alexander duality holds.*

PROOF. The result follows readily from Theorem 5.43 because acyclic tournaments are transitive. ♠

EXAMPLE 5.45. Let $\mathcal{D}$ be the weighted oriented graph whose edges and weights are

$$(x_2, x_1), (x_3, x_2), (x_3, x_4), (x_3, x_1),$$

and $d_1 = 1, d_2 = 2, d_3 = 1, d_4 = 1$, respectively. This digraph is transitive. Thus $I(\mathcal{D})^* = I(\mathcal{D})^\vee$.

EXAMPLE 5.46. The irreducible decomposition of the ideal $I = (x_1x_2^2, x_1x_3^2, x_2x_3^2)$ is

$$I = (x_1, x_2) \cap (x_1, x_3^2) \cap (x_2^2, x_3^2),$$

in this case $I^\vee = (x_1x_2, x_1x_3^2, x_2^2x_3^2) = (x_1, x_2^2) \cap (x_1, x_3^2) \cap (x_2, x_3^2) = I^*$.

EXAMPLE 5.47. The irreducible decomposition of the ideal $I = (x_1x_2^2, x_3x_1^2, x_2x_3^2)$ is

$$I = (x_1^2, x_2) \cap (x_1, x_3^2) \cap (x_2^2, x_3) \cap (x_1^2, x_2^2, x_3^2),$$

in this case $I^\vee = (x_1^2x_2, x_1x_3^2, x_2^2x_3) \subsetneq (x_1, x_2^2) \cap (x_3, x_1^2) \cap (x_2, x_3^2) = I^*$.

EXAMPLE 5.48. The irreducible decomposition of the ideal $I = (x_1x_2^2, x_1^2x_3)$ is

$$I = (x_1) \cap (x_1^2, x_2^2) \cap (x_3, x_2^2),$$

in this case $I^\vee = (x_1, x_2^2x_3) \supsetneq I^* = (x_1, x_2^2) \cap (x_1^2, x_3) = (x_1^2, x_1x_3, x_2^2x_3)$.

We come to the main result of this section.

THEOREM 5.49. *Let $\mathcal{D}$ be a weighted oriented forest without isolated vertices and let G be its underlying forest. The following conditions are equivalent:*

(a) *$\mathcal{D}$ is Cohen–Macaulay.*
(b) *$I(\mathcal{D})$ is unmixed, that is, all its associated primes have the same height.*
(c) *G has a perfect matching $\{x_1, y_1\}, \ldots, \{x_r, y_r\}$ so that for $i = 1, \ldots, r$ we have*

$$\deg_G(y_i) = 1 \text{ and } d(x_i) = d_i = 1 \text{ if } (x_i, y_i) \in E(\mathcal{D}).$$

PROOF. It suffices to show the result when G is connected, that is, when $\mathcal{D}$ is an oriented tree. Indeed $\mathcal{D}$ is Cohen–Macaulay (resp. unmixed) if and only if all connected components of $\mathcal{D}$ are Cohen–Macaulay (resp. unmixed) [**PRT17, Vil90**].

$(a) \Rightarrow (b)$: This implication follows from the general fact that Cohen–Macaulay graded ideals are unmixed [**Vil15**, Corollary 3.1.17].

$(b) \Rightarrow (c)$: According to the results of [**Vil90**] one has that $|V(G)| = 2r$ and G has a perfect matching $\{x_1, y_1\}, \ldots, \{x_r, y_r\}$ so that $\deg_G(y_i) = 1$ for $i = 1, \ldots, r$. Consider the oriented graph $\mathcal{H}$ with vertex set $V(\mathcal{H}) = \{x_1, \ldots, x_r\}$ whose edges are all (x_i, x_j) such that $(x_i, x_j) \in E(\mathcal{D})$. As $\mathcal{H}$ is acyclic, by Lemma 5.41, we may assume that the vertices of $\mathcal{H}$ have a "topological" order, that is, if $(x_i, x_j) \in E(\mathcal{H})$, then $i < j$. If $(y_i, x_i) \in E(\mathcal{D})$ for $i = 1, \ldots, r$, there is nothing to prove. Assume that $(x_k, y_k) \in E(\mathcal{D})$ for some k. To complete the proof we need only show that $d(x_k) = d_k = 1$. We proceed by contradiction assuming that $d_k \geq 2$. In particular x_k cannot be a source of $\mathcal{H}$. Setting $X = \{x_1, \ldots, x_r\}$, consider the set of vertices

$$C = (X \setminus N^-_{\mathcal{H}}(x_k)) \cup \{y_i |\, x_i \in N^-_{\mathcal{H}}(x_k)\} \cup \{y_k\},$$

where $N^-_{\mathcal{H}}(x_k)$ is the *in-neighbor* set of x_k consisting of all $y \in V(\mathcal{H})$ such that $(y, x_k) \in E(\mathcal{H})$. Clearly C is a vertex cover of G with $r + 1$ elements because the set $N^-_{\mathcal{H}}(x_k)$ is an independent set of G. Let us show that C is a strong cover of $\mathcal{D}$. The set $N^-_{\mathcal{H}}(x_k)$ is not

empty because x_k is not a source of $\mathcal{D}$. Thus x_k is not in $L_3(C)$. Since $L_3(C) \subset \{x_k, y_k\} \subset C$, we get $L_3(C) = \{y_k\}$. There is no arrow of $\mathcal{D}$ with source at x_k and head outside of C, that is, x_k is in $L_2(C)$. Hence (x_k, y_k) is in $E(\mathcal{D})$ with $x_k \in L_2(C)$ and $d(x_k) \geq 2$. This means that C is a strong cover of $\mathcal{D}$. Applying Theorem 5.34 gives that $\mathfrak{p} = (C)$ is an associated prime of $I(\mathcal{D})$ with $r+1$ elements, a contradiction because $I(\mathcal{D})$ is an unmixed ideal of height r.

$(c) \Rightarrow (a)$: We proceed by induction on r. The case $r = 1$ is clear because $I(\mathcal{D})$ is a principal ideal, hence Cohen–Macaulay. Let $\mathcal{H}$ be the graph defined in the proof of the previous implication. As before we may assume that the vertices of $\mathcal{H}$ are in topological order and we set $R = K[x_1, \ldots, x_r, y_1, \ldots, y_r]$.

Case (I): Assume that $(y_r, x_r) \in E(\mathcal{D})$. Then x_r is a sink of $\mathcal{D}$ (i.e., has only arrows entering x_r). Using the equalities

$$(I(\mathcal{D})\colon x_r^{d_r}) = (N_G(x_r), I(\mathcal{D} \setminus N_G(x_r))) \text{ and } (I(\mathcal{D}), x_r^{d_r}) = (x_r^{d_r}, I(\mathcal{D} \setminus \{x_r\})),$$

and applying the induction hypothesis to $I(\mathcal{D} \setminus N_G(x_r))$ and $I(\mathcal{D} \setminus \{x_r\})$ we obtain that the ideals $(I(\mathcal{D})\colon x_r^{d_r})$ and $(I(\mathcal{D}), x_r^{d_r})$ are Cohen–Macaulay of dimension r. Therefore, as $I(\mathcal{D})$ has height r, from the exact sequence

$$0 \to R/(I(\mathcal{D})\colon x_r^{d_r})[-d_r] \xrightarrow{x_r^{d_r}} R/I(\mathcal{D}) \to R/(I(\mathcal{D}), x_r^{d_r}) \to 0$$

and using the depth lemma (see [**Vil15**, Lemma 2.3.9]) we obtain that $I(\mathcal{D})$ is Cohen–Macaulay.

Case (II): Assume that $(x_r, y_r) \in E(\mathcal{D})$. Then $d(x_r) = d_r = 1$ and $x_r y_r^{e_r} \in I(\mathcal{D})$, where $d(y_r) = e_r$. Using the equalities

$$(I(\mathcal{D})\colon x_r) = (N_G(x_r) \setminus \{y_r\}, y_r^{e_r}, I(\mathcal{D} \setminus N_G(x_r))) \text{ and } (I(\mathcal{D}), x_r) = (x_r, I(\mathcal{D} \setminus \{x_r\})),$$

and applying the induction hypothesis to $I(\mathcal{D} \setminus N_G(x_r))$ and $I(\mathcal{D} \setminus \{x_r\})$ we obtain that the ideals $(I(\mathcal{D})\colon x_r)$ and $(I(\mathcal{D}), x_r)$ are Cohen–Macaulay of dimension r. Therefore, as $I(\mathcal{D})$ has height r, from the exact sequence

$$0 \to R/(I(\mathcal{D})\colon x_r)[-1] \xrightarrow{x_r} R/I(\mathcal{D}) \to R/(I(\mathcal{D}), x_r) \to 0$$

and using the depth lemma [**Vil15**, Lemma 2.3.9] we obtain that $I(\mathcal{D})$ is Cohen–Macaulay. ♠

The following result was conjectured in a preliminary version of this thesis and proved recently in [**HLM$^+$18**] using polarization of monomial ideals.

THEOREM 5.50. [**HLM$^+$18**, Theorem 3.1] *Let $\mathcal{D}$ be a weighted oriented graph and let G be its underlying graph. Suppose that G has a perfect matching $\{x_1, y_1\}, \ldots, \{x_r, y_r\}$ where $\deg_G(y_i) = 1$ for each i. The following conditions are equivalent:*

(a) *$\mathcal{D}$ is Cohen–Macaulay.*
(b) *$I(\mathcal{D})$ is unmixed, that is, all its associated primes have the same height.*
(c) *$d(x_i) = 1$ for any edge of $\mathcal{D}$ of the form (x_i, y_i).*

The equivalence between (b) and (c) was also proved in [**PRT17**, Theorem 4.16].

REMARK 5.51. If $\mathcal{D}$ is a Cohen–Macaulay weighted oriented graph, then $I(\mathcal{D})$ is unmixed and $\operatorname{rad}(I(\mathcal{D}))$ is Cohen–Macaulay. This follows from the fact that Cohen–Macaulay ideals are unmixed and using a result of Herzog, Takayama and Terai [**HTT05**, Theorem 2.6] which is valid for any monomial ideal. It is an open question whether the converse is true [**PRT17**, Conjecture 5.5].

EXAMPLE 5.52. The radical of the ideal $I = (x_2x_1, x_3x_2^2, x_3x_4)$ is Cohen–Macaulay and I is not unmixed. The irreducible components of I are (x_1, x_3), (x_2, x_3), (x_1, x_2^2, x_4), (x_2, x_4).

EXAMPLE 5.53. (Terai) The ideal $I = (x_1, x_2)^2 \cap (x_2, x_3)^2 \cap (x_3, x_4)^2$ is unmixed, $\operatorname{rad}(I)$ is Cohen-Macaulay, and I is not Cohen–Macaulay.

CHAPTER 6

Depth and regularity of monomial ideals via polarization and combinatorial optimization

Here we use polarization to study the behavior of the depth and regularity of a monomial ideal I, locally at a variable x_i, when we lower the degree of all the highest powers of the variable x_i occurring in the minimal generating set of I, and examine the depth and regularity of powers of edge ideals of clutters using combinatorial optimization techniques. If I is the edge ideal of an unmixed clutter with the max-flow min-cut property, we show that the powers of I have non-increasing depth and non-decreasing regularity. As a consequence edge ideals of unmixed bipartite graphs have non-increasing depth. We are able to show that the symbolic powers of the ideal of covers of the clique clutter of a strongly perfect graph have non-increasing depth. A similar result holds for the ideal of covers of a uniform ideal clutter.

6.1. Depth and regularity of monomial ideals via polarization

Let $R = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K and let I be a monomial ideal. The unique minimal set of generators of I consisting of monomials is denoted by $G(I)$. The goal of this section is to use polarization to control the depth and regularity of R/I when the powers of a variable appearing in $G(I)$ are reduced. To do so, we first recall some known results, then show a series of equivalent conditions that will allow us to study the behavior of the depth and the regularity of R/I.

In [**DHS13**, Lemma 5.1] it was shown that $\operatorname{depth}(R/(I\colon x_i)) \geq \operatorname{depth}(R/I)$ for all i. By noting that a generating set for $(I\colon x_i)$ can be found from $G(I)$ by reducing all powers of x_i by one, this can be viewed as the first step in reaching the goal. The result was recently generalized in [**CHH$^+$17**, Theorem 3.1] to any monomial ideal. We provide an alternate proof using polarization. We begin by treating the squarefree case using Stanley-Reisner complexes.

Recall that if Δ is a simplicial complex with vertices $x_1, \ldots, x_n$, the *Stanley-Reisner ideal* of Δ, denoted by I_Δ, is the ideal of R whose squarefree monomial generators correspond to non-faces of Δ. That is,

$$I_\Delta = (x_{i_1} \cdots x_{i_t} | \{x_{i_1}, \ldots, x_{i_t}\} \notin \Delta).$$

The following result shows how the structure of the simplicial complex can be used to find the depth of the associated ideal.

THEOREM 6.1. **[S$^+$90]** *Let Δ be a simplicial complex with vertex set $V = \{x_1, \ldots, x_n\}$, let I_Δ be its Stanley–Reisner ideal, and $K[\Delta] = R/I_\Delta$. Then*

$$\operatorname{depth}(R/I_\Delta) = 1 + \max\{i \mid K[\Delta^i] \text{ is Cohen–Macaulay}\},$$

where $\Delta^i = \{F \in \Delta \mid \dim(F) \leq i\}$ is the i-skeleton and $-1 \leq i \leq \dim(\Delta)$.

The *star* of a face σ in a simplicial complex Δ, denoted $\operatorname{star}_\Delta(\sigma)$, is defined to be the subcomplex of Δ generated by all facets of Δ that contain σ.

LEMMA 6.2. **[CHH$^+$17**, Theorem 3.1] *Let $I \subset R$ be a squarefree monomial ideal and let f be a squarefree monomial. Then* $\operatorname{depth}(R/(I\colon f)) \geq \operatorname{depth}(R/I)$.

PROOF. Let $\sigma = \operatorname{supp}(f)$ be the set of all variables that occur in f. We may assume that f is a zero divisor of R/I because otherwise $(I\colon f) = I$ and there is nothing to prove. We may also assume that f is not in all minimal primes of I because in this case $(I\colon f) = R$ and $\operatorname{depth}(0) = \infty$. Let Δ and Δ' be the Stanley–Reisner complexes of I and $(I\colon f)$, respectively. Setting $d = \dim(\Delta)$, $d' = \dim(\Delta')$, one has $d' \leq d$. Assume that Δ^i is Cohen–Macaulay for some $i \leq d$. We claim that $i \leq d'$. If $i > d'$, take a facet F of Δ' of dimension d', that is, F is a facet of Δ of dimension d' containing σ. As F is a face of Δ^i and this complex is pure, we get that F is properly contained in a face of Δ of dimension i, a contradiction. Hence $i \leq d'$. The simplicial complex Δ' is equal to $\operatorname{star}_\Delta(\sigma)$. Therefore, from the equalities

$$(\Delta')^i = (\operatorname{star}_\Delta(\sigma))^i = \operatorname{star}_{\Delta^i}(\sigma),$$

and using that the star of a face of a Cohen–Macaulay complex is again Cohen–Macaulay **[Vil15**, p. 224], we get that $(\Delta')^i$ is Cohen–Macaulay. Hence, by Theorem 6.1, it follows that the depth of $R/(I\colon f)$ is greater than or equal to $\operatorname{depth}(R/I)$. ♠

A common technique in commutative algebra is to start with a short exact sequence of the form

$$0 \longrightarrow R/(I\colon f)[-k] \xrightarrow{f} R/I \longrightarrow R/(I, f) \longrightarrow 0,$$

where $I \subset R$ is a graded ideal and f is a homogeneous polynomial of degree k, and use information about two of the terms to glean desired information about the third. Both depth and regularity are known to behave well relative to short exact sequences. There are several versions of the depth lemma that appear in the literature. The following lemmas provide the information relating the depths and regularity of the terms of a short exact sequence in a format that will be particularly useful in the remainder of this chapter.

