Centro de Investigación y de Estudios Avanzados
del Instituto Politécnico Nacional

Unidad Zacatenco

Departamento de Matemáticas

# Ideales Anuladores y Códigos de Segre

Tesis que presenta

**Azucena Tochimani Tiro**

para obtener el Grado de

**Doctor en Ciencias**

en la Especialidad de

**Matemáticas**

Director de Tesis: Dr. Rafael Heraclio Villarreal Rodríguez

Ciudad de México Junio, 2016

Center for Research and Advanced Studies
of the National Polythechnic Institute

Campus Zacatenco

Department of Mathematics

# Vanishing Ideals and Segre Codes

A dissertation presented by

**Azucena Tochimani Tiro**

to obtain the Degree of

**Doctor in Science**

in the Speciality of

**Mathematics**

Thesis Advisor: Dr. Rafael Heraclio Villarreal Rodríguez

Mexico city June, 2016

# Acknowledgements

Agradezco al *Consejo Nacional de Ciencia y Tecnología* la beca que me otorgó para la realización de mis estudios de doctorado.

Agradezco a la *Comisión de Equidad y Género de la Sociedad Matemática Mexicana* dentro del proyecto CONACyT 19683 “Las mujeres en las matemáticas mexicanas” por el apoyo complementario otorgado para concluir el doctorado.

Agradezco a la *Fundación Sofía Kovalévskaia* por el apoyo complementario otorgado para concluir el doctorado.

Agradezco a Dr.Carlos Valencia Oleta, Dr. Enrique Reyes Espinoza, Dr. Carlos Rentería Márquez, Dr. Eliseo Sarmiento, Dra. Maria Vaz Pinto, Dr. Víctor Gonzalo López Neumann y Dr. Jorge Neves por dedicar un poco de su valioso tiempo en la revisión de esta tesis. Agradezco todos sus comentarios y correcciones.

Agradezco al Dr. Rafael H. Villarreal por todo el esfuerzo, dedicación y paciencia brindados en estos años. Su motivación ha sido fundamental.

# Resumen

Sean $K$ un campo y $\mathbb{X}$ (resp. $\mathbb{X}^*$) un subconjunto del espacio proyectivo $\mathbb{P}^{s-1}$ (resp. espacio afín $\mathbb{A}^s$) sobre el campo $K$, parametrizado por funciones racionales. Sea $I(\mathbb{X})$ (resp. $I(\mathbb{X}^*)$) el ideal anulador de $\mathbb{X}$ (resp. $\mathbb{X}^*$). Una de las principales contribuciones de esta tesis consiste en determinar fórmulas para $I(\mathbb{X})$ (resp. $I(\mathbb{X}^*)$), con el fin de calcular sus invariantes algebraicos usando teoría de eliminación y bases de Gröbner. Las fórmulas para los ideales anuladores sobre campos finitos que proporcionamos en este trabajo, fueron descubiertas haciendo experimentos con *Macaulay*2; estamos especialmente interesados en este caso debido a su relación con la teoría algebraica de códigos. También consideramos a los conjuntos $X$ y $X^*$ en $\mathbb{P}^{s-1}$ y $\mathbb{A}^s$, respectivamente, parametrizados por funciones racionales sujetas a ciertas restricciones. Posteriormente usamos nuestros resultados para estudiar: el grado y la estructura de los ideales anuladores, la cerradura proyectiva de $\mathbb{X}^*$ y los parámetros básicos de códigos tipo Reed-Muller afines y proyectivos. Cabe destacar que recuperamos algunos resultados para ideales anuladores con parametrizaciones monomiales.

Sea $K = \mathbb{F}_q$ un campo finito. Introducimos una familia de códigos tipo Reed-Muller, llamados *códigos proyectivos de Segre*. Usando métodos de álgebra conmutativa y álgebra lineal, estudiamos sus parámetros básicos y demostramos que dichos códigos son productos directos de códigos tipo Reed-Muller. Como una consecuencia inmediata recuperamos algunos resultados acerca de códigos proyectivos tipo Reed-Muller sobre la variedad de Segre y sobre el toro proyectivo.

Caracterizamos, en términos algebraicos y geométricos, cuándo un ideal anulador graduado es generado por binomios sobre cualquier campo $K$. Después damos una clasificación de los ideales anuladores de intersección completa en conjuntos parametrizados de tipo clutter sobre campos finitos.

# Abstract

Let $K$ be a field and let $\mathbb{X}$ (resp. $\mathbb{X}^*$) be a subset of a projective space $\mathbb{P}^{s-1}$ (resp. affine space $\mathbb{A}^s$), over the field $K$, parameterized by rational functions. Let $I(\mathbb{X})$ (resp. $I(\mathbb{X}^*)$) be the vanishing ideal of $\mathbb{X}$ (resp. $\mathbb{X}^*$). Some of the main contributions of this thesis are in determining formulas for $I(\mathbb{X})$ (resp. $I(\mathbb{X}^*)$) to compute their algebraic invariants using elimination theory and Gröbner bases. The formulas for vanishing ideals over finite fields that we give in this work were discovered by making experiments with *Macaulay*2, we are specially interested in this case because of its relation to algebraic coding theory. We also consider sets $X$ and $X^*$ in $\mathbb{P}^{s-1}$ and $\mathbb{A}^s$, respectively, parameterized by rational functions which are subject to some restrictions. Then we use our results to study: the degree and structure of vanishing ideals, the projective closure of $\mathbb{X}^*$, and the basic parameters of affine and projective Reed-Muller-type codes. We recover some results for vanishing ideals over monomial parameterizations.

Let $K = \mathbb{F}_q$ be a finite field. We introduce a family of projective Reed-Muller-type codes called *projective Segre codes*. Using commutative algebra and linear algebra methods, we study their basic parameters and show that they are direct products of projective Reed-Muller-type codes. As a consequence we recover some results on projective Reed-Muller-type codes over the Segre variety and over projective tori.

We characterize, in algebraic and geometric terms, when a graded vanishing ideal is generated by binomials over any field $K$. Then we give a classification of complete intersection vanishing ideals on parameterized sets of clutter type over finite fields.

# Introduction

This dissertation studies the structure of vanishing ideals over rational parameterizations over arbitrary fields, and their algebraic invariants (degree, regularity, Hilbert function) and algebraic properties (complete intersection). The structure of binomial vanishing ideals and complete intersection vanishing ideals is studied in this thesis. We are specially interested in the case that the field is finite because of its relation to algebraic coding theory. We are also interested in studying the corresponding Reed-Muller-type codes associated to vanishing ideals over finite fields and in examining their basic parameters (length, dimension, minimum distance, generalized Hamming weights). Special attention is given to examine the family of projective Segre codes and the role that Segre products and direct product codes play in this setting.

**Contents of Chapter 1** In this chapter, we present some of the results that will be needed throughout this work and introduce some notation. All results of this chapter are well-known.

We recall some necessary preliminaries on algebraic geometry and commutative algebra. Some of the main topics are graded modules, Gröbner bases, projective closure, vanishing ideals, and Hilbert functions. We introduce the algebraic invariants of affine and graded algebras (regularity, degree, Hilbert polynomial), and examine some of their properties.

Then we introduce the family of projective Reed-Muller-type codes, examine their basic parameters (length, dimension, minimum distance), and explain how the basic parameters relate to Hilbert functions and vanishing ideals (see Proposition 1.5.3). Finally we study the vanishing ideal of the projective closure of an affine set and its connection to Gröbner bases. This will allows us to link affine and projective Reed-Muller-type codes, and affine and graded algebras (see Propositions 1.5.3, 1.4.21, and 1.5.4).

**Contents of Chapter 2** In this chapter we extend the scope of [49, 52] to include vanishing ideals of sets in affine and projective spaces parameterized by rational functions over finite fields. We also include the case of rational parameterizations over infinite fields which is treated in a slightly different way than that of [9, Chapter 3] because here we emphasize the role of vanishing ideals in the implicitization problem when the field is infinite.