LEMMA 6.3. *Let* $0 \to N \to M \to L \to 0$ *be a short exact sequence of modules over a local ring* R*. The following conditions are equivalent.*

(a) $\operatorname{depth}(N) \geq \operatorname{depth}(M)$.
(b) $\operatorname{depth}(M) = \operatorname{depth}(N)$ *or* $\operatorname{depth}(M) = \operatorname{depth}(L)$.
(c) $\operatorname{depth}(L) \geq \operatorname{depth}(M) - 1$.

PROOF. It follows from the depth lemma [**Vil15**, Lemma 2.3.9]. ♠

There is a similar statement for the regularity.

LEMMA 6.4. *Let* $0 \to N \to M \to L \to 0$ *be a short exact sequence of graded finitely generated* R*-modules. The following conditions are equivalent.*

(a) $\operatorname{reg}(M) \geq \operatorname{reg}(N) - 1$.
(b) $\operatorname{reg}(M) = \operatorname{reg}(N)$ *or* $\operatorname{reg}(M) = \operatorname{reg}(L)$.
(c) $\operatorname{reg}(M) \geq \operatorname{reg}(L)$.

PROOF. It follows from [**Eis13**, Corollary 20.19]. ♠

LEMMA 6.5. *Let* $0 \to N \to M \to L \to 0$ *be an exact sequence of graded finitely generated* R*-modules with homomorphisms of degree* 0 *and* $k \geq 1$ *an integer. The following are equivalent.*

(a) $\operatorname{reg}(N) \leq \operatorname{reg}(M) + k$.
(b) $\operatorname{reg}(L) \leq \operatorname{reg}(M) + k - 1$.

PROOF. (a) $\Rightarrow$ (b): We may assume $\operatorname{reg}(M) \leq \operatorname{reg}(L) - 1$, otherwise there is nothing to prove. Hence, by [**Eis13**, Corollary 20.19], we get

$$\operatorname{reg}(L) \leq \max(\operatorname{reg}(N) - 1, \operatorname{reg}(M)) \leq \operatorname{reg}(M) + k - 1.$$

(b) $\Rightarrow$ (a): As $\operatorname{reg}(L) + 1 \leq \operatorname{reg}(M) + k$, by [**Eis13**, Corollary 20.19], we get

$$\operatorname{reg}(N) \leq \max(\operatorname{reg}(M), \operatorname{reg}(L) + 1) \leq \operatorname{reg}(M) + k.$$

♠

Let $\mathcal{C}$ be a *clutter* with vertex set $X = \{x_1, \ldots, x_n\}$, that is, $\mathcal{C}$ consists of a family of subsets of X, called edges, none of which is included in another. The sets of vertices and edges of $\mathcal{C}$ are denoted by $V(\mathcal{C})$ and $E(\mathcal{C})$, respectively. If $V \subset X$, the clutter obtained from $\mathcal{C}$ by deleting all edges of $\mathcal{C}$ that intersect V will be denoted by $\mathcal{C} \setminus V$. The *edge ideal* of $\mathcal{C}$, denoted $I(\mathcal{C})$, is the ideal of R generated by all squarefree monomials $x_e = \prod_{x_i \in e} x_i$ such that $e \in E(\mathcal{C})$. The *ideal of covers* $I(\mathcal{C})^\vee$ of $\mathcal{C}$ is the edge ideal of $\mathcal{C}^\vee$, the clutter of minimal vertex covers of $\mathcal{C}$ [**Vil15**, p. 221]. The ideal $I(\mathcal{C})^\vee$ is also called the *Alexander dual* of $I(\mathcal{C})$ or simply the *cover ideal* of $\mathcal{C}$.

LEMMA 6.6. *Let $I(\mathcal{C}) \subset R$ be the edge ideal of a clutter $\mathcal{C}$ and let $f = x_{i_1} \cdots x_{i_k}$ be a squarefree monomial of R. The following hold.*

(i) $(I(\mathcal{C})^\vee \colon f)^\vee = I(\mathcal{C} \setminus \{x_{i_1}, \ldots, x_{i_k}\})$.
(ii) $(I(\mathcal{C}) \colon f)^\vee = I(\mathcal{C}^\vee \setminus \{x_{i_1}, \ldots, x_{i_k}\})$.
(iii) If x_i is a variable, then $(I(\mathcal{C}), x_i)^\vee = x_i I(\mathcal{C} \setminus \{x_i\})^\vee$.

PROOF. (i): Let $E(\mathcal{C})$ be the set of edges of $\mathcal{C}$. We set $V = \{x_{i_1}, \ldots, x_{i_k}\}$ and $I = I(\mathcal{C})$. Then

$$(I^\vee \colon f)^\vee = \left(\bigcap_{e \in E(\mathcal{C})} (e) \colon f \right)^\vee = \left(\bigcap_{e \in E(\mathcal{C} \setminus V)} (e) \right)^\vee = (I(\mathcal{C} \setminus V)^\vee)^\vee = I(\mathcal{C} \setminus V).$$

(ii): Notice the equalities $I(\mathcal{C}^\vee)^\vee = (I(\mathcal{C})^\vee)^\vee = I(\mathcal{C})$. Thus this part follows from (i) by replacing $\mathcal{C}$ with $\mathcal{C}^\vee$.

(iii): Setting $L = (I(\mathcal{C}), x_i)$ and $J = I(\mathcal{C} \setminus \{x_i\})$, it follows readily that

$$L = (I(\mathcal{C} \setminus \{x_i\}), x_i) = (J, x_i) = \bigcap_{\mathfrak{p} \in \operatorname{Ass}(R/J)} (x_i, \mathfrak{p}).$$

Hence, by duality [**Vil15**, Theorem 6.3.39], one has $(I(\mathcal{C}), x_i)^\vee = x_i I(\mathcal{C} \setminus \{x_i\})^\vee$. ♠

Our interest in the duality results above is partially motivated by the following result relating regularity and projective dimension, and thus depth, when passing to the dual.

THEOREM 6.7. (Terai [**Ter99**]) *If $I \subset R$ is a squarefree monomial ideal, then*

$$\operatorname{reg}(I) = 1 + \operatorname{reg}(R/I) = \operatorname{pd}(R/I^\vee).$$

In [**CHH$^+$17**, Theorem 3.1] it is shown that conditions (ii) and (iv) of the next result hold (cf. [**DHS13**, Lemmas 5.1 and 2.10]). For squarefree monomial ideals—using the above duality theorem of Terai [**Ter99**]—we show that these conditions are in fact equivalent (cf. Remark 6.9). Roughly speaking the inequalities of (ii) and (iv) are dual of each other via the duality theorem of Terai.

PROPOSITION 6.8. *Let $I \subset R$ be a squarefree monomial ideal and let $f = x_{i_1} \cdots x_{i_k}$ be a squarefree monomial of R of degree k. Then any of the following equivalent conditions hold.*

(i) $\operatorname{depth}(R/(f, I)) \geq \operatorname{depth}(R/I) - 1$.
(ii) [**CHH$^+$17**, Theorem 3.1] $\operatorname{depth}(R/I) \leq \operatorname{depth}(R/(I \colon f))$.
(iii) $\operatorname{depth}(R/(x_{i_1}, \ldots, x_{i_k}, I)) \geq \operatorname{depth}(R/I) - k$.
(iv) [**CHH$^+$17**, Theorem 3.1] $\operatorname{reg}(R/I) \geq \operatorname{reg}(R/(I \colon f))$.
(v) $\operatorname{reg}(R/(f, I)) \leq \operatorname{reg}(R/I) + k - 1$.

PROOF. By Lemma 6.2, condition (ii) holds for any squarefree monomial ideal I and for any squarefree monomial f. Thus it suffices to show that (i) and (ii) are equivalent and that (i) and (iii)–(v) are equivalent conditions. Since I is squarefree, there is a clutter $\mathcal{C}$ such that $I = I(\mathcal{C})$.

(i) $\Leftrightarrow$ (ii): This follows from applying Lemma 6.3 to the short exact sequence

$$0 \longrightarrow R/(I\colon f)[-k] \xrightarrow{f} R/I \longrightarrow R/(I,f) \longrightarrow 0. \tag{6.1.1}$$

(i) $\Rightarrow$ (iii): This follows directly by induction on k.

(iii) $\Rightarrow$ (iv): As (iii) holds for squarefree monomials, applying (iii) to $I(\mathcal{C}^\vee)$, we get

$$k + \operatorname{depth}(R/(x_{i_1},\ldots,x_{i_k},I(\mathcal{C}^\vee))) \geq \operatorname{depth}(R/I(\mathcal{C}^\vee)).$$

Therefore, setting $V = \{x_{i_1},\ldots,x_{i_k}\}$ and $X = \{x_1,\ldots,x_n\}$, we get

$$\begin{aligned}\operatorname{depth}(R/I(\mathcal{C}^\vee \setminus V)) &= k + \operatorname{depth}(K[X\setminus V]/I(\mathcal{C}^\vee \setminus V))\\ &= k + \operatorname{depth}(R/(V,I(\mathcal{C}^\vee))) \geq \operatorname{depth}(R/I(\mathcal{C}^\vee)),\end{aligned}$$

that is, $\operatorname{depth}(R/I(\mathcal{C}^\vee \setminus V)) \geq \operatorname{depth}(R/I(\mathcal{C}^\vee))$, where $I(\mathcal{C}^\vee) = I(\mathcal{C})^\vee$. Hence, applying the Auslander–Buchsbaum formula [**Vil15**, Theorem 3.5.13] to both sides of this inequality and then using Terai's formula of Theorem 6.7, we get

$$\operatorname{reg}(R/I(\mathcal{C})) \geq \operatorname{reg}(R/I(\mathcal{C}^\vee \setminus V)^\vee).$$

By Lemma 6.6(ii) one has $I(\mathcal{C}^\vee \setminus V) = (I(\mathcal{C})\colon f)^\vee$. Thus, $I(\mathcal{C}^\vee \setminus V)^\vee = (I(\mathcal{C})\colon f)$, and the required inequality follows.

(iv) $\Rightarrow$ (iii): As (iv) holds for squarefree monomials, applying (iv) to $I(\mathcal{C}^\vee)$, we get

$$\operatorname{reg}(R/I(\mathcal{C}^\vee)) \geq \operatorname{reg}(R/(I(\mathcal{C}^\vee)\colon f)).$$

Therefore, applying Terai's formula of Theorem 6.7 and Lemma 6.6(i), we get

$$\operatorname{pd}_R(R/I(\mathcal{C})) \geq \operatorname{pd}_R(R/I(\mathcal{C}\setminus V)).$$

Hence, applying the Auslander–Buchsbaum formula [**Vil15**, Theorem 3.5.13] to both sides of this inequality and using depth properties, we obtain

$$\begin{aligned}k + \operatorname{depth}(R/(V,I(\mathcal{C}))) &= k + \operatorname{depth}(K[X\setminus V]/I(\mathcal{C}\setminus V))\\ &= \operatorname{depth}(R/I(\mathcal{C}\setminus V)) \geq \operatorname{depth}(R/I(\mathcal{C})).\end{aligned}$$

(iv) $\Leftrightarrow$ (v): Since $\operatorname{reg}((R/(I\colon f))[-k]) = k + \operatorname{reg}(R/(I\colon f))$, the equivalence between (iv) and (v) follows applying Lemma 6.5 to the exact sequence of Eq. (6.1.1). ♠

In [**CHH$^+$17**, Corollary 3.3] it is shown that condition (vii) below holds (cf. [**DHS13**, Lemma 2.10]).

REMARK 6.9. (A) Conditions (i)–(v) are equivalent to
(vi) $\operatorname{depth}(R/I) = \operatorname{depth}(R/(I\colon f))$ or $\operatorname{depth}(R/I) = \operatorname{depth}(R/(f, I))$.
(B) For $k = \deg(f) = 1$ conditions (i)–(vi) are equivalent to:
(vii) $\operatorname{reg}(R/I) = \operatorname{reg}(R/(I\colon f)) + 1$ or $\operatorname{reg}(R/I) = \operatorname{reg}(R/(f, I))$.
This follows applying Lemmas 6.3 and 6.4 to the exact sequence given in Eq. (6.1.1).

Depth and regularity via polarization. In what follows we will use the polarization technique due to Fröberg that we briefly recall now (see [**Vil15**, p. 203] and the references therein). Note that alternate labelings of polarizations and partial polarizations exist in the literature (see, for example, [**Far06, HH11, Pee10**]); however, the notation used here will prove beneficial in Section 6.2.

Let $J \subset R$ be a monomial ideal minimally generated by $G(J) = \{g_1, \ldots, g_s\}$. We set γ_i equal to $\max\{\deg_{x_i}(g) | \, g \in G(J)\}$. To polarize J we use the set of new variables

$$X_J = \cup_{i=1}^{n} \{x_{i,2}, \ldots, x_{i,\gamma_i}\},$$

where $\{x_{i,2}, \ldots, x_{i,\gamma_i}\}$ is empty if $\gamma_i = 0$ or $\gamma_i = 1$. It is convenient to identify the variable x_i with $x_{i,1}$ for all i. Recall that a power $x_i^{c_i}$ of a variable x_i, $1 \leq c_i \leq \gamma_i$, polarizes to $(x_i^{c_i})^{\mathrm{pol}} = x_i$ if $\gamma_i = 1$, to $(x_i^{c_i})^{\mathrm{pol}} = x_{i,2} \cdots x_{i,c_i+1}$ if $c_i < \gamma_i$, and to $(x_i^{c_i})^{\mathrm{pol}} = x_{i,2} \cdots x_{i,\gamma_i} x_i$ if $c_i = \gamma_i$. This induces a polarization g_i^{pol} of g_i for each $i = 1, \ldots, s$. The *full polarization* J^{pol} of J is the ideal of $R[X_J]$ generated by $g_1^{\mathrm{pol}}, \ldots, g_s^{\mathrm{pol}}$. The next lemma is well known.

LEMMA 6.10. *Let J be a monomial ideal of R. Then*

(a) (Fröberg [**Frö82**]) $\operatorname{depth}(R[X_J]/J^{\mathrm{pol}}) = |X_J| + \operatorname{depth}(R/J) = \operatorname{depth}(R[X_J]/J)$.
(b) $\operatorname{pd}(R/J) = \operatorname{pd}(R[X_J]/J^{\mathrm{pol}})$.
(c) $\operatorname{pd}(R/J) = \operatorname{reg}(R[X_J]/(J^{\mathrm{pol}})^{\vee}) + 1$.
(d) [**HH11**, Corollary 1.6.3] $\operatorname{reg}(R/J) = \operatorname{reg}(R[X_J]/J^{\mathrm{pol}})$.

PROOF. Part (b) follows applying the Auslander–Buchsbaum formula [**Vil15**, Theorem 3.5.13]to part (a). Part (c) follows from Theorem 6.7 and part (b). ♠

Let $I \subset R$ be a monomial ideal and let f be a monomial. Using polarization, one can extend Proposition 6.8 and Remark 6.9 to general monomial ideals. The following result will be needed when relating the depth and the regularity of a monomial ring R/I with those of the ring $R[X_L]/I^{\mathrm{pol}}$, where L is the ideal (f, I) and I^{pol} is the polarization of I with respect to $R[X_L]$ (cf. Lemma 6.10).

PROPOSITION 6.11. *Let $I \subset R$ be a monomial ideal and let f be a monomial. If $L = (f, I)$ and X_L is the set of new variables that are needed to polarize L, then*

(i) $\operatorname{depth}(R[X_L]/L^{\mathrm{pol}}) - \operatorname{depth}(R[X_L]/(f_1^{\mathrm{pol}}, \ldots, f_r^{\mathrm{pol}})) = \operatorname{depth}(R/L) - \operatorname{depth}(R/I)$,

(ii) $\operatorname{reg}(R[X_L]/L^{\mathrm{pol}}) = \operatorname{reg}(R/L)$ *and* $\operatorname{reg}(R[X_L]/(f_1^{\mathrm{pol}}, \ldots, f_r^{\mathrm{pol}})) = \operatorname{reg}(R/I)$,

where $G(I) = \{f_1, \ldots, f_r\}$, and f_i^{pol} is the polarization of f_i in $R[X_L]$.