Let $R = K[\mathbf{y}] = K[y_1, \ldots, y_n]$ be a polynomial ring over an arbitrary field $K$ and let $F$ be a finite set $\{f_1/g_1, \ldots, f_s/g_s\}$ of rational functions in $K(\mathbf{y})$, the quotient field of $R$, where $f_i$ (resp. $g_i$) is in $R$ (resp. $R \setminus \{0\}$) for all $i$. As usual we denote the affine and projective spaces over the field $K$ by $\mathbb{A}^s$ and $\mathbb{P}^{s-1}$, respectively. Points of the projective space $\mathbb{P}^{s-1}$ are denoted by $[\alpha]$, where $0 \neq \alpha \in K^s$. We consider the following sets parameterized by these rational functions:

(i) $\mathbb{X}$ is the set of all points $[(f_1(x)/g_1(x), \ldots, f_s(x)/g_s(x))]$ in $\mathbb{P}^{s-1}$ that are well defined, i.e., $x \in K^n$, $f_i(x) \neq 0$ for some $i$, and $g_i(x) \neq 0$ for all $i$. We call $\mathbb{X}$ the *projective set parameterized* by $F$.

(ii) $X$ is the set of all points $[(f_1(x)/g_1(x), \ldots, f_s(x)/g_s(x))]$ in $\mathbb{P}^{s-1}$ such that $x \in K^n$ and $f_i(x)g_i(x) \neq 0$ for all $i$. We call $X$ the *projective algebraic set parameterized* by $F$.

(iii) $\mathbb{X}^*$ is the set of all points $(f_1(x)/g_1(x), \ldots, f_s(x)/g_s(x))$ in $\mathbb{A}^s$ such that $x \in K^n$ and $g_i(x) \neq 0$ for all $i$. We call $\mathbb{X}^*$ *the affine set parameterized* by $F$.

(iv) $X^*$ is the set of all points $(f_1(x)/g_1(x), \ldots, f_s(x)/g_s(x))$ in $\mathbb{A}^s$ such that $x \in K^n$ and $f_i(x)g_i(x) \neq 0$ for all $i$. We call $X^*$ the *affine algebraic set parameterized* by $F$.

(v) $\overline{\phi(\mathbb{X}^*)}$ (resp. $\overline{\phi(X^*)}$), is the *projective closure* of $\mathbb{X}^*$ (resp. $X^*$), where $\phi\colon \mathbb{A}^s \to \mathbb{P}^s$ is the map given by $\alpha \mapsto [(\alpha, 1)]$.

The reason we are calling $X$ and $X^*$ the projective *algebraic* set and affine *algebraic* set, respectively, is to remind us that in certain cases $X$ and $X^*$ are *algebraic* groups acting on $\mathbb{X}$ and $\mathbb{X}^*$, respectively (e.g., when $K = \mathbb{C}$ and $f_i, g_i$ are monomials for all $i$).

Let $S = K[t_1, \ldots, t_s] = \oplus_{d=0}^{\infty} S_d$ be a polynomial ring over the field $K$ with the standard grading. The graded ideal $I(\mathbb{X})$ (resp. $I(X)$) generated by the homogeneous polynomials of $S$ that vanish at all points of $\mathbb{X}$ (resp. $X$) is called the *vanishing ideal* of $\mathbb{X}$ (resp. $X$). The *vanishing ideal* $I(\mathbb{X}^*)$ (resp. $I(X^*)$) is the ideal of $S$ of all polynomials that vanish at all points of $\mathbb{X}^*$ (resp. $X^*$). Thus $S/I(\mathbb{X})$ is a graded ring and $S/I(\mathbb{X}^*)$ is an affine ring.

There are good reasons to study vanishing ideals and their algebraic invariants (degree, Hilbert polynomial, regularity) over infinite and finite fields. They are used in algebraic geometry [34] and algebraic coding theory [29]. They are also used in polynomial interpolation problems as we briefly explain. Let $d \geq 1$ be an integer and let $Y = \{P_1, \ldots, P_m\}$ be a set of $m$ points in the affine space $\mathbb{A}^s$.

*Interpolation problem* Given scalars $b_1, \ldots, b_m$ in $K$, i.e., given $(b_1, \ldots, b_m)$ in $\mathbb{A}^m$, can we find a polynomial $f \in S$ of degree at most $d$ such that $f(P_i) = b_i$ for all $i$ ?

The answer to this problem can be given in terms of the regularity of $S/I(Y)$. The answer is positive if and only if $d \geq \operatorname{reg}^a S/I(Y)$ (see Section 1.5). Since the regularity of the affine ring $S/I(Y)$ is at most $m - 1$ the answer is positive if $d = m - 1$. The construction of an interpolating polynomial $f$ is a difficult task except when $s = 1$. For information about algebraic and computational aspects of polynomial interpolation in several variables see the survey article [19, Section 6] and [57]. For the interpolation problem over finite fields see [36].

The parameterized sets $X$ and $X^*$, and their vanishing ideals, were studied in [52] and [44], respectively, when $f_i$ and $g_i$ are monomials of $K[\mathbf{y}]$ for all $i$ and $K$ is a finite field, i.e., when $X$ and $X^*$ are parameterized by Laurent monomials over a finite field.

The contents of this chapter are as follows. In Section 2.1 we give a formula for the presentation ideal of the subring $K[F] \subset K(\mathbf{y})$, which is related to the rational implicitization problem [9, Theorem 2, p. 131] (see Proposition 2.1.2). It is known that the degree of a monomial subring $K[F]$ is independent of the field $K$ [51]. When $F$ is a set of polynomials this is no longer true, we show an example where the degree of the subring $K[F]$ depends on $K$ (see Example 2.1.4).

Some of the main contributions of this chapter are in determining formulas for the vanishing ideals of the parameterized sets $\mathbb{X}$, $X$, $\mathbb{X}^*$, $X^*$ introduced above (see Theorems 2.2.5, 2.2.10, 2.2.11, and 2.2.13 for the case of infinite fields, and Theorems 2.3.7, 2.3.10, 2.3.12, and 2.3.14 for the case of finite fields). For finite fields the first formulas for $I(X)$ and $I(X^*)$ were given in [52, Theorems 2.1] and [44, Theorem 3.4], respectively, when $X$ and $X^*$ are parameterized by monomials. We show the following relations among vanishing ideals

$$(I(\mathbb{X})\colon t_1\cdots t_s) = I(X) \ \text{ and } \ (I(\mathbb{X}^*)\colon t_1\cdots t_s) = I(X^*),$$

that is $I(X)$ (resp. $I(X^*)$) is the colon ideal of $I(\mathbb{X})$ (resp. $I(\mathbb{X}^*)$) with respect to $t_1\cdots t_s$ (see Definition 1.3.20, and Propositions 2.3.9 and 2.3.13).

Using the computer algebra system *Macaulay*2 [30], our results can be used to compute the degree, regularity, Hilbert polynomial, and a Gröbner basis of a vanishing ideal over a rational parameterization over a field $K$ (see Example 2.3.17). By the algebraic methods introduced in [52] (see Chapter 1), our results can also be used to compute the length and the dimension of a Reed-Muller-type code over a rational parameterization over a finite field $K$ (see Example 2.3.18). The formulas for vanishing ideal over finite fields that we give in this chapter were discovered by making experiments with *Macaulay*2.

Our main results are also useful from a theoretical point of view as we now explain. We are able to show the following results about the structure of vanishing ideals:

(a) Let $K$ be an infinite field and let $I \subset S$ be a graded ideal. Then $I$ is the vanishing ideal of a projective set in $\mathbb{P}^{s-1}$ parameterized by Laurent monomials if and only if $I$ is a prime ideal of $S$ generated by binomials (see Corollary 2.2.8), i.e., $I$ is a vanishing ideal if and only if $I$ is a toric ideal in the sense of [61, p. 31].