PROOF. (i): We may assume f is not in I, otherwise there is nothing to prove. Let $L^{\mathrm{pol}} \subset R[X_L]$ be the full polarization of L. For use below we set

$$\delta_i = \max\{\deg_i(g) | \, g \in G(I)\}$$

and $f = x_1^{a_1} \cdots x_n^{a_n}$. The set of variables of R is denoted by $X = \{x_1, \ldots, x_n\}$.

Subcase (i.a): $a_i > \delta_i$ for some i. Then $G(L) = \{f, f_1, \ldots, f_r\}$. For simplicity of notation we assume there is an integer k such that $a_1 > \delta_1, \ldots, a_k > \delta_k$ and $a_i \leq \delta_i$ for $i > k$. If $\delta_i = 0$ for some $i > k$, then the variable x_i does not occur in any element of $G(L)$ because $a_i = 0$. Hence we can replace R by $K[X \setminus \{x_i\}]$. Thus we may assume that $\delta_i \geq 1$ for $i > k$. To polarize L we use the set of variables

$$X_L = (\cup_{i=1}^{k} \{x_{i,2}, \ldots, x_{i,\delta_i}, x_{i,\delta_i+1}, \ldots, x_{i,a_i}\}) \cup (\cup_{i=k+1}^{n} \{x_{i,2}, \ldots, x_{i,\delta_i}\}),$$

where $\{x_{i,2}, \ldots, x_{i,c}\}$ is the empty set if $c = 0$ or $c = 1$. We identify x_i with $x_{i,1}$ for all i. In this setting the monomial $x_i^{a_i}$ polarizes to $(x_i^{a_i})^{\mathrm{pol}} = x_{i,2} \cdots x_{i,a_i} x_i$ for $i = 1, \ldots, k$ and the monomial $x_i^{\delta_i}$ polarizes to $(x_i^{\delta_i})^{\mathrm{pol}} = x_{i,2} \cdots x_{i,\delta_i} x_i$ for $i > k$. Let f^{pol} and f_i^{pol} be the polarizations in $R[X_L]$ of f and f_i (see Example 6.14). By Lemma 6.10 one has

(6.1.2)

$$\operatorname{depth}(R[X_L]/L^{\mathrm{pol}}) = |X_L| + \operatorname{depth}(R/L) = \sum_{i=1}^{k} (a_i - 1) + \sum_{i=k+1}^{n} (\delta_i - 1) + \operatorname{depth}(R/L).$$

Next we relate the depth of $R[X_L]/(f_1^{\mathrm{pol}}, \ldots, f_r^{\mathrm{pol}}))$ to the depth of R/I. For this consider the polynomial ring $R' = K[X']$, where $X' = (X \setminus \{x_i\}_{i=1}^{k}) \cup \{x_{1,\delta_i+1}\}_{i=1}^{k}$, and let f_i' be the polynomial of R' obtained from f_i by replacing x_i by x_{i,δ_i+1} for $i = 1, \ldots, k$. If I' is the ideal of R' generated by $f_1', \ldots, f_r'$, then $K[X]/I$ and $K[X']/I'$ are isomorphic and have the same depth. By polarizing f_i' with respect to

$$X_{I'} = \cup_{i=1}^{n} \{x_{i,2}, \ldots, x_{i,\delta_i}\}$$

we obtain that $(f_i')^{\mathrm{pol}}$ is equal to f_i^{pol}, the polarization of f_i with respect to X_L. The full polarization of I' is $(I')^{\mathrm{pol}} = ((f_1')^{\mathrm{pol}}, \ldots, (f_r')^{\mathrm{pol}})$. Therefore, by Lemma 6.10, one has

$$\operatorname{depth}(R[X_L]/(f_1^{\mathrm{pol}}, \ldots, f_r^{\mathrm{pol}})) = \operatorname{depth}(R[X_L]/((f_1')^{\mathrm{pol}}, \ldots, (f_r')^{\mathrm{pol}})), \tag{6.1.3}$$

$$\operatorname{depth}(R'[X_{I'}]/((f_1')^{\mathrm{pol}},\ldots,(f_r')^{\mathrm{pol}})) = |X_{I'}| + \operatorname{depth}(R'/I') = |X_{I'}| + \operatorname{depth}(R/I) \tag{6.1.4}$$

As $|X \cup X_L| = \sum_{i=1}^{k} a_i + \sum_{i=k+1}^{n} \delta_i$ and $|X' \cup X_{I'}| = \sum_{i=1}^{n} \delta_i$, we get

$$|(X \cup X_L) \setminus (X' \cup X_{I'})| = \sum_{i=1}^{k} (a_i - \delta_i),$$

that is, the number of variables of $R[X_L]$ that do not occur in $R'[X_{I'}]$ is $\sum_{i=1}^{k}(a_i - \delta_i)$. Therefore from Eqs. (6.1.3) and (6.1.4), and using that $|X_{I'}| = \sum_{i=1}^{n}(\delta_i - 1)$, we get

$$\begin{aligned} \operatorname{depth}(R[X_L]/(f_1^{\mathrm{pol}},\ldots,f_r^{\mathrm{pol}})) &= \sum_{i=1}^{k}(a_i - \delta_i) + \operatorname{depth}(R'[X_{I'}]/((f_1')^{\mathrm{pol}},\ldots,(f_r')^{\mathrm{pol}})) \\ &= \sum_{i=1}^{k}(a_i - 1) + \sum_{i=k+1}^{n}(\delta_i - 1) + \operatorname{depth}(R/I). \end{aligned} \tag{6.1.5}$$

Using Eqs. (6.1.2) and (6.1.5) the required equality follows.

Subcase (i.b): $a_i \leq \delta_i$ for all i. This case follows adapting the arguments of Subcase (i.a), noting that $k = 0$ in this case.

(ii): To prove this part we keep the notation of part (i).

Subcase (ii.a): Assume that $a_i > \delta_i$ for some i. The first equality follows at once from Lemma 6.10. As $R'[X_{I'}]$ is a subring of $R[X_L]$, the regularity of $(I')^{\mathrm{pol}}R'[X_{I'}]$ is equal to that of $(I')^{\mathrm{pol}}R[X_L]$. Hence, by Lemma 6.10, we get

$$\operatorname{reg}(R[X_L]/(I')^{\mathrm{pol}}) = \operatorname{reg}(R'[X_{I'}]/(I')^{\mathrm{pol}}) = \operatorname{reg}(R'/I') = \operatorname{reg}(R/I).$$

Subcase (ii.b): $a_i \leq \delta_i$ for all i. This case follows adapting the arguments of Subcase (ii.a). ♠

The following corollary extends Proposition 6.8 and Remark 6.9 from squarefree monomial ideals to arbitrary monomial ideals using polarization. It will be used throughout the thesis (e.g., Lemma 6.20, Theorem 6.34, Proposition 6.40). This result is later extended using Gröbner bases (Corollary 6.13).

COROLLARY 6.12. *Let $I \subset R$ be a monomial ideal, let f be a monomial of degree k, and let $x_{i_1},\ldots,x_{i_k}$ be a set of distinct variables of R. The following hold.*

(i) $\operatorname{depth}(R/(f,I)) \geq \operatorname{depth}(R/I) - 1$.

(ii) [**CHH$^+$17**, Theorem 3.1] $\operatorname{depth}(R/I) \leq \operatorname{depth}(R/(I\colon f))$.

(iii) $\operatorname{depth}(R/(x_{i_1},\ldots,x_{i_k},I)) \geq \operatorname{depth}(R/I) - k$.

(iv) [**CHH$^+$17**, Theorem 3.1] $\operatorname{reg}(R/I) \geq \operatorname{reg}(R/(I\colon f))$.

(v) $\operatorname{reg}(R/(f,I)) \leq \operatorname{reg}(R/I) + k - 1$.

(vi) $\operatorname{depth}(R/I) = \operatorname{depth}(R/(I\colon f))$ *or* $\operatorname{depth}(R/I) = \operatorname{depth}(R/(f,I))$.

(vii) **[CHH$^+$17, DHS13]** *If* $k = 1$, *then* $\operatorname{reg}(R/I) = \operatorname{reg}(R/(I\colon f)) + 1$ *or* $\operatorname{reg}(R/I) = \operatorname{reg}(R/(f,I))$.

PROOF. If I and f are squarefree, the result holds true. Indeed, by Lemma 6.2, one has the inequality $\operatorname{depth}(R/(I\colon f)) \geq \operatorname{depth}(R/I)$. Then by Proposition 6.8 and Remark 6.9 the statements all hold. To show the general case we will use the polarization technique.

(i) One may assume that $f \notin I$. We set $G(I) = \{f_1, \ldots, f_r\}$ and $L = (f, I)$. Let X_L be the set of new variables needed to polarize L and let f^{pol}, f_i^{pol} be the polarizations in $R[X_L]$ of f, f_i, respectively. As these polarizations are squarefree, by Proposition 6.8 one has

$$\operatorname{depth}(R[X_L]/(f^{\mathrm{pol}}, f_1^{\mathrm{pol}}, \ldots, f_r^{\mathrm{pol}})) \geq \operatorname{depth}(R[X_L]/(f_1^{\mathrm{pol}}, \ldots, f_r^{\mathrm{pol}})) - 1,$$

where $L^{\mathrm{pol}} = (f^{\mathrm{pol}}, f_1^{\mathrm{pol}}, \ldots, f_r^{\mathrm{pol}})$. Hence, by Proposition 6.11,

$$\operatorname{depth}(R/L) \geq \operatorname{depth}(R/I) - 1.$$

(ii): According to Lemma 6.3 parts (ii) and (i) are equivalent.

(iii): It follows from part (i) using induction on k.

(iv)–(v): Setting $N = (R/(I\colon f))[-k]$, $M = R/I$ and $L = R/(I, f)$, and noticing that $\operatorname{reg}(N) = k + \operatorname{reg}(R/(I\colon f))$, from Lemma 6.5 it follows that (iv) and (v) are equivalent. Since $f^{\mathrm{pol}}, f_1^{\mathrm{pol}}, \ldots, f_r^{\mathrm{pol}}$ are squarefree, by Proposition 6.8 one has

$$\operatorname{reg}(R[X_L]/L^{\mathrm{pol}}) - \operatorname{reg}(R[X_L]/(f_1^{\mathrm{pol}}, \ldots, f_r^{\mathrm{pol}})) \leq k - 1.$$

Hence, by Proposition 6.11, one has $\operatorname{reg}(R/L) - \operatorname{reg}(R/I) \leq k - 1$. Thus (v) and (iv) hold.

(vi): This condition is equivalent to (i). This follows applying Lemma 6.3 to the exact sequence

$$0 \longrightarrow R/(I\colon f)[-k] \xrightarrow{f} R/I \longrightarrow R/(I, f) \longrightarrow 0.$$

(vii): Recall that $\operatorname{reg}(R/(I\colon f))[-k] = k + \operatorname{reg}(R/(I\colon f))$. If $k = 1$, using Lemma 6.4 it follows that conditions (vii) and (iv) are equivalent. ♠

COROLLARY 6.13. *Let* $I \subset R$ *be a monomial ideal and let* f *be a homogeneous polynomial of degree* k. *If there exists a monomial order* $\prec$ *on* R *such that*

$$\operatorname{in}_\prec(I, f) = I + (\operatorname{in}_\prec(f)),$$

then

(a) $\operatorname{depth}(R/(I\colon f)) \geq \operatorname{depth}(R/I)$,

(b) $\operatorname{reg}(R/(I, f)) \leq \operatorname{reg}(R/I) + k - 1$.

(c) $\operatorname{reg}(R/I) \geq \operatorname{reg}(R/(I\colon f))$.

PROOF. (a): Assume that $\operatorname{depth}(R/I) > \operatorname{depth}(R/(I\colon f))$. From the exact sequence

$$0 \longrightarrow R/(I\colon f)[-k] \xrightarrow{f} R/I \longrightarrow R/(I,f) \longrightarrow 0,$$

using the depth lemma [**Vil15**, Lemma 2.3.9] and the fact that the depth of $R/(I,f)$ is greater than or equal to the depth of $R/\operatorname{in}_{\prec}(I,f)$ [**HH11**, Theorem 3.3.4(d)], we get

$$\operatorname{depth}(R/(I\colon f)) = \operatorname{depth}(R/(I,f)) + 1 \geq \operatorname{depth}(R/(I+\operatorname{in}_{\prec}(f))) + 1.$$

By Corollary 6.12(i), we have $\operatorname{depth}(R/(I+\operatorname{in}_{\prec}(f))) \geq \operatorname{depth}(R/I) - 1$. Hence we obtain $\operatorname{depth}(R/(I\colon f)) \geq \operatorname{depth}(R/I)$, a contradiction.

(b): Using that the regularity of $R/(I,f)$ is less than or equal to the regularity of $R/\operatorname{in}_{\prec}(I,f)$ [**HH11**, Theorem 3.3.4(c)] and Corollary 6.12(v), we get

$$\operatorname{reg}(R/(I,f)) \leq \operatorname{reg}(R/\operatorname{in}_{\prec}(I,f)) = \operatorname{reg}(R/(I+\operatorname{in}_{\prec}(f))) \leq \operatorname{reg}(R/I) + k - 1.$$

(c): Setting $N = R/(I\colon f)[-k]$, $M = R/I$, and $L = R/(I,f)$. If $\operatorname{reg}(R/(I\colon f)) > \operatorname{reg}(R/I)$, that is, $\operatorname{reg}(N) \geq \operatorname{reg}(M) + k + 1$. On the other hand, by part (b), one has $\operatorname{reg}(L) \leq \operatorname{reg}(N) - 2$. According to [**Eis13**, Corollary 20.19](a), one has either $\operatorname{reg}(N) \leq \operatorname{reg}(M)$ or $\operatorname{reg}(N) \leq \operatorname{reg}(L) + 1$, a contradiction. ♠

The next example illustrates the polarizations used in the proof of Proposition 6.11. For convenience we use the notation of that proof.

EXAMPLE 6.14. Let $f = x_1^3x_2^3$, $f_1 = x_1^2x_3$, $f_2 = x_1x_3^2$, $f_3 = x_2^2x_3$ be monomials in the polynomial ring $R = K[x_1, x_2, x_3]$ and set $I = (f_1, f_2, f_3)$ and $L = (f, I)$. Setting

$$f^{\mathrm{pol}} = x_{1,2}x_{1,3}x_1x_{2,2}x_{2,3}x_2,\ f_1^{\mathrm{pol}} = x_{1,2}x_{1,3}x_{3,2},\ f_2^{\mathrm{pol}} = x_{1,2}x_{3,2}x_3,\ f_3^{\mathrm{pol}} = x_{2,2}x_{2,3}x_{3,2},$$

and $X_L = \{x_{1,2}, x_{1,3}\} \cup \{x_{2,2}, x_{2,3}\} \cup \{x_{3,2}\}$, the full polarization of L is

$$L^{\mathrm{pol}} = (f^{\mathrm{pol}}, f_1^{\mathrm{pol}}, f_2^{\mathrm{pol}}, f_3^{\mathrm{pol}}) \subset R[X_L].$$

Making the change of variables $x_1 \to x_{1,3}$, $x_2 \to x_{2,3}$ in I and setting

$$f_1' = x_{1,3}^2x_3,\ f_2' = x_{1,3}x_3^2,\ f_3' = x_{2,3}^2x_3,\ I' = (f_1', f_2', f_3'),$$

$X_{I'} = \{x_{1,2}\} \cup \{x_{2,2}\} \cup \{x_{3,2}\}$, $R' = K[x_{1,3}, x_{2,3}, x_3]$, the full polarization of I' is

$$(I')^{\mathrm{pol}} = ((f_1')^{\mathrm{pol}}, (f_2')^{\mathrm{pol}}, (f_3')^{\mathrm{pol}}) \subset R'[X_{I'}],$$

where $(f_1')^{\mathrm{pol}} = x_{1,2}x_{1,3}x_{3,2}$, $(f_2')^{\mathrm{pol}} = x_{1,2}x_{3,2}x_3$, $(f_3')^{\mathrm{pol}} = x_{2,2}x_{2,3}x_{3,2}$. Thus f_i^{pol} is equal to $(f_i')^{\mathrm{pol}}$ for $i = 1, 2, 3$. Setting $X_I = \{x_{1,2}, x_{2,2}, x_{3,2}\}$ the full polarization of I is generated by the monomials $x_{1,2}x_1x_{3,2}$, $x_{1,2}x_{3,2}x_3$, $x_{2,2}x_2x_{3,2}$.

6.2. Depth and regularity locally at each variable

In this section we use polarization to study the behavior of the depth and regularity of a monomial ideal locally at each variable when lowering the top degree.

Let $R = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K, let I be a monomial ideal of R and let x_i be a fixed variable that occurs in $G(I)$. Given a monomial $x^a = x_1^{a_1} \cdots x_n^{a_n}$, we set $\deg_{x_i}(x^a) = a_i$. Consider the integer

$$q := \max\{\deg_{x_i}(x^a) |\, x^a \in G(I)\},$$

and the corresponding set $\mathcal{B}_i := \{x^a |\, \deg_{x_i}(x^a) = q\} \cap G(I)$. That is, $\mathcal{B}_i$ is the set of all monomial of $G(I)$ of highest degree in x_i. Setting

$$\mathcal{A}_i := \{x^a |\, \deg_{x_i}(x^a) < q\} \cap G(I) = G(I) \setminus \mathcal{B}_i,$$

$p := \max\{\deg_{x_i}(x^a) |\, x^a \in \mathcal{A}_i\}$ and $L := (\{x^a/x_i |\, x^a \in \mathcal{B}_i\} \cup \mathcal{A}_i\})$, we are interested in comparing the depth (resp. regularity) of R/I with the depth (resp. regularity) of R/L.

One of the main results of this section shows that the depth is locally non-decreasing at each variable x_i when lowering the top degree:

THEOREM 6.15. *Let I be a monomial ideal of R and let x_i be a variable. The following hold.*

(a) If $p \geq 1$ and $q - p \geq 2$, then $\operatorname{depth}(R/I) = \operatorname{depth}(R/L)$.
(b) If $p \geq 0$ and $q - p = 1$, then $\operatorname{depth}(R/L) \geq \operatorname{depth}(R/I)$.
(c) If $p = 0$ and $q \geq 2$, then

$$\operatorname{depth}(R/I) = \operatorname{depth}(R/(\{x^a/x_i^{q-1} |\, x^a \in \mathcal{B}_i\} \cup \mathcal{A}_i\})).$$

PROOF. (a): By simplicity set $i = 1$. We may assume that $G(I) = \{f_1, \ldots, f_r\}$, where $f_1, \ldots, f_m$ is the set of all elements of $G(I)$ that contain x_1^q and $f_{m+1}, \ldots, f_s$ is the set of all elements of $G(I)$ that contain some positive power x_1^ℓ of x_1 for some $1 \leq \ell < q$. Making a partial polarization of x_1^q with respect to the new variables $x_{1,2}, \ldots, x_{1,q-1}$ **[Vil15**, p. 203], gives that f_j polarizes to $f_j^{\text{pol}} = x_{1,2} \cdots x_{1,q-1} x_1^2 f_j'$ for $j = 1, \ldots, m$, where $f_1', \ldots, f_m'$ are monomials that do not contain x_1 and $f_j = x_1^q f_j'$ for $j = 1, \ldots, m$. Hence, using that $q - p \geq 2$, one has the partial polarization

$$I^{\text{pol}} = (x_{1,2} \cdots x_{1,q-1} x_1^2 f_1', \ldots, x_{1,2} \cdots x_{1,q-1} x_1^2 f_m', f_{m+1}^{\text{pol}}, \ldots, f_s^{\text{pol}}, f_{s+1}, \ldots, f_r),$$

where $f_{m+1}^{\text{pol}}, \ldots, f_s^{\text{pol}}$ do not contain x_1 and I^{pol} is an ideal of $R^{\text{pol}} = R[x_{1,2}, \ldots, x_{1,q-1}]$. On the other hand, from the equality

$$G(L) = \{f_1/x_1, \ldots, f_m/x_1, f_{m+1}, \ldots, f_r\},$$

one has the partial polarization

$$L^{\mathrm{pol}} = (x_{1,2}\cdots x_{1,q-1}x_1f_1', \ldots, x_{1,2}\cdots x_{1,q-1}x_1f_m', f_{m+1}^{\mathrm{pol}}, \ldots, f_s^{\mathrm{pol}}, f_{s+1}, \ldots, f_r).$$

By making the substitution $x_1^2 \to x_1$ in each element of $G(I^{\mathrm{pol}})$ this will not affect the depth of $R^{\mathrm{pol}}/I^{\mathrm{pol}}$ (see [**NPV14**, Lemmas 3.3 and 3.5]). Thus

$$q - 2 + \operatorname{depth}(R/I) = \operatorname{depth}(R^{\mathrm{pol}}/I^{\mathrm{pol}}) = \operatorname{depth}(R^{\mathrm{pol}}/L^{\mathrm{pol}}) = q - 2 + \operatorname{depth}(R/L),$$

and consequently $\operatorname{depth}(R/I) = \operatorname{depth}(R/L)$.

(b): To simplify notation we set $i = 1$. Assume $p = 0$, then $q = 1$. Note that the ring R/L is equal to $R/(I\colon x_1)$. Hence, by Corollary 6.12, its depth is greater than or equal to $\operatorname{depth}(R/I)$. Thus we may assume that $p \geq 1$. We may also assume that $G(I) = \{f_1, \ldots, f_r\}$, where $f_1, \ldots, f_m$ is the set of all elements of $G(I)$ that contain x_1^q, and $f_{m+1}, \ldots, f_t$ is the set of all elements of $G(I)$ that contain x_1^{q-1} but not x_1^q, and $f_{t+1}, \ldots, f_s$ is the set of all elements of $G(I)$ that contain some power x_1^ℓ, with $1 \leq \ell < q-1$, but not $x_1^{\ell+1}$. Let R' be the polynomial ring $K[x_{1,q}, x_2, \ldots, x_n]$, with $x_{1,q}$ a new variable, and let L' be the ideal of R' obtained from L by making the change of variable $x_1 \to x_{1,q}$ in each element of $G(L)$. Clearly

$$\operatorname{depth}(R/L) = \operatorname{depth}(R'/L') = \operatorname{depth}(R'[x_1]/L') - 1.$$

The partial polarization of I with respect to x_1 using the variables $x_{1,2}, \ldots, x_{1,q}$ is given by

$$\begin{aligned} I^{\mathrm{pol}} = (&x_{1,2}\cdots x_{1,q}x_1f_1', \ldots, x_{1,2}\cdots x_{1,q}x_1f_m',\\ &x_{1,2}\cdots x_{1,q}f_{m+1}', \ldots, x_{1,2}\cdots x_{1,q}f_t',\\ &f_{t+1}^{\mathrm{pol}}, \ldots, f_s^{\mathrm{pol}}, f_{s+1}, \ldots, f_r), \end{aligned}$$

where $f_1', \ldots, f_t', f_{t+1}^{\mathrm{pol}}, \ldots, f_s^{\mathrm{pol}}, f_{s+1}, \ldots, f_r$ do not contain x_1 and I^{pol} is an ideal of the ring $R^{\mathrm{pol}} = R[x_{1,2}, \ldots, x_{1,q}]$. Therefore

$$\begin{aligned} (I^{\mathrm{pol}}\colon x_1) = (&x_{1,2}\cdots x_{1,q}f_1', \ldots, x_{1,2}\cdots x_{1,q}f_m',\\ &x_{1,2}\cdots x_{1,q}f_{m+1}', \ldots, x_{1,2}\cdots x_{1,q}f_t', f_{t+1}^{\mathrm{pol}}, \ldots, f_s^{\mathrm{pol}}, f_{s+1}, \ldots, f_r). \end{aligned}$$

The following is a generating set for L', which is not necessarily minimal:

$$\begin{aligned} L' = (&x_{1,q}^{q-1}f_1', \ldots, x_{1,q}^{q-1}f_m', x_{1,q}^{q-1}f_{m+1}', \ldots, x_{1,q}^{q-1}f_t',\\ &x_{1,q}^{a_{t+1}}f_{t+1}', \ldots, x_{1,q}^{a_s}f_s', f_{s+1}, \ldots, f_r), \end{aligned}$$

where $1 \leq a_i < q-1$ for $i = t+1, \ldots, s$. Hence, it is seen that, $(I^{\mathrm{pol}} \colon x_1)$ is equal to $(L')^{\mathrm{pol}}$, the polarization of L' with respect to the variable $x_{1,q}$ using the variables $x_{1,2}, \ldots, x_{1,q-1}$. Therefore, using Lemma 6.2, we get

$$\begin{aligned}(q-1) + \operatorname{depth}(R/L) &= 1 + ((q-2) + \operatorname{depth}(R'/L')) \\ &= 1 + \operatorname{depth}((R')^{\mathrm{pol}}/(L')^{\mathrm{pol}}) = \operatorname{depth}((R'[x_1])^{\mathrm{pol}}/(L')^{\mathrm{pol}}) \\ &= \operatorname{depth}(R^{\mathrm{pol}}/(L')^{\mathrm{pol}}) = \operatorname{depth}(R^{\mathrm{pol}}/(I^{\mathrm{pol}} \colon x_1)) \\ &\geq \operatorname{depth}(R^{\mathrm{pol}}/I^{\mathrm{pol}}) = (q-1) + \operatorname{depth}(R/I).\end{aligned}$$

Thus $\operatorname{depth}(R/L) \geq \operatorname{depth}(R/I)$.

(c): It suffices to notice that by making the substitution $x_i^q \to x_i$ in each element of $G(I)$ this will not affect the depth of R/I (see [**NPV14**, Lemmas 3.3 and 3.5]). ♠

Let $\mathcal{D}$ be a *vertex-weighted digraph*, that is, $\mathcal{D}$ is a finite set $V(\mathcal{D}) = \{x_1, \ldots, x_n\}$ of vertices, a prescribed collection $E(\mathcal{D})$ of ordered pairs of distinct points called *edges* or *arrows*, and $\mathcal{D}$ is endowed with a function $d \colon V(\mathcal{D}) \to \mathbb{N}_+$, where $\mathbb{N}_+$ is the set $\{1, 2, \ldots\}$. The weight $d(x_i)$ of x_i is denoted simply by d_i. The *edge ideal* of $\mathcal{D}$, denoted $I(\mathcal{D})$, is the ideal of R given by

$$I(\mathcal{D}) := (x_i x_j^{d_j} \mid (x_i, x_j) \in E(\mathcal{D})).$$

Edge ideals of vertex-weighted digraphs occur in the theory of Reed-Muller-type codes as initial ideals of vanishing ideals of projective spaces over a finite field [**MBPV17, Sor91**].

COROLLARY 6.16. [**GMBS$^+$17**, Corollary 6] *Let $I = I(\mathcal{D})$ be the edge ideal of a vertex-weighted digraph with vertices $x_1, \ldots, x_n$ and let d_i be the weight of x_i. If $\mathcal{U}$ is the digraph obtained from $\mathcal{D}$ by assigning weight 2 to every vertex x_i with $d_i \geq 2$, then I is Cohen–Macaulay if and only if $I(\mathcal{U})$ is Cohen–Macaulay.*

PROOF. By applying Theorem 6.15 to each vertex x_i of $\mathcal{D}$ of weight at least 3, we obtain that the depth of $R/I(\mathcal{D})$ is equal to the depth of $R/I(\mathcal{U})$. Since $I(\mathcal{D})$ and $I(\mathcal{U})$ have the same height, then $I(\mathcal{D})$ is Cohen-Macaulay if and only if $I(\mathcal{U})$ is Cohen–Macaulay. ♠

COROLLARY 6.17. [**HTT05**] *If I is a monomial ideal, then*

$$\operatorname{depth}(R/\operatorname{rad}(I)) \geq \operatorname{depth}(R/I).$$

In particular if I is Cohen–Macaulay, then $\operatorname{rad}(I)$ is Cohen–Macaulay.

PROOF. It follows by applying Theorem 6.15 to every vertex x_i as many times as necessary. ♠

As a consequence if I is squarefree, then $\operatorname{depth}(R/I) \geq \operatorname{depth}(R/I^k)$ for all $k \geq 1$.

REMARK 6.18. Let $L \subset R$ be a monomial ideal. If x_i^k is in $G(L)$ for some $k \geq 1$, $1 \leq i \leq n$ and L' is the ideal of R generated by all elements of $G(I)$ that do not contain x_i, then $(L, x_i) = (L', x_i)$ and by a repeated application of Theorem 6.15 one has

$$\operatorname{depth}(R/L) \leq \operatorname{depth}(R/(L', x_i)) = \operatorname{depth}(R/L') - 1.$$

Before proving an analog of Theorem 6.15 for regularity, we first provide a basic fact regarding the effect of a change of variables on the resolution of an ideal.

LEMMA 6.19. *Let I be a homogeneous ideal of R, let d_1 be a positive integer, and define $\phi\colon R \to R$ by $\phi(x_1) = x_1^{d_1}$ and $\phi(x_i) = x_i$ for $2 \leq i \leq n$. If $\phi(I)$ is homogeneous, then a minimal resolution of $\phi(I)$ over R can be obtained by applying ϕ to a minimal resolution of I. Moreover, the (non-graded) Betti numbers of I and $\phi(I)$ will be equal and* $\operatorname{reg}(\phi(I)) \geq \operatorname{reg} I$.

PROOF. Define $S = K[x_1, \ldots, x_n]$ to be a polynomial ring with the non-standard grading $d(x_1) = d_1$ and $d(x_i) = 1$ for $2 \leq i \leq n$. Note that the map ϕ factors through S. Write $\phi = \psi\sigma$, where $\sigma\colon R \to S$ is given by $\sigma(x_i) = x_i$ for all i and $\psi\colon S \to R$ is given by $\psi(x_1) = x_1^{d_1}$ and $\psi(x_i) = x_i$ for $2 \leq i \leq n$. Then, by assumption, I is a homogeneous ideal of R and $\sigma(I)$ is again homogeneous in S. Applying σ to a minimal resolution of I yields a minimal resolution of $\sigma(I)$, where the modules and maps are unchanged except that the degrees of some of the maps, and thus the shifts in the resolution, may have increased, showing $\operatorname{reg}(\sigma(I)) \geq \operatorname{reg}(I)$. Now the map ψ is precisely the map used in [**NPV14**, Lemma 3.5 and Theorem 3.6(b)]. The result follows from combining these results. ♠

LEMMA 6.20. *Let I and J be monomial ideals of R and let x_i be a variable. Suppose that $(I\colon x_i) = J$ and $(I, x_i) = (J, x_i)$, then*

(i) $\operatorname{reg}(R/J) \leq \operatorname{reg}(R/I) \leq \operatorname{reg}(R/J) + 1$.
(ii) $\operatorname{depth}(R/J) - 1 \leq \operatorname{depth}(R/I) \leq \operatorname{depth}(R/J)$.

PROOF. (i): By Corollary 6.12(v), we have $\operatorname{reg}(R/(I, x_i)) \leq \operatorname{reg}(R/I)$ and $\operatorname{reg}(R/(J, x_i)) \leq \operatorname{reg}(R/J)$, and by Corollary 6.12(vii), we have either

$$\operatorname{reg}(R/I) = \operatorname{reg}(R/(I\colon x_i)) + 1 = \operatorname{reg}(R/J) + 1$$

or

$$\operatorname{reg}(R/I) = \operatorname{reg}(R/(I, x_i)) = \operatorname{reg}(R/(J, x_i)) \leq \operatorname{reg}(R/J).$$

In the latter case one has $\operatorname{reg}(R/I) = \operatorname{reg}(R/J)$ because by Corollary 6.12(iv), one has $\operatorname{reg}(R/J) \leq \operatorname{reg}(R/I)$. Combining these facts we obtain

$$\operatorname{reg}(R/J) \leq \operatorname{reg}(R/I) \leq \operatorname{reg}(R/J) + 1.$$

(ii): Similarly by Corollary 6.12(vi), we have either $\operatorname{depth}(R/I) = \operatorname{depth}(R/J)$ or $\operatorname{depth}(R/I) = \operatorname{depth}(R/(I, x_i))$. In the latter case one has

$$\begin{aligned} \operatorname{depth}(R/J) &\geq \operatorname{depth}(R/I) \\ &= \operatorname{depth}(R/(I, x_i)) \\ &= \operatorname{depth}(R/(J, x_i)) \\ &\geq \operatorname{depth}(R/J) - 1. \end{aligned}$$

because by parts (ii) and (i) of Corollary 6.12 we have $\operatorname{depth}(R/J) \geq \operatorname{depth}(R/I)$ and $\operatorname{depth}(R/(J, x_i)) \geq \operatorname{depth}(R/J) - 1$, respectively. ♠

Using the notation introduced for Theorem 6.15 we are now able to control regularity when lowering the degrees of the generators of a monomial ideal.