(b) If $K$ is an algebraically closed field and $\mathbb{X}^*$ is parameterized by Laurent monomials, using a result of Katsabekis and Thoma [39, 40], we show that the Zariski closure $\overline{\mathbb{X}^*}$ is parameterized by Laurent monomials (see Corollary 2.2.15).

(c) If $K$ is an infinite field, we give a method to compute the degree of $S/I(\overline{\phi(\mathbb{X}^*)})$, without using Gröbner bases, for any affine set $\mathbb{X}^*$ in $\mathbb{A}^s$ parameterized by Laurent monomials (see Corollary 2.2.21 and Remark 2.2.22). As an application we use this method to give a formula for the degree of the projective closure of a monomial curve (see Corollary 2.2.23).

(d) Let $K = \mathbb{F}_q$ be a finite field. If $\mathbb{X}$, $X$, $\mathbb{X}^*$, $X^*$ are parameterized by Laurent monomials, then $I(\mathbb{X})$, $I(X)$, $I(\mathbb{X}^*)$, $I(X^*)$ are binomial ideals (see Corollary 2.3.20).

(e) Let $K = \mathbb{F}_q$ be a finite field. If $\mathbb{X}$ is a projective set parameterized by Laurent monomials, then $I(\mathbb{X})$ is a radical Cohen-Macaulay binomial ideal of dimension 1 (see Corollary 2.3.21).

As another application we recover the following result:

(f) [52, Theorem 2.1] Let $K = \mathbb{F}_q$ be a finite field. If $X$ is a projective algebraic set parameterized by Laurent monomials, then $I(X)$ is a radical Cohen-Macaulay lattice ideal of dimension 1 (see Corollary 2.3.22). The converse is true by [49, Proposition 6.7].

We give a family of ideals where the converse of (e) is true; see Proposition 2.3.25. This leads us to pose the following conjecture.

*Conjecture* Let $K = \mathbb{F}_q$ be a finite field and let $\mathbb{Y}$ be a subset of $\mathbb{P}^{s-1}$. If $I(\mathbb{Y})$ is a binomial ideal, then $\mathbb{Y}$ is a projective set parameterized by Laurent monomials (see Conjecture 2.3.26).

This conjecture fails for infinite fields (see Example 2.2.9).

For a finite field $K = \mathbb{F}_q$ there are some rational parameterizations where the algebraic invariants and explicit sets of generators for $I(\mathbb{X})$, $I(X)$, $I(\mathbb{X}^*)$, and $I(X^*)$ are known. The simplest and more natural parameterization by rational functions occurs when $f_i = y_i$ and $g_i = 1$ for all $i$. In this case one has the following well-known descriptions [29, 37, 52, 55, 59]:

(i) $\mathbb{X} = \mathbb{P}^{s-1}$, deg $S/I(\mathbb{X}) = (q^s - 1)/(q-1)$, $\operatorname{reg} S/I(\mathbb{X}) = (s-1)(q-1)+1$, and

$$I(\mathbb{X}) = (t_i^q t_j - t_i t_j^q \,|\, 1 \leq i < j \leq s),$$

(ii) $X = T$, deg $S/I(X) = (q-1)^{s-1}$, $\operatorname{reg} S/I(X) = (s-1)(q-2)$, and

$$I(X) = (t_i^{q-1} - t_j^{q-1} \,|\, 1 \leq i < j \leq s),$$

(iii) $\mathbb{X}^* = \mathbb{A}^s = K^s$, deg $S/I(\mathbb{X}^*) = q^s$, $\operatorname{reg}^a S/I(\mathbb{X}^*) = s(q-1)$, and

$$I(\mathbb{X}^*) = (t_i^q - t_i \,|\, i = 1, \ldots, s),$$

(iv) $X^* = T^* = (K^*)^s$, deg $S/I(X^*) = (q-1)^s$, $\operatorname{reg}^a S/I(X^*) = s(q-2)$,

$$I(X^*) = (t_i^{q-1} - 1 \,|\, i = 1, \ldots, s),$$

where $T$ and $T^*$ are the *affine* and *projective torus* respectively, that is, $T^* = (K^*)^s$, $K^* = K \setminus \{0\}$, and $T$ is the image of $T^*$ under the map $\mathbb{A}^s \to \mathbb{P}^{s-1}$, $\alpha \mapsto [\alpha]$. In these four cases the minimum distance and the dimension of the corresponding Reed-Muller-type codes are also known (see [29, 52, 55, 59] and the references therein).