THEOREM 6.21. *Let I be a monomial ideal and consider the ideal L' define by $(\{x^a/x_i^{q-1} \mid x^a \in \mathcal{B}_i\} \cup \mathcal{A}_i\})$, where x_i is a variable. The following hold.*

(a) If $p \geq 1$ and $q - p \geq 2$, then $\operatorname{reg}(R/L) \leq \operatorname{reg}(R/I) \leq \operatorname{reg}(R/L) + 1$.
(b) If $p \geq 0$ and $q - p = 1$, then $\operatorname{reg}(R/L) \leq \operatorname{reg}(R/I)$.
(c) If $p = 0$ and $q \geq 2$, then $\operatorname{reg}(R/L') \leq \operatorname{reg}(R/I) \leq \operatorname{reg}(R/L') + q - 1$.

PROOF. (a): As in Theorem 6.15, we assume $i = 1$. Forming a partial polarization of x_1^q with respect to new variables $x_{1,2}, \ldots, x_{1,q-1}$ will not change the regularity by Lemma 6.10 (d). By the same argument, forming a full polarization of $x_2, \ldots, x_n$ will also not change the regularity. Thus we may assume that $I = (x_1^2 h_1, \ldots, x_1^2 h_m, h_{m+1}, \ldots, h_r)$ and $L = (x_1 h_1, \ldots, x_1 h_m, h_{m+1}, \ldots, h_r)$ where h_j are squarefree monomials and x_1 does not divide h_j for all j. Also, note that $(I, x_1) = (L, x_1)$ and $(I \colon x_1) = L$. Thus, by Lemma 6.20, $\operatorname{reg}(R/I) = \operatorname{reg}(R/L) + 1$ or $\operatorname{reg}(R/I) = \operatorname{reg}(R/L)$ as claimed.

(b): This part follows from the proof of Theorem 6.15(b) and Lemma 6.10(d).

(c): We proceed by induction on $q \geq 2$. There are monomials $h_1, \ldots, h_r$ not containing x_1 such that

$$I = (x_1^q h_1, \ldots, x_1^q h_m, h_{m+1}, \ldots, h_r) \text{ and } L = (x_1^{q-1} h_1, \ldots, x_1^{q-1} h_m, h_{m+1}, \ldots, h_r).$$

Note that $(I, x_1) = (L, x_1)$ and $L = (I\colon x_1)$. Then, applying Lemma 6.20 to I and L, one has $\operatorname{reg}(R/L) \leq \operatorname{reg}(R/I) \leq \operatorname{reg}(R/L) + 1$. In particular the required inequality holds for $q = 2$. If $q > 3$, applying induction to L, the inequality follows. ♠

COROLLARY 6.22. *Let I be a monomial ideal of R and let J be its radical. The following hold.*

(i) **[Rav90]** $\operatorname{reg}(R/J) \leq \operatorname{reg}(R/I)$.

(ii) *If I is Cohen–Macaulay, then $a(R/J) \leq a(R/I)$, where $a(\cdot)$ is the a-invariant.*

PROOF. (i): It follows by applying Theorem 6.21 to every vertex x_i as many times as necessary.

(ii): By Corollary 6.17, J is Cohen–Macaulay. Hence, by **[Vas04]**, one has $a(M) = \operatorname{reg}(M) - \operatorname{depth}(M)$ for $M = R/I$ and $M = R/J$. As

$$\dim(R/I) = \dim(R/J) = \operatorname{depth}(R/I) = \operatorname{depth}(R/J),$$

the inequality follows from part (i). ♠

REMARK 6.23. Let $I \subset R$ be a monomial ideal and let f be a monomial which is a non-zero divisor of R/I. Then $\operatorname{reg}(R/fI) = \operatorname{reg}(R/I) + \deg(f)$ and $\operatorname{reg}(R/(I, f)) = \operatorname{reg}(R/I) + \deg(f) - 1$. This follows from Proposition 6.43. Thus the upper bound of Theorem 6.21(c) is tight.

EXAMPLE 6.24. The ideals $I = (x_1^2x_2x_3^2, x_3^2x_4, x_4^3x_5)$ and $J = (x_1x_2x_3^2, x_3^2x_4, x_4^3x_5)$ have regularity 5. Thus the lower bound of Theorem 6.21(c) is also tight.

EXAMPLE 6.25. $I = (x_1^7x_2x_3^2, x_1^7x_5^3, x_1^6x_3^2x_4, x_2x_5^7)$, $L = (x_1^6x_2x_3^2, x_1^6x_5^3, x_1^6x_3^2x_4, x_2x_5^7)$ have regularity 16 and 13, respectively. Thus in Theorem 6.21(b), $\operatorname{reg}(R/L) + 1$ is not an upper bound for $\operatorname{reg}(R/I)$.

6.3. Edge ideals of clutters with non increasing depth

Let $\mathcal{C}$ be a clutter with vertex set $X = \{x_1, \ldots, x_n\}$ and let $\{x^{v_1}, \ldots, x^{v_r}\}$ be the minimal generating set of $I(\mathcal{C})$. The matrix A whose column vectors are $v_1^\top, \ldots, v_r^\top$ is called the *incidence matrix* of $\mathcal{C}$. The *set covering polyhedron* of $\mathcal{C}$ is given by:

$$\mathcal{Q}(A) := \{x \in \mathbb{R}^n \,|\, x \geq 0;\, xA \geq \mathbf{1}\},$$

where $\mathbf{1} = (1, \ldots, 1)$. The rational polyhedron $\mathcal{Q}(A)$ is called *integral* if it has only integral vertices. A clutter is called *uniform* (resp. *unmixed*) if all its edges (resp. minimal vertex covers) have the same cardinality. A clutter is *ideal* if its set covering polyhedron is integral **[Cor01]**.

DEFINITION 6.26. A clutter $\mathcal{C}$, with incidence matrix A, has the *max-flow min-cut* (MFMC) property if both sides of the LP-duality equation

$$\min\{\langle \alpha, x\rangle |\, x \geq 0; xA \geq \mathbf{1}\} = \max\{\langle y, 1\rangle |\, y \geq 0; Ay \leq \alpha\} \tag{6.3.1}$$

have integral optimum solutions x, y for each nonnegative integral vector α.

DEFINITION 6.27. Let I be a squarefree monomial ideal of R and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be the associated primes of I. Given an integer $k \geq 1$, we define the k-th *symbolic power* of I to be the ideal

$$I^{(k)} := (I^k R_{\mathfrak{p}_i} \cap R) = \mathfrak{p}_1^k \cap \cdots \cap \mathfrak{p}_r^k.$$

An ideal I of R is called *normally torsion-free* if $\operatorname{Ass}(R/I^k)$ is contained in $\operatorname{Ass}(R/I)$ for all $k \geq 1$. Notice that if I is a squarefree monomial ideal, then I is normally torsion-free if and only if $I^k = I^{(k)}$ for all $k \geq 1$. A major result of **[GRV09, GVV07]** shows that a clutter $\mathcal{C}$ has the max-flow min-cut property if and only if $I(\mathcal{C})$ is normally torsion free.

LEMMA 6.28. (**[GRV09**, Lemma 5.6], **[DV11**, Lemma 2.1]) *If $\mathcal{C}$ is a uniform clutter and $\mathcal{Q}(A)$ is integral, then there exists a minimal vertex cover of $\mathcal{C}$ intersecting every edge of $\mathcal{C}$ in exactly one vertex.*

THEOREM 6.29. **[Cor01**, Theorem 1.17] *If $\mathcal{Q}(A)$ is integral and B is the incidence matrix of the clutter $\mathcal{C}^\vee$ of minimal vertex covers of $\mathcal{C}$, then $\mathcal{Q}(B)$ is integral.*

LEMMA 6.30. *If $\mathcal{C}$ is an unmixed clutter and $\mathcal{Q}(A)$ is integral, then there exists an edge of $\mathcal{C}$ intersecting every minimal vertex cover of $\mathcal{C}$ in exactly one vertex.*

PROOF. By duality **[Vil15**, Theorem 6.3.39] the minimal vertex covers of $\mathcal{C}^\vee$ (resp. edges of $\mathcal{C}^\vee$) are the edges of $\mathcal{C}$ (resp. minimal vertex covers of $\mathcal{C}$). Let B be the incidence matrix of $\mathcal{C}^\vee$. As $\mathcal{Q}(A)$ is integral and $\mathcal{C}$ is unmixed, by Lemma 6.29, $\mathcal{Q}(B)$ is also integral and $\mathcal{C}^\vee$ is uniform. Thus applying Lemma 6.28 to $\mathcal{C}^\vee$, there exists a minimal vertex cover of $\mathcal{C}^\vee$ intersecting every edge of $\mathcal{C}^\vee$ in exactly one vertex. Hence by duality the result follows. ♠

Let $I \subset R$ be a homogeneous ideal and let $\mathfrak{m} = (x_1, \ldots, x_n)$ be the maximal irrelevant ideal of R. Recall that the *analytic spread* of I, denoted by $\ell(I)$, is given by

$$\ell(I) = \dim R[It]/\mathfrak{m}R[It].$$

This number satisfies $\operatorname{ht}(I) \leq \ell(I) \leq \dim(R)$ **[Vas94**, Corollary 5.1.4].

THEOREM 6.31. **[Bur72, EH83]** $\inf_i\{\operatorname{depth}(R/I^i)\} \leq \dim(R) - \ell(I)$, *with equality if the associated graded ring $\operatorname{gr}_I(R)$ is Cohen–Macaulay.*

Brodmann [**Bro79**] improved this inequality by showing that $\operatorname{depth}(R/I^k)$ is constant for $k \gg 0$ and that this constant value is bounded from above by $\dim(R) - \ell(I)$. For a generalization of these results to other ideal filtrations see [**HH05a**, Theorem 1.1]. The constant value of $\operatorname{depth}(R/I^k)$ for $k \gg 0$ is called the *limit depth* of I and is denoted by $\lim_{k\to\infty} \operatorname{depth}(R/I^k)$.

DEFINITION 6.32. A homogeneous ideal $I \subset R$ has *non-increasing depth* if

$$\operatorname{depth}(R/I^k) \geq \operatorname{depth}(R/I^{k+1}) \; \forall \; k \geq 1,$$

and I has *non-decreasing regularity* if $\operatorname{reg}(R/I^k) \leq \operatorname{reg}(R/I^{k+1})$ for all $k \geq 1$. The ideal I has the *persistence property* if $\operatorname{Ass}(R/I^k) \subset \operatorname{Ass}(R/I^{k+1})$ for $k \geq 1$.

There are some classes of monomial ideals with non-increasing depth and non-decreasing regularity [**CHH$^+$17, CPSF$^+$15, Han17, HT$^+$17, SF18**]. A natural way to show these properties for a monomial ideal I is to prove the existence of a monomial f such that $(I^{k+1}\colon f) = I^k$ for $k \geq 1$. This was exploited in [**CHH$^+$17, MV12**] and in [**HM10**, Corollary 3.11] in connection to normally torsion-free ideals.

THEOREM 6.33. [**CHH$^+$17**, Theorem 5.1] *If $I(\mathcal{C})$ is the edge ideal of a clutter $\mathcal{C}$ which has a good leaf, then $I(\mathcal{C})$ has non-increasing depth and non-decreasing regularity.*

In particular edge ideals of forests or simplicial trees have non-increasing depth and non-decreasing regularity. Our next result gives another wide family of ideals with these properties.

THEOREM 6.34. *Let $\mathcal{C}$ be a clutter and let $I = I(\mathcal{C})$ be its edge ideal. If $\mathcal{C}$ is unmixed and satisfies the max-flow min-cut property, then*

(a) $\operatorname{depth}(R/I^k) \geq \operatorname{depth}(R/I^{k+1})$ *for* $k \geq 1$, *and*
(b) $\operatorname{reg}(R/I^k) \leq \operatorname{reg}(R/I^{k+1})$ *for* $k \geq 1$.

PROOF. Let $C_1, \ldots, C_s$ be the minimal vertex covers of $\mathcal{C}$. If $\mathfrak{p}_i$ is the ideal of R generated by C_i for $i = 1, \ldots, s$, then $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ are the minimal primes of I [**Vil15**, Theorem 6.3.39]. As $\mathcal{C}$ has the max-flow min-cut property, by [**Sch98**, Corollary 22.1c], $\mathcal{Q}(A)$ is integral. Therefore, by Lemma 6.30, there exists and edge e of $\mathcal{C}$ intersecting every C_i in exactly one vertex. Thus $|e \cap \mathfrak{p}_i| = 1$ for $i = 1, \ldots, s$. We claim that $(I^{k+1}\colon x_e) = I^k$ for $k \geq 1$, where $x_e = \prod_{x_i \in e} x_i$. The k-th symbolic power of I is given by

$$I^{(k)} = \mathfrak{p}_1^k \cap \cdots \cap \mathfrak{p}_s^k, \tag{6.3.2}$$

and by [**GVV07**, Corollary 3.14], $I^k = I^{(k)}$ for $k \geq 1$. Clearly I^k is contained in $(I^{k+1}\colon x_e)$ because x_e is in I. To show the other inclusion take x^a in $(I^{k+1}\colon x_e)$. Fix any $1 \leq i \leq s$.

Then $x^a x_e$ is in $I^{k+1} \subset \mathfrak{p}_i^{k+1}$. Thus there are $x_{j_1}, \ldots, x_{j_{k+1}}$ in $\mathfrak{p}_i$ with $j_1 \leq \cdots \leq j_{k+1}$ such that

$$x^a x_e = x_{j_1} \cdots x_{j_{k+1}} x^b,$$

for some x^b. Since $|e \cap \mathfrak{p}_i| = 1$ from this equality, we get that with one possible exception all variables that occur in x_e divide x^b. Thus $x^a \in \mathfrak{p}_i^k$. As i was an arbitrary fixed integer, using Eq. (6.3.2), we obtain $x^a \in I^{(k)} = I^k$. Thus $(I^{k+1} \colon x_e) = I^k$, as claimed. To prove parts (a) and (b) note that, by Corollary 6.12(ii), one has

$$\operatorname{depth}(R/I^k) = \operatorname{depth}(R/(I^{k+1} \colon x_e)) \geq \operatorname{depth}(R/I^{k+1}),$$

and by Corollary 6.12(iv), one has $\operatorname{reg}(R/I^k) = \operatorname{reg}(R/(I^{k+1} \colon x_e)) \leq \operatorname{reg}(R/I^{k+1})$. ♠

COROLLARY 6.35. *Let $\mathcal{C}$ be a clutter and let $J = I(\mathcal{C})^\vee$ be its ideal of covers. If $\mathcal{C}$ is uniform and its set covering polyhedron is integral, then*

(a) $\operatorname{depth}(R/J^{(k)}) \geq \operatorname{depth}(R/J^{(k+1)})$ *for* $k \geq 1$, *and*
(b) $\operatorname{reg}(R/J^{(k)}) \leq \operatorname{reg}(R/J^{(k+1)})$ *for* $k \geq 1$.

PROOF. This follows using duality and adapting the proof of Theorem 6.34. ♠

6.4. Edge ideals of graphs

Let G be a graph with vertex set $V(G) = \{x_1, \ldots, x_n\}$. A connected component of G with at least two vertices is called non-trivial. We denote the set of isolated vertices of G by $\operatorname{isol}(G)$ and the number of non-trivial bipartite components of G by $c_0(G)$. The *neighbor* set of x_i, denoted $N_G(x_i)$, is the set of all $x_j \in V(G)$ such that $\{x_i, x_j\}$ is an edge of G.

PROPOSITION 6.36. *Let $I(G)$ be the edge ideal of G. The following hold for $k \geq 1$ and $i = 1, \ldots, n$.*

(a) $\operatorname{depth}(R/(I(G)^k \colon x_i^k)) \leq \operatorname{depth}(R/(I(G \setminus N_G(x_i))^k, N_G(x_i)))$.
(b) **[Vil15**, p. 293] $(I(G) \colon x_i) = (I(G \setminus N_G(x_i)), N_G(x_i))$.
(c) $\dim(R) - \ell(I(G)) = |\operatorname{isol}(G)| + c_0(G)$.
(d) **[TT12**, Theorem 4.4(1)] $\lim_{k\to\infty} \operatorname{depth}(R/I(G)^k) = |\operatorname{isol}(G)| + c_0(G)$.
(e) *If $H = G \setminus N_G(x_i)$, then*

$$\lim_{k\to\infty} \operatorname{depth}(R/(I(H)^k, N_G(x_i))) = |\operatorname{isol}(H)| + c_0(H)$$

.

PROOF. (a): Clearly $x_j^k \in (I(G)^k \colon x_i^k)$ for $x_j \in N_G(x_i)$. Setting $H = G \setminus N_G(x_i)$, it is not hard to see that x_j^k is a minimal generator of the ideal $(I(G)^k \colon x_i^k)$ for $x_j \in N_G(x_i)$ and that

any minimal generator of $I(H)^k$ is a minimal generator of $(I(G)^k\colon x_i^k)$. The colon ideal $(I(G)^k\colon x_i^k)$ is minimally generated by

$$\{x_j^k \,|\, x_j \in N_G(x_i)\} \cup G(I(H)^k) \cup \{x^{\alpha_1}, \ldots, x^{\alpha_r}\},$$

for some monomials $x^{\alpha_1}, \ldots, x^{\alpha_r}$ such that each x^{α_i} contains at least one variable in $N_G(x_i)$. One has the equality

$$(N_G(x_i), (I(G)^k\colon x_i^k)) = (N_G(x_i), I(H)^k).$$

Therefore, starting with the ideal $(I(G)^k\colon x_i^k)$ and any variable x_j in $N_G(x_i)$, and successively applying Theorem 6.15, the required inequality follows.

(c): Let $G_1, \ldots, G_m$ be the non-trivial connected components of G. The analytic spread of $I(G_i)$ is $|V(G_i)|$ if G_i is non-bipartite and $|V(G_i)| - 1$ otherwise (see [**Vil15**, Corollary 10.1.21 and Proposition 14.2.12]). Hence the equality follows from the fact that the analytic spread is additive in the sense of [**MBMV12**, Lemma 3.4].

(e): This follows at once from part (d). ♠

LEMMA 6.37. *Let G be a bipartite graph with vertices $x_1, \ldots, x_n$, let $I(G)$ be its edge ideal, and let $k \geq 1$, $1 \leq i \leq n$ be integers. The following hold.*

(a) $(I(G)\colon x_i)^k = (I(G)\colon x_i)^{(k)}$.

(b) $(I(G)^k\colon x_i^k) = (I(G)\colon x_i)^k$.

PROOF. (a): The graph $G \setminus N_G(x_i)$ is bipartite. Hence, according to [**SVV94**, Theorem 5.9], the ideal $I(G \setminus N_G(x_i))$ is normally torsion-free and so is the ideal $(N_G(x_i))$ generated by $N_G(x_i)$. Therefore, by [**SVV94**, Corollary 5.6], the ideal $(I(G \setminus N_G(x_i)), N_G(x_i))$ is normally torsion-free. Thus it suffices to observe that $(I(G)\colon x_i)$ is equal to $(I(G \setminus N_G(x_i)), N_G(x_i))$ (see [**Vil15**, p. 293]).

(b): Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be the associated primes of $I(G)$. Since G is bipartite, its edge ideal is normally torsion-free [**SVV94**, Theorem 5.9]. Therefore, using part (a) and noticing that the primary decomposition of $(I(G)\colon x_i)$ is $\cap_{x_i \notin \mathfrak{p}_j} \mathfrak{p}_j$, we get

$$\begin{aligned}(I(G)^k\colon x_i^k) &= \left(\left(\bigcap_{j=1}^{s} \mathfrak{p}_j\right)^k\colon x_i^k\right) = \left(\left(\bigcap_{j=1}^{s} \mathfrak{p}_j^k\right)\colon x_i^k\right) = \bigcap_{x_i \notin \mathfrak{p}_j} \mathfrak{p}_j^k \\ &= (I(G)\colon x_i)^{(k)} = (I(G)\colon x_i)^k.\end{aligned}$$

♠

The regularity of powers of the cover ideal of a bipartite graph was studied in [**JNS18**] and the depth of symbolic powers of cover ideals of graphs was examined in [**KTT$^+$17,**

Fak17]. It is an open problem whether or not the edge ideal of a graph has non-increasing depth.

COROLLARY 6.38. *Let G be a bipartite graph. The following hold.*

(a) *If G is unmixed, then $I(G)$ has non-increasing depth.*
(b) ([**CPSF$^+$15**, Theorem 3.2], [**Han17**],[**HT$^+$17**, Corollary 2.4]) *$I(G)^\vee$ has non-increasing depth.*
(c) *$I(G)^\vee$ has non-decreasing regularity.*

PROOF. (a): By [**GRV09**, Theorem 4.6 and Proposition 4.27], the graph G has the max-flow min-cut property and since G is unmixed the result follows at once from Theorem 6.34.

(b)–(c): By [**GRV09**, Theorem 4.6 and Corollary 4.28], $G^\vee$ has the max-flow min-cut property, and $G^\vee$ is unmixed because its minimal vertex covers are the edges of G. Thus by Theorem 6.34 the ideal $I(G^\vee) = I(G)^\vee$ has non-increasing depth and non-decreasing regularity. ♠

The next interesting example is due to Kaiser, Stehlík, and Škrekovski [**KSŠ14**]. It shows that the Alexander dual of a graph does not always has the persistence property for associated primes. This example also shows that part (b) of Corollary 6.38 fails for non-bipartite graphs.

EXAMPLE 6.39. [**KSŠ14**] Let $J = I^\vee$ be the Alexander dual of the edge ideal

$$\begin{aligned} I = \ & (x_1x_2, x_2x_3, x_3x_4, x_4x_5, x_5x_6, x_6x_7, x_7x_8, x_8x_9, x_9x_{10}, x_1x_{10}, x_2x_{11}, x_8x_{11}, \\ & x_3x_{12}, x_7x_{12}, x_1x_9, x_2x_8, x_3x_7, x_4x_6, x_1x_6, x_4x_9, x_5x_{10}, x_{10}x_{11}, x_{11}x_{12}, x_5x_{12}). \end{aligned}$$

Using *Macaulay*2 [**GSa**], it is seen that the values of $\operatorname{depth}(R/J^i)$, for $i = 1, \ldots, 4$ are 8, 5, 0, 4, respectively.

If G is a very well-covered graph (i.e., G is unmixed, has no isolated vertices and $|V(G)|$ is equal to $2\operatorname{ht}(I(G))$), then the depth of symbolic powers of $I(G)^\vee$ form a non-increasing sequence [**SF18**] (cf. [**KTT$^+$17**]). The next result complements this fact.

PROPOSITION 6.40. *If G is a very well-covered graph, then the symbolic powers of $I(G)$ have non-increasing depth and non-decreasing regularity.*

PROOF. The graph G has a perfect matching by [**GV10**, Corollary 3.7(ii)]. Pick an edge e in a perfect matching of G and set $x_e = \prod_{x_i \in e} x_i$. Note that any minimal vertex cover of G intersects e in exactly one vertex because G is unmixed. Therefore $(I^{(k+1)} : x_e) = I^{(k)}$ for $k \geq 1$. Thus the result follows from parts (ii) and (iv) of Corollary 6.12. ♠

We will give another family of squarefree monomial ideals whose symbolic powers have non-increasing depth. A *clique* of a graph G is a set of vertices inducing a complete subgraph. The *clique clutter* of G, denoted by $\mathrm{cl}(G)$, is the clutter on $V(G)$ whose edges are the maximal cliques of G (maximal with respect to inclusion).

DEFINITION 6.41. A graph G is called *strongly perfect* if every induced subgraph H of G has a maximal independent set of vertices C such that $|C \cap e| = 1$ for any maximal clique e of H.

PROPOSITION 6.42. *If G is a strongly perfect graph and $J = I(\mathrm{cl}(G)^\vee)$, then*

(a) $\mathrm{depth}(R/J^{(k)}) \geq \mathrm{depth}(R/J^{(k+1)})$ *for* $k \geq 1$, *and*
(b) $\mathrm{reg}(R/J^{(k)}) \leq \mathrm{depth}(R/J^{(k+1)})$ *for* $k \geq 1$.

PROOF. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be the set of all ideals (e) such that $e \in E(\mathrm{cl}(G))$. From the equality

$$J = I(\mathrm{cl}(G)^\vee) = I(\mathrm{cl}(G))^\vee = \bigcap_{e \in E(\mathrm{cl}(G))} (e) = \bigcap_{i=1}^{s} \mathfrak{p}_i,$$

we get $J^{(k)} = \cap_{i=1}^{s} \mathfrak{p}_i^k$ for $k \geq 1$. As G is strongly perfect, G has a maximal independent set of vertices C such that $|C \cap e| = 1$ for any $e \in \mathrm{cl}(G)$, that is, $|C \cap \mathfrak{p}_i| = 1$ for $i = 1, \ldots, s$. Hence, setting $f = \prod_{x_i \in C} x_i$, one has the equalities

$$(J^{(k+1)} : f) = \left(\bigcap_{i=1}^{s} \mathfrak{p}_i{}^{k+1} : f \right) = \bigcap_{i=1}^{s} (\mathfrak{p}_i^{k+1} : f) = \bigcap_{i=1}^{s} \mathfrak{p}_i^k = J^{(k)} \ \text{ for } \ k \geq 1.$$

Therefore, by parts (ii) and (iv) of Corollary 6.12, one has

$$\mathrm{depth}(R/J^{(k)}) = \mathrm{depth}(R/(J^{(k+1)} : f)) \geq \mathrm{depth}(R/J^{(k+1)}),$$

and $\mathrm{reg}(R/J^{(k)}) = \mathrm{reg}(R/(J^{(k+1)} : f)) \leq \mathrm{reg}(R/J^{(k+1)})$. ♠

PROPOSITION 6.43. *Let $A = K[X]$ and $B = K[Y]$ be polynomial rings over a field K in disjoint sets of variables, let I and J be nonzero homogeneous proper ideals of A and B respectively, and let $R = K[X, Y]$. The following hold.*

(a) [**HTT16**, Proposition 3.7] *$R/(I + J)^i$ is Cohen–Macaulay for all $i \leq k$ if and only if A/I^i and B/J^i are Cohen–Macaulay for all $i \leq k$.*
(b) [**HT10**, Lemma 3.2] $\mathrm{reg}(R/(I + J)) = \mathrm{reg}(A/I) + \mathrm{reg}(B/J)$.
(c) [**HT10**, Lemma 3.2] $\mathrm{reg}(R/IJ) = \mathrm{reg}(A/I) + \mathrm{reg}(B/J) + 1$.

The Cohen-Macaulay property of the square of an edge ideal can be expressed in terms of its connected components. For additional results on the depth of powers of sums of

ideals see [**HTT16**] and the references therein. Let G be a graph and let $I = I(G)$ be its edge ideal. Lower bounds for the depth of the first three powers of I in terms of the diameter of G are given in [**FM15**].

COROLLARY 6.44. *Let G be a graph with connected components $G_1, \ldots, G_m$. Then $I(G)^2$ is Cohen–Macaulay if and only if $I(G_i)^2$ is Cohen–Macaulay for $i = 1, \ldots, m$.*

PROOF. Since the radical of a Cohen–Macaulay monomial ideal is Cohen–Macaulay [**HTT05**] (see Corollary 6.17), the results follows from Proposition 6.43. ♠

EXAMPLE 6.45. Let $A = K[x_1, x_2, x_3]$ and $B = K[y_1, y_2, y_3]$ be polynomial rings over a field K, let $I = (x_1x_2, x_2x_3, x_1x_3)$ and $J = (y_1y_2, y_2y_3, y_1y_3)$ be ideals of A and B respectively, and let $R = K[X, Y]$. Then A/I^2 and B/I^2 have depth 0 but $R/(I + J)^2$ has depth 1, that is, the depth of squares of monomial ideals is not additive on disjoint sets of variables.

LEMMA 6.46. *Let G be a graph without isolated vertices. The following hold.*

(a) *If $R/I(G)^2$ is Cohen–Macaulay, then $R/(I(G \setminus N_G(x_i))^2$ is Cohen–Macaulay for any x_i.*

(b) $\operatorname{depth}(R/I(G)^2) = 0$ *if and only if G has a triangle C_3 that intersects $N_G(x_i)$ for any x_i outside C_3. In particular if the depth of $R/I(G)^2$ is 0, then G is connected.*

PROOF. (a) Using Proposition 6.36(a) and Corollary 6.12(ii), we get

$$\operatorname{depth}(R/(I(G \setminus N_G(x_i))^2, N_G(x_i))) \geq \operatorname{depth}(R/(I(G)^2 \colon x_i^2)) \geq \operatorname{depth}(R/I(G)^2)$$

for all i. Thus $R/(I(G \setminus N_G(x_i))^2$ is Cohen–Macaulay for all i.

(b) ($\Rightarrow$) As $\mathfrak{m} = (x_1, \ldots, x_n)$ is an associated prime of $I(G)^2$, we have that there exists $x^a = x_1^{a_1} \cdots x_n^{a_n}$ such that $(I(G)^2 \colon x^a) = \mathfrak{m}$. Thus $x_i x^a \in I(G)^2$ for all i and $x^a \notin I(G)^2$. Note that x^a is squarefree. Indeed if $a_k \geq 2$ for some k, then we obtain $x_k x^a = x^b f_i f_j$ for some monomial x^b and some minimal generators f_i, f_j of $I(G)$, which is impossible because f_i, f_j are squarefree monomials of degree 2 and $x^a \notin I(G)^2$. Thus we may assume that $x^a = x_1 \cdots x_r$, for some $r \geq 3$, and $x_1x_2 \in I(G)$. Then $x_3x^a = x^b f_i f_j$ for some x^b and some minimal generators f_i, f_j of $I(G)$. One can write $f_i = x_3x_k$ and $f_j = x_3x_\ell$, $k \neq \ell$, $k \neq 3$, $\ell \neq 3$. Clearly either $x_k = x_1$ or $x_k = x_2$ and either $x_\ell = x_1$ or $x_\ell = x_2$ because x^a is not in $I(G)^2$. Thus x_1, x_2, x_3 are the vertices of a triangle of G that we denote by C_3. Since $x_r x^a \in I(G)^2$, it follows that $r = 3$. Take any vertex x_k not in C_3. As $x_k x^a = x_k(x_1x_2x_3)$ and $x_k x^a$ is in $I(G)^2$, we get that x_k is adjacent to some vertex of C_3.

(b) ($\Leftarrow$) Pick a triangle C_3 of G such that any vertex outside C_3 is adjacent to a vertex of C_3. Setting $x^a = \prod_{x_i \in V(C_3)} x_i$, we get that $(I(G)^2 \colon x^a)$ is the maximal ideal $\mathfrak{m} = (x_1, \ldots, x_n)$.

Thus $\mathfrak{m}$ is an associated prime of $I(G)^2$, that is, $\operatorname{depth}(R/I(G)^2) = 0$. This part could also follow from a general construction of [**CMS02**]. ♠

In [**KTT$^+$17, T$^+$16**] the Cohen–Macaulay property of the square of the edge ideal of a graph is classified.

THEOREM 6.47. [**T$^+$16**, Theorem 4.4] *Let G be a graph with vertex set $V(G) = \{x_1, \ldots, x_n\}$ and without isolated vertices. Then $I(G)^2$ is Cohen–Macaulay if and only if G is a triangle-free unmixed graph and $G \setminus \{x_i\}$ is unmixed for all i.*

As an application we recover the following facts.