This suggests the following:

*Problem* If $K = \mathbb{F}_q$ and $f_i/g_i = y^{v_i}$ is a Laurent monomial for all $i$, find formulas for the algebraic invariants of a vanishing ideal and for the basic parameters of a Reed-Muller-type code of degree $d$, over the corresponding parameterization, in terms of $s$, $q$, $d$, and the combinatorics of $v_1, \ldots, v_s$.

This is an open problem where our results can be used to try to find formulas for the degree and the regularity of vanishing ideals (see Problem 2.3.29 and the discussion that follows), and for the dimension and length of Reed-Muller-type codes over finite fields. The degree is the easiest invariant to compute. Formulas for the degree of $S/I(X)$ are known when $y^{v_1}, \ldots, y^{v_s}$ are square-free monomials of degree 2 [50]. The regularity is harder to compute. Some formulas for the regularity of $S/I(X)$ are known when $X$ is parameterized by the edges of a graph (see [28, 49, 50] and the references therein).

If $f_i, g_i$ are monomials for all $i$, the sets $X$ and $\mathbb{X}$ are related as follows (a similar relation holds for $X^*$ and $\mathbb{X}^*$). Notice that in this situation $X$ is a multiplicative group under componentwise multiplication. The group $X$ acts on $\mathbb{X}$ by multiplication:

$$X \times \mathbb{X} \to \mathbb{X}, \quad ([\alpha], [\gamma]) \mapsto [\alpha] \cdot [\gamma],$$

where $[\alpha] = [(\alpha_1 \ldots, \alpha_s)]$, $[\gamma] = [(\gamma_1, \ldots, \gamma_s)]$ and $[\alpha] \cdot [\gamma] = [(\alpha_1\gamma_1, \ldots, \alpha_s\gamma_s)]$. If $K = \mathbb{F}_q$ is a finite field one can use this action to find a formula for the degree of $I(\mathbb{X})$ when $\mathbb{X}$ is parameterized by the edges of a complete graph or by the edges of a complete bipartite graph (see Propositions 2.3.27 and 2.3.28).

**Contents of Chapter 3** Reed-Muller-type evaluation codes have been extensively studied using commutative algebra methods (e.g., Hilbert functions, resolutions, Gröbner bases); see [7, 20, 52] and the references therein. In this work we use these methods—together with linear algebra techniques—to study projective Segre codes over finite fields. There are other works that have studied evaluation codes from the commutative algebra perspective [3, 33, 65].

Let $K$ be an arbitrary field, let $a_1, a_2$ be two positive integers, let $\mathbb{P}^{a_1-1}$, $\mathbb{P}^{a_2-1}$ be projective spaces over $K$, and let $K[\mathbf{x}] = K[x_1, \ldots, x_{a_1}]$, $K[\mathbf{y}] = K[y_1, \ldots, y_{a_2}]$, $K[\mathbf{t}] = K[t_{1,1}, \ldots, t_{a_1,a_2}]$ be polynomial rings with the standard grading. If $d \in \mathbb{N}$, let $K[\mathbf{t}]_d$ denote the set of homogeneous polynomials of total degree $d$ in $K[\mathbf{t}]$, together with the zero polynomial. Thus $K[\mathbf{t}]_d$ is a $K$-linear space and $K[\mathbf{t}] = \oplus_{d=0}^{\infty} K[\mathbf{t}]_d$. In this grading each $t_{i,j}$ is homogeneous of degree one.