COROLLARY 6.48. [**KTT$^+$17**, Proposition 4.2] *Let G be a bipartite graph without isolated vertices. Then $I(G)^2$ is Cohen–Macaulay if and only if $I(G)$ is a complete intersection, that is, G is a disjoint union of edges.*

PROOF. $\Rightarrow$) Since $I(G)$ is the radical of $I(G)^2$, by Corollary 6.17, the ideal $I(G)$ is Cohen–Macaulay. Hence, according to a structure theorem for Cohen–Macaulay bipartite graphs [**HH05b**, Theorem 3.4], there is a bipartition $V_1 = \{x_1, \ldots, x_g\}$, $V_2 = \{y_1, \ldots, y_g\}$ of G such that:
(i) $\{x_i, y_i\} \in E(G)$ for all i,
(ii) if $\{x_i, y_j\} \in E(G)$, then $i \leq j$, and
(iii) if $\{x_i, y_j\}$, $\{x_j, y_k\}$ are in $E(G)$ and $i < j < k$, then $\{x_i, y_k\} \in E(G)$.

We proceed by induction on g. If $g = 1$, $I(G)$ is clearly a complete intersection. Using the connected components of G together with Corollaries 6.17 and 6.44, and Proposition 6.43, we may assume that $I(G)^2$ is Cohen–Macaulay and that G is a Cohen–Macaulay connected bipartite graph. Consider the graph $H = G \setminus N_G(y_1)$. We set $R = K[V_1 \cup V_2]$. Note that $N_G(y_1) = \{x_1\}$. Hence, by Lemma 6.46(a), $I(G \setminus \{x_1\})^2$ is Cohen–Macaulay and so is $I(G \setminus \{x_1\})$. Therefore by induction $I(G \setminus \{x_1\})$ is generated by $x_2y_2, \ldots, x_gy_g$. As G is connected, using (i)–(iii), it is seen that the edges of G are the edges of the perfect matching and all edges of the form $\{x_1, y_i\}$, $i \geq 1$. It is not hard to see (by a separate induction procedure) that the square of $I(G)$ is not Cohen–Macaulay if $g \geq 2$. Thus $g = 1$.

$\Leftarrow$) If $I(G)$ is a complete intersection, it is well known that all powers of $I(G)$ are Cohen–Macaulay [**Mat89**, 17.4, p. 139]. ♠

COROLLARY 6.49. [**KTT$^+$17**, Corollary 2.3] *Let G be a graph without isolated vertices. If $I(G)^2$ is Cohen–Macaulay, then G has no triangles.*

PROOF. Let $V(G) = \{x_1, \ldots, x_n\}$ be the vertex set of G and let R be the polynomial ring $K[V(G)]$. We proceed by induction on n. The result is clear for $n = 1, 2, 3$. Assume $n \geq 4$.

We proceed by contradiction assuming that G has a triangle C_3. Using the connected components of G together with Corollaries 6.17 and 6.44, and Proposition 6.43, we may assume that $I(G)^2$ is Cohen–Macaulay and G is connected. Thus, by Lemma 6.46(a), $I(G \setminus N_G(x_i))^2$ is Cohen–Macaulay for all i. If G has a vertex x_i not in C_3 such that $N_G(x_i)$ do not intersect the vertex set $V(C_3)$ of C_3, then C_3 is a triangle of $G \setminus N_G(x_i)$, a contradiction. Thus any vertex outside C_3 is adjacent to a vertex of C_3. Hence, by Lemma 6.46(b), we get $\operatorname{depth}(R/I(G)^2) = 0$, a contradiction. This part could also follow from a general construction of **[CMS02]**. ♠

EXAMPLE 6.50. **[T$^+$16]** The square of the edge ideal of the graph G of Fig. 1 is Cohen–Macaulay and $I(G)$ is Gorenstein. This can be verified using *Macaulay*2 **[GSa]**. A result of Hoang **[T$^+$16**, Theorem 4.4] shows that for a graph G without isolated vertices $I(G)^2$ is Cohen–Macaulay if and only if G is triangle free and Gorenstein.

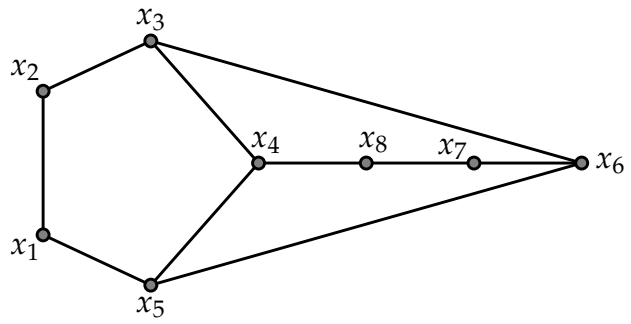


FIGURE 1. Gorenstein Graph G.

CHAPTER 7

Conclusions and future work

First, we gave a fundamental relation between the r-th generalized Hamming weight of a code and the Vancoscelos function and the footprint: Let K be a field and let $\mathbb{X}$ be a finite subset of $\mathbb{P}^{s-1}$. If $|\mathbb{X}| \geq 2$ and $\delta_{\mathbb{X}}(d,r)$ is the r-th generalized Hamming weight of $C_{\mathbb{X}}(d)$, then

$$\delta_{\mathbb{X}}(d,r) = \delta_{I(\mathbb{X})}(d,r) = \vartheta_I(d,r) \text{ for } d \geq 1 \text{ and } 1 \leq r \leq H_{I(\mathbb{X})}(d),$$

and $\delta_{\mathbb{X}}(d,r) = r$ for $d \geq \operatorname{reg}(S/I(\mathbb{X}))$.

Second, we find a characterization of a weighted oriented graph: Let $\mathcal{D}$ be a weighted oriented forest without isolated vertices and let G be its underlying forest. The following conditions are equivalent:

(a) $\mathcal{D}$ is Cohen–Macaulay.
(b) $I(\mathcal{D})$ is unmixed, that is, all its associated primes have the same height.
(c) G has a perfect matching $\{x_1, y_1\}, \ldots, \{x_r, y_r\}$ so that for $i = 1, \ldots, r$ we have

$$\deg_G(y_i) = 1 \text{ and } d(x_i) = d_i = 1 \text{ if } (x_i, y_i) \in E(\mathcal{D}).$$

Finally, we obtain the behavior of the depth and regularity of monomial ideals via polarization: Let $I \subset R$ be a monomial ideal and let f be a monomial. If $L = (f, I)$ and X_L is the set of new variables that are needed to polarize L, then

(i) $\operatorname{depth}(R[X_L]/L^{\text{pol}}) - \operatorname{depth}(R[X_L]/(f_1^{\text{pol}}, \ldots, f_r^{\text{pol}})) = \operatorname{depth}(R/L) - \operatorname{depth}(R/I)$,
(ii) $\operatorname{reg}(R[X_L]/L^{\text{pol}}) = \operatorname{reg}(R/L)$ and $\operatorname{reg}(R[X_L]/(f_1^{\text{pol}}, \ldots, f_r^{\text{pol}})) = \operatorname{reg}(R/I)$,

where $G(I) = \{f_1, \ldots, f_r\}$, and f_i^{pol} is the polarization of f_i in $R[X_L]$.
Let I be a monomial ideal of R and let x_i be a variable. The following hold.

(a) If $p \geq 1$ and $q - p \geq 2$, then $\operatorname{depth}(R/I) = \operatorname{depth}(R/L)$.
(b) If $p \geq 0$ and $q - p = 1$, then $\operatorname{depth}(R/L) \geq \operatorname{depth}(R/I)$.
(c) If $p = 0$ and $q \geq 2$, then

$$\operatorname{depth}(R/I) = \operatorname{depth}(R/(\{x^a/x_i^{q-1} \mid x^a \in \mathcal{B}_i\} \cup \mathcal{A}_i\})).$$

and if we consider the ideal L' define by $(\{x^a/x_i^{q-1} | \, x^a \in \mathcal{B}_i\} \cup \mathcal{A}_i\})$, where x_i is a variable. The following hold.

(a) If $p \geq 1$ and $q - p \geq 2$, then $\operatorname{reg}(R/L) \leq \operatorname{reg}(R/I) \leq \operatorname{reg}(R/L) + 1$.
(b) If $p \geq 0$ and $q - p = 1$, then $\operatorname{reg}(R/L) \leq \operatorname{reg}(R/I)$.
(c) If $p = 0$ and $q \geq 2$, then $\operatorname{reg}(R/L') \leq \operatorname{reg}(R/I) \leq \operatorname{reg}(R/L') + q - 1$.

In the future I would like to use more geometric notions as schemes to address issues such as codes. In fact, I already found a relationship between the minimum distance and a type of 0-scheme. I am also interested in the use of the techniques used here to compute the local cohomology of monomial ideals.

Bibliography

[AM94] Michael Francis Atiyah and Ian Grant Macdonald, *Introduction to commutative algebra*, Westview press, 1994.

[Bah04] Carlos EN Bahiano, *Symbolic powers of edge ideals*, Journal of Algebra **273** (2004), no. 2, 517–537.

[Bas63] Hyman Bass, *On the ubiquity of gorenstein rings*, Mathematische Zeitschrift **82** (1963), no. 1, 8–28.

[BD17] Peter Beelen and Mrinmoy Datta, *Generalized hamming weights of affine cartesian codes*, arXiv preprint arXiv:1706.02114 (2017).

[BG00] Isabel Bermejo and Philippe Gimenez, *On castelnuovo-mumford regularity of projective curves*, Proceedings of the American Mathematical Society **128** (2000), no. 5, 1293–1299.

[BG06] ———, *Saturation and castelnuovo–mumford regularity*, Journal of Algebra **303** (2006), no. 2, 592–617.

[BH98] Winfried Bruns and H Jürgen Herzog, *Cohen-macaulay rings*, Cambridge University Press, 1998.

[BHHW98] Ian Blake, Chris Heegard, Tom Hoholdt, and Victor Wei, *Algebraic-geometry codes*, IEEE Transactions on Information Theory **44** (1998), no. 6, 2596–2618.

[BIR$^+$] W Bruns, B Ichim, T Römer, R Sieg, and C Söger Normaliz, *Algorithms for rational cones and affine monoids*.

[BJG08] Jørgen Bang-Jensen and Gregory Z Gutin, *Digraphs: theory, algorithms and applications*, Springer Science & Business Media, 2008.

[Bla11] Paul E Bland, *Rings and their modules*, Walter de Gruyter, 2011.

[Bro79] Markus Brodmann, *The asymptotic nature of the analytic spread*, Mathematical Proceedings of the Cambridge Philosophical Society, vol. 86, Cambridge University Press, 1979, pp. 35–39.

[Buc] B Buchberger, *An algorithmic method in polynomial ideal theory, chapter 6 in nk bose*, Recent Trends in Multidimensional System Theory.

[Bur72] Lindsay Burch, *Codimension and analytic spread*, Mathematical Proceedings of the Cambridge Philosophical Society, vol. 72, Cambridge University Press, 1972, pp. 369–373.

[BW93] Thomas Becker and Volker Weispfenning, *Gröbner bases*, Gröbner Bases, Springer, 1993, pp. 187–242.

[Car13] Cícero Carvalho, *On the second hamming weight of some reed–muller type codes*, Finite Fields and Their Applications **24** (2013), 88–94.

[CEHH13] Susan M Cooper, Robert JD Embree, Huy Tài Hà, and Andrew H Hoefel, *Symbolic powers of monomial ideals*, arXiv preprint arXiv:1309.5082 (2013).

[CHH$^+$17] Giulio Caviglia, Huy Tai Ha, Jürgen Herzog, Manoj Kummini, Naoki Terai, and Ngo Viet Trung, *Depth and regularity modulo a principal ideal*, arXiv preprint arXiv:1706.09675 (2017).

[CLO07] David Cox, John Little, and Donal O'shea, *Ideals, varieties, and algorithms*, vol. 3, Springer, 2007.

[CMS02] Janet Chen, Susan Morey, and Anne Sung, *The stable set of associated primes of the ideal of a graph*, The Rocky Mountain journal of mathematics (2002), 71–89.

[CN76] RC Cowsik and MV Nori, *On the fibres of blowing up*, Journal of the Indian Mathematical Society **40** (1976), no. 1-4, 217–222.

[CNL17] Cícero Carvalho, Victor GL Neumann, and Hiram H López, *Projective nested cartesian codes*, Bulletin of the Brazilian Mathematical Society, New Series **48** (2017), no. 2, 283–302.

[Cor01] Gérard Cornuéjols, *Combinatorial optimization, volume 74 of cbms-nsf regional conference series in applied mathematics*, Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA (2001).

[CPSF+15] A Constantinescu, MR Pournaki, SA Seyed Fakhari, N Terai, and S Yassemi, *Cohen–macaulayness and limit behavior of depth for powers of cover ideals*, Communications in Algebra **43** (2015), no. 1, 143–157.

[CQ10] Veronica Crispin Quiñonez, *Integral closure and other operations on monomial ideals*, Journal of Commutative Algebra, vol. 2, 2010, pp. 359–386.

[DDSG+15] Hailong Dao, Alessandro De Stefani, Eloísa Grifo, Craig Huneke, and Luis Núñez-Betancourt, *Symbolic powers of ideals*, Singularities and Foliations. Geometry, Topology and Applications, Springer, 2015, pp. 387–432.

[DG17] Mrinmoy Datta and Sudhir Ghorpade, *Number of solutions of systems of homogeneous polynomial equations over finite fields*, Proceedings of the American Mathematical Society **145** (2017), no. 2, 525–541.

[DHS13] Hailong Dao, Craig Huneke, and Jay Schweig, *Bounds on the regularity and projective dimension of ideals associated to graphs*, Journal of Algebraic Combinatorics **38** (2013), no. 1, 37–55.

[DRTR01] Iwan M Duursma, C Rentería, and Horacio Tapia-Recillas, *Reed-muller codes on complete intersections*, Applicable Algebra in Engineering, Communication and Computing **11** (2001), no. 6, 455–462.

[DS93] Andreas Dress and Robert Simon, *A new algebraic criterion for shellability*, Beitrage zur Alg. und Geom **340** (1993), no. 1, 45–55.

[DV10] Luis A Dupont and Rafael H Villarreal, *Edge ideals of clique clutters of comparability graphs and the normality of monomial ideals*, Mathematica Scandinavica (2010), 88–98.

[DV11] ———, *Algebraic and combinatorial properties of ideals and algebras of uniform clutters of tdi systems*, Journal of Combinatorial Optimization **21** (2011), no. 3, 269–292.

[EGSS01] David Eisenbud, Daniel R Grayson, Mike Stillman, and Bernd Sturmfels, *Computations in algebraic geometry with macaulay 2*, vol. 8, Springer Science & Business Media, 2001.

[EH83] David Eisenbud and Craig Huneke, *Cohen-macaulay rees algebras and their specialization*.

[Eis05] David Eisenbud, *The geometry of syzygies: a second course in algebraic geometry and commutative algebra*, vol. 229, Springer Science & Business Media, 2005.

[Eis13] ———, *Commutative algebra: with a view toward algebraic geometry*, vol. 150, Springer Science & Business Media, 2013.

[ErH11] Viviana Ene and J rgen Herzog, *Gr bner bases in commutative algebra*, vol. 130, 2011.

[EVY05] C Escobar, Rafael H Villarreal, and Yuji Yoshino, *Torsion freeness and normality of blowup rings of monomial ideals*, Commutative Algebra: Geometric, Homological, Combinatorial and Computational Aspects, Proceedings: Sevilla and Lisbon (A. Corso et al., Eds.), Lect. Notes Pure Appl. Math **244** (2005), 69–84.

[Fak17] SA Seyed Fakhari, *Depth and stanley depth of symbolic powers of cover ideals of graphs*, Journal of Algebra **492** (2017), 402–413.

[Far06] Sara Faridi, *Monomial ideals via square-free monomial ideals*, Lecture Notes in Pure and Applied Mathematics **244** (2006), 85.

[FHM13] Christopher A Francisco, Huy Tài Hà, and Jeffrey Mermin, *Powers of square-free monomial ideals and combinatorics*, Commutative Algebra, Springer, 2013, pp. 373–392.

[FL98] Jeanne Fitzgerald and Robert F Lax, *Decoding affine variety codes using gröbner bases*, Designs, Codes and Cryptography **13** (1998), no. 2, 147–158.