Given $\mathbb{X}_i \subset \mathbb{P}^{a_i-1}$, $i = 1, 2$, denote by $I(\mathbb{X}_1)$ (resp. $I(\mathbb{X}_2)$) the *vanishing ideal* of $\mathbb{X}_1$ (resp. $\mathbb{X}_2$) generated by the homogeneous polynomials of $K[\mathbf{x}]$ (resp. $K[\mathbf{y}]$) that vanish at all points of $\mathbb{X}_1$ (resp. $\mathbb{X}_2$). The *Segre embedding* is given by

$$\begin{array}{rcl} \psi\colon \mathbb{P}^{a_1-1} \times \mathbb{P}^{a_2-1} & \to & \mathbb{P}^{a_1a_2-1} \\ ([\alpha_1, \ldots, \alpha_{a_1}], [\beta_1, \ldots, \beta_{a_2}]) & \to & [(\alpha_i\beta_j)], \end{array}$$

where $[(\alpha_i\beta_j)] := [(\alpha_1\beta_1, \alpha_1\beta_2, \ldots, \alpha_1\beta_{a_2}, \ldots, \alpha_{a_1}\beta_1, \alpha_{a_1}\beta_2, \ldots, \alpha_{a_1}\beta_{a_2})]$. The map $\psi$ is well-defined and injective [35, p. 13]. The image of $\mathbb{X}_1 \times \mathbb{X}_2$ under the map $\psi$, denoted by $\mathbb{X}$, is called the *Segre product* of $\mathbb{X}_1$ and $\mathbb{X}_2$. The vanishing ideal $I(\mathbb{X})$ of $\mathbb{X}$ is a graded ideal of $K[\mathbf{t}]$, where the $t_{i,j}$ variables are ordered as $t_{1,1},\ldots,t_{1,a_2},\ldots,t_{a_1,1},\ldots,t_{a_1,a_2}$. The Segre embedding is used in algebraic geometry to show that the product of projective varieties is again a projective variety, see [34, Lecture 2]. If $\mathbb{X}_i=\mathbb{P}^{a_i-1}$ for $i=1,2$, the set $\mathbb{X}$ is a projective variety and is called a *Segre variety* [34, p. 25]. The Segre embedding is used in coding theory to study the generalized Hamming weights of some product codes; see [58] and the references therein.

The contents of Chapter 3 are as follows. Let $K=\mathbb{F}_q$ be a finite field. In Section 3.1 we introduce linear codes and recall two results about the basic parameters and the second generalized Hamming weight of direct product codes (see Theorems 3.1.1 and 3.1.2). Then for an arbitrary field $K$ we show that $K[\mathbf{t}]/I(\mathbb{X})$ is the Segre product of $K[\mathbf{x}]/I(\mathbb{X}_1)$ and $K[\mathbf{y}]/I(\mathbb{X}_2)$ (see Definition 3.2.1 and Theorem 3.2.3). The Segre product of these two graded algebras is a subalgebra of

$$(K[\mathbf{x}]/I(\mathbb{X}_1))\otimes_K(K[\mathbf{y}]/I(\mathbb{X}_2)),$$

the tensor product algebra. Segre products have been studied by many authors; see [13, 29, 38] and the references therein. We give full proofs of two results for which we could not find a reference with the corresponding proof (see Lemma 3.1.4 and Theorem 3.2.3). Apart from this all results of this section are well known.