[FM15] Louiza Fouli and Susan Morey, *A lower bound for depths of powers of edge ideals*, Journal of Algebraic Combinatorics **42** (2015), no. 3, 829–848.

[Frö82] Ralf Fröberg, *A study of graded extremal rings and of monomial rings*, Mathematica Scandinavica (1982), 22–34.

[Gei08] Olav Geil, *On the second weight of generalized reed-muller codes*, Designs, Codes and Cryptography **48** (2008), no. 3, 323–330.

[GKR93] Anthony V Geramita, Martin Kreuzer, and Lorenzo Robbiano, *Cayley-bacharach schemes and their canonical modules*, Transactions of the American Mathematical Society **339** (1993), no. 1, 163–189.

[GLS05] Leah Gold, John Little, and Hal Schenck, *Cayley–bacharach and evaluation codes on complete intersections*, Journal of Pure and Applied Algebra **196** (2005), no. 1, 91–99.

[GMBS+17] Philippe Gimenez, José Martınez-Bernal, Aron Simis, Rafael H Villarreal, and Carlos E Vivares, *Monomial ideals and cohen-macaulay vertex-weighted digraphs*, arXiv preprint arXiv:1706.00126 (2017).

[GN94] Shirō Gotō and Kōji Nishida, *The cohen-macaulay and gorenstein rees algebras associated to filtrations*, vol. 526, American Mathematical Soc., 1994.

[GP12] Gert-Martin Greuel and Gerhard Pfister, *A singular introduction to commutative algebra*, Springer Science & Business Media, 2012.

[GRV09] Isidoro Gitler, Enrique Reyes, and Rafael H Villarreal, *Blowup algebras of square-free monomial ideals and some links to combinatorial optimization problems*, The Rocky Mountain Journal of Mathematics (2009), 71–102.

[GSa] D Grayson and M Stillman, *Macaulay2 (available via anonymous ftp from math. uiuc. edu, 1996)*, Google Scholar.

[GSb] Daniel R Grayson and Michael E Stillman, *Macaulay 2, a software system for research in algebraic geometry, 2006*.

[GSRTR02] Manuel Gonzalez-Sarabia, C Renterıa, and H Tapia-Recillas, *Reed-muller-type codes over the segre variety*, Finite Fields and their Applications **8** (2002), no. 4, 511–518.

[GSVV13] Philippe Gimenez, Aron Simis, Wolmer V Vasconcelos, and Rafael H Villarreal, *On complete monomial ideals*, arXiv preprint arXiv:1310.7793 (2013).

[GT13] Olav Geil and Casper Thomsen, *Weighted reed–muller codes revisited*, Designs, codes and cryptography **66** (2013), no. 1-3, 195–220.

[GV10] Isidoro Gitler and Carlos Valencia, *On bounds for some graph invariants*, Boletín de la Sociedad Matemática Mexicana: Tercera Serie **16** (2010), no. 2, 73–94.

[GV11] Isidoro Gitler and Rafael H Villarreal, *Graphs, rings and polyhedra*, vol. 35, Cinvestav, 2011.

[GVV07] Isidoro Gitler, C Valencia, and Rafael H Villarreal, *A note on rees algebras and the mfmc property*, Beiträge Algebra Geom **48** (2007), no. 1, 141–150.

[Han17] Nguyen Thu Hang, *Stability of depth functions of cover ideals of balanced hypergraphs*, arXiv preprint arXiv:1711.09178 (2017).

[Har] Frank Harary, *Graph theory. 1969*.

[Har13] Robin Hartshorne, *Algebraic geometry*, vol. 52, Springer Science & Business Media, 2013.

[HH05a] Jürgen Herzog and Takayuki Hibi, *The depth of powers of an ideal*, Journal of Algebra **291** (2005), no. 2, 534–550.

[HH05b] ———, *Distributive lattices, bipartite graphs and alexander duality*, Journal of Algebraic Combinatorics **22** (2005), no. 3, 289–302.

[HH11] ———, *Monomial ideals*, Monomial Ideals, Springer, 2011, pp. 3–22.

[HHT07] Jürgen Herzog, Takayuki Hibi, and Ngô Viêt Trung, *Symbolic powers of monomial ideals and vertex cover algebras*, Advances in Mathematics **210** (2007), no. 1, 304–322.

[HKM77] Tor Helleseth, Torleiv Kløve, and Johannes Mykkeltveit, *The weight distribution of irreducible cyclic codes with block lengths n1 ((q1- 1) n)*, Discrete Mathematics **18** (1977), no. 2, 179–211.

[HLM+18] Huy Tài Hà, Kuei-Nuan Lin, Susan Morey, Enrique Reyes, and Rafael H Villarreal, *Edge ideals of oriented graphs*, arXiv preprint arXiv:1805.04167 (2018).

[HM10] Huy Tài Hà and Susan Morey, *Embedded associated primes of powers of square-free monomial ideals*, Journal of Pure and Applied Algebra **214** (2010), no. 4, 301–308.

[HT10] Le Tuan Hoa and Nguyen Duc Tam, *On some invariants of a mixed product of ideals*, Archiv der Mathematik **94** (2010), no. 4, 327–337.

[HT+17] Nguyen Thu Hang, Tran Nam Trung, et al., *The behavior of depth functions of cover ideals of unimodular hypergraphs*, Arkiv för Matematik **55** (2017), no. 1, 89–104.

[HTT05] Jürgen Herzog, Yukihide Takayama, and Naoki Terai, *On the radical of a monomial ideal*, Archiv der Mathematik **85** (2005), no. 5, 397–408.

[HTT16] Huy Tài Hà, Ngo Viet Trung, and Trân Nam Trung, *Depth and regularity of powers of sums of ideals*, Mathematische Zeitschrift **282** (2016), no. 3-4, 819–838.

[HU89] Craig Huneke and Bernd Ulrich, *Powers of licci ideals*, Commutative algebra, Springer, 1989, pp. 339–346.

[HVLP98] Tom Høholdt, Jacobus H Van Lint, and Ruud Pellikaan, *Algebraic geometry codes*, Handbook of coding theory **1** (1998), no. Part 1, 871–961.

[JNS18] AV Jayanthan, N Narayanan, and S Selvaraja, *Regularity of powers of bipartite graphs*, Journal of Algebraic Combinatorics **47** (2018), no. 1, 17–38.

[KSŠ14] Tomáš Kaiser, Matěj Stehlík, and Riste Škrekovski, *Replication in critical graphs and the persistence of monomial ideals*, Journal of Combinatorial Theory, Series A **123** (2014), no. 1, 239–251.

[KTT+17] Kyouko Kimura, Naoki Terai, Tran Nam Trung, et al., *Stability of depths of symbolic powers of stanley–reisner ideals*, Journal of Algebra **473** (2017), 307–323.

[LRMV14] Hiram H López, Carlos Rentería-Márquez, and Rafael H Villarreal, *Affine cartesian codes*, Designs, codes and cryptography **71** (2014), no. 1, 5–19.

[LSPV12] Hiram López, Eliseo Sarmiento, Maria Pinto, and Rafael Villarreal, *Parameterized affine codes*, Studia Scientiarum Mathematicarum Hungarica **49** (2012), no. 3, 406–418.

[Mat80] Hideyuki Matsumura, *Commutative algebra, volume 56 of mathematics lecture note series*, 1980.

[Mat89] _____, *Commutative ring theory*, vol. 8, Cambridge university press, 1989.

[MBMV12] José Martínez-Bernal, Susan Morey, and Rafael H Villarreal, *Associated primes of powers of edge ideals*, Collectanea Mathematica **63** (2012), no. 3, 361–374.

[MBMVV18] Jose Martínez-Bernal, Susan Morey, Rafael H Villarreal, and Carlos E Vivares, *Depth and regularity of monomial ideals via polarization and combinatorial optimization*, arXiv preprint arXiv:1803.02017 (2018).

[MBPV16] José Martínez-Bernal, Yuriko Pitones, and Rafael H Villarreal, *Minimum distance functions of complete intersections*, arXiv preprint arXiv:1601.07604 (2016).

[MBPV17] José Martínez-Bernal, Yuriko Pitones, and Rafael H Villarreal, *Minimum distance functions of graded ideals and reed–muller-type codes*, Journal of Pure and Applied Algebra **221** (2017), no. 2, 251–275.

[MBRV11] José Martínez-Bernal, C Rentería, and Rafael H Villarreal, *Combinatorics of symbolic rees algebras of edge ideals of clutters*, Contemp. Math **555** (2011), 151–164.

[McA06] Stephen McAdam, *Asymptotic prime divisors*, vol. 1023, Springer, 2006.

[Mil98] Ezra Miller, *Alexander duality for monomial ideals and their resolutions*, arXiv preprint math/9812095 (1998).

[Mil00] _____, *The alexander duality functors and local duality with monomial support*, Journal of Algebra **231** (2000), no. 1, 180–234.

[MS77] Florence Jessie MacWilliams and Neil James Alexander Sloane, *The theory of error-correcting codes*, Elsevier, 1977.

[MS04] Ezra Miller and Bernd Sturmfels, *Combinatorial commutative algebra*, vol. 227, Springer Science & Business Media, 2004.

[MV12] Susan Morey and Rafael H Villarreal, *Edge ideals: algebraic and combinatorial properties*, Progress in Commutative Algebra, Combinatorics and Homology **1** (2012), 85–126.

[Nag59] Masayoshi Nagata, *On the 14-th problem of hilbert*, American Journal of Mathematics **81** (1959), no. 3, 766–772.

[NM65] Masayoshi Nagata and M Pavaman Murthy, *Lectures on the fourteenth problem of hilbert*, vol. 31, Tata Institute of fundamental research Bombay, 1965.

[NPV14] Jorge Neves, Maria Vaz Pinto, and Rafael H Villarreal, *Regularity and algebraic properties of certain lattice ideals*, Bulletin of the Brazilian Mathematical Society, New Series **45** (2014), no. 4, 777–806.

[NSZN16] Abbas Nasrollah Nejad, Aron Simis, and Rashid Zaare-Nahandi, *The aluffi algebra of the jacobian of points in projective space: torsion-freeness*, Journal of Algebra **467** (2016), 268–283.

[OPVV14] Liam O'Carroll, Francesc Planas-Vilanova, and Rafael H Villarreal, *Degree and algebraic properties of lattice and matrix ideals*, SIAM Journal on Discrete Mathematics **28** (2014), no. 1, 394–427.

[Pee10] Irena Peeva, *Graded syzygies*, vol. 14, Springer Science & Business Media, 2010.

[PRT17] Yuriko Pitones, Enrique Reyes, and Jonathan Toledo, *Monomial ideals of weighted oriented graphs*, arXiv preprint arXiv:1710.03785 (2017).

[PSW13] Chelsey Paulsen and Sean Sather-Wagstaff, *Edge ideals of weighted graphs*, Journal of Algebra and Its Applications **12** (2013), no. 05, 1250223.

[Rav90] MS Ravi, *Regularity of ideals and their radicals*, manuscripta mathematica **68** (1990), no. 1, 77–87.

[Rav99] G Ravindra, *Some classes of strongly perfect graphs*, Discrete mathematics **206** (1999), no. 1-3, 197–203.

[RMSV11] Carlos Rentería-Márquez, Aron Simis, and Rafael H Villarreal, *Algebraic methods for parameterized codes and invariants of vanishing ideals over finite fields*, Finite Fields and Their Applications **17** (2011), no. 1, 81–104.

[Rob90] Paul Roberts, *An infinitely generated symbolic blow-up in a power series ring and a new counterexample to hilbert's fourteenth problem*, Journal of Algebra **132** (1990), no. 2, 461–473.

[S$^+$90] Dean E Smith et al., *On the cohen-macaulay property in commutative algebra and simplicial topology.*, Pacific Journal of Mathematics **141** (1990), no. 1, 165–196.

[Sch98] Alexander Schrijver, *Theory of linear and integer programming*, John Wiley & Sons, 1998.

[Sch03] _____, *Combinatorial optimization. algorithms and combinatorics, vol. 24*, 2003.

[SCSV18] Manuel González Sarabia, Eduardo Camps, Eliseo Sarmiento, and Rafael H Villarreal, *The second generalized hamming weight of some evaluation codes arising from a projective torus*, Finite Fields and Their Applications **52** (2018), 370–394.

[SF18] SA Seyed Fakhari, *Symbolic powers of cover ideal of very well-covered and bipartite graphs*, Proceedings of the American Mathematical Society **146** (2018), no. 1, 97–110.

[Sim96] Aron Simis, *Effective computation of symbolic powers by jacobian matrices*, Communications in Algebra **24** (1996), no. 11, 3561–3565.

[Sor91] Anders Bjaert Sorensen, *Projective reed-muller codes*, IEEE Transactions on Information Theory **37** (1991), no. 6, 1567–1576.

[SPV11] Eliseo Sarmiento, Maria Vaz Pinto, and Rafael H Villarreal, *The minimum distance of parameterized codes on projective tori*, Applicable Algebra in Engineering, Communication and Computing **22** (2011), no. 4, 249–264.

[ST88] Aron Simis and Ngô Viêt Trung, *The divisor class group of ordinary and symbolic blow-ups*, Mathematische Zeitschrift **198** (1988), no. 4, 479–491.

[Sta78] Richard P Stanley, *Hilbert functions of graded algebras*, Advances in Mathematics **28** (1978), no. 1, 57–83.

[SVV94] Aron Simis, Wolmer V Vasconcelos, and Rafael H Villarreal, *On the ideal theory of graphs*, Journal of Algebra **167** (1994), no. 2, 389–416.

[SW03] Hans Georg Schaathun and Wolfgang Willems, *A lower bound on the weight hierarchies of product codes*, Discrete Applied Mathematics **128** (2003), no. 1, 251–261.

[SZ] P Samuel and O Zariski, *Commutative algebra. vol. ii. reprint of the 1960 edition*, Graduate Texts in Mathematics **29**.

[T$^+$16] Tran Nam Trung et al., *A characterization of triangle-free gorenstein graphs and cohen–macaulayness of second powers of edge ideals*, Journal of Algebraic Combinatorics **43** (2016), no. 2, 325–338.

[Ter99] Naoki Terai, *Alexander duality theorem and stanley-reisner rings*, **1078** (1999), 174–184.

[Toh09] Ştefan O Tohneanu, *Lower bounds on minimal distance of evaluation codes*, Applicable Algebra in Engineering, Communication and Computing **20** (2009), no. 5-6, 351.

[TT12] Naoki Terai and Ngo Viet Trung, *Cohen–macaulayness of large powers of stanley–reisner ideals*, Advances in Mathematics **229** (2012), no. 2, 711–730.

[TV13] Michael Tsfasman and Serge G Vladut, *Algebraic-geometric codes*, vol. 58, Springer Science & Business Media, 2013.

[TV15] Azucena Tochimani and Rafael H Villarreal, *Vanishing ideals over finite fields*, arXiv preprint arXiv:1502.05451 (2015).

[Vas94] Wolmer V Vasconcelos, *Arithmetic of blowup algebras*, vol. 195, Cambridge University Press, 1994.

[Vas04] Wolmer Vasconcelos, *Computational methods in commutative algebra and algebraic geometry*, vol. 2, Springer Science & Business Media, 2004.

[Vil90] Rafael H Villarreal, *Cohen-macaulay graphs*, manuscripta mathematica **66** (1990), no. 1, 277–293.

[Vil01] ———, *Monomial algebras, volume 238 of monographs and textbooks in pure and applied mathematics*, 2001.

[Vil15] Rafael Villarreal, *Monomial algebras*, vol. 8, CRC Press, 2015.

[VT13] Adam Van Tuyl, *A beginners guide to edge and cover ideals*, Monomial ideals, computations and applications, Springer, 2013, pp. 63–94.

[Wal00] Judy L Walker, *Codes and curves*, vol. 7, American Mathematical Soc., 2000.

[Wei91] Victor K Wei, *Generalized hamming weights for linear codes*, IEEE Transactions on information theory **37** (1991), no. 5, 1412–1418.

[WY93] Victor K Wei and Kyeongcheol Yang, *On the generalized hamming weights of product codes*, IEEE transactions on information theory **39** (1993), no. 5, 1709–1713.

Index of Definitions