If $K=\mathbb{F}_q$ is a finite field, we introduce a family $\{C_{\mathbb{X}}(d)\}_{d\in\mathbb{N}}$ of projective Reed-Muller-type codes that we call *projective Segre codes* (see Definition 3.3.1). It turns out that $C_{\mathbb{X}}(d)$ is isomorphic to $K[\mathbf{t}]_d/I(\mathbb{X})_d$, as $K$-vector spaces, where $I(\mathbb{X})_d$ is equal to $I(\mathbb{X})\cap K[\mathbf{t}]_d$. Accordingly $C_{\mathbb{X}_1}(d)\simeq K[\mathbf{x}]_d/I(\mathbb{X}_1)_d$ and $C_{\mathbb{X}_2}(d)\simeq K[\mathbf{y}]_d/I(\mathbb{X}_2)_d$. In Section 3.3 we study the basic parameters (length, dimension, minimum distance) and the second generalized Hamming weight of projective Segre codes. Our main result expresses the basic parameters of $C_{\mathbb{X}}(d)$ in terms of those of $C_{\mathbb{X}_1}(d)$ and $C_{\mathbb{X}_2}(d)$, and shows that $C_{\mathbb{X}}(d)$ is the direct product of $C_{\mathbb{X}_1}(d)$ and $C_{\mathbb{X}_2}(d)$ (see Theorem 3.3.2); this means that the direct product of two projective Reed-Muller-type codes of degree $d$ is again a projective Reed-Muller-type code of degree $d$.

Formulas for the basic parameters of affine and projective Reed-Muller-type codes are known for a number of families [8, 10, 11, 12, 21, 23, 24, 27, 29, 43, 55, 59]. Since affine Reed-Muller-type codes can be regarded as projective Reed-Muller-type codes [44], our results can be applied to obtain explicit formulas for the basic parameters of $C_{\mathbb{X}}(d)$ if $C_{\mathbb{X}_1}(d)$ is in one of these families and $C_{\mathbb{X}_2}(d)$ is in another of these families or both are in the same family.

As an application we recover some results on Reed-Muller-type codes over projective tori and over the Segre variety [24, 25, 26, 29]. If $K^*=K\setminus\{0\}$ and $\mathbb{X}_i$ is the image of $(\mathbb{K}^*)^{a_i}$, under the map $(K^*)^{a_i}\to\mathbb{P}^{a_i-1}$, $x\to[x]$, we call $\mathbb{X}_i$ a *projective torus* in $\mathbb{P}^{a_i-1}$. In particular: If $\mathbb{X}_1=\mathbb{P}^{a_1-1}$ and $\mathbb{X}_2=\mathbb{P}^{a_2-1}$, using Theorem 3.3.2 we recover the formula for the minimum distance of $C_{\mathbb{X}}(d)$ given in [29, Theorem 5.1], and if $\mathbb{X}_i$ is a projective torus for $i=1,2$, using Theorem 3.3.2 we recover the formula for the minimum distance of $C_{\mathbb{X}}(d)$ given in [24, Theorem 5.5]. In these two cases formulas for the basic parameters of $C_{\mathbb{X}_i}(d)$, $i = 1, 2$, are given in [59, Theorem 1] and [55, Theorem 3.5], respectively. We also recover the formulas for the second generalized Hamming weight given in [25, Theorem 5.1] and [26, Theorem 3] (see Corollary 3.3.6).

**Contents of Chapter 4** Let $S = K[t_1, \ldots, t_s]$ be a polynomial ring over a field $K$ with the standard grading induced by setting $\deg(t_i) = 1$ for all $i$. By the *dimension* of an ideal $I \subset S$ we mean the Krull dimension of $S/I$. The affine and projective spaces over the field $K$ of dimensions $s$ and $s-1$ are denoted by $\mathbb{A}^s$ and $\mathbb{P}^{s-1}$, respectively. Points of $\mathbb{P}^{s-1}$ are denoted by $[\alpha]$, where $0 \neq \alpha \in \mathbb{A}^s$.

Given a set $\mathbb{Y} \subset \mathbb{P}^{s-1}$ define $I(\mathbb{Y})$, the *vanishing ideal* of $\mathbb{Y}$, as the graded ideal generated by the homogeneous polynomials in $S$ that vanish at all points of $\mathbb{Y}$. Conversely, given a homogeneous ideal $I \subset S$ define $V(I)$, the *zero set* of $I$, as the set of all $[\alpha] \in \mathbb{P}^{s-1}$ such that $f(\alpha) = 0$ for all homogeneous polynomial $f \in I$. The zero sets are the closed sets of the *Zariski topology* of $\mathbb{P}^{s-1}$. The Zariski closure of $\mathbb{Y}$ is denoted by $\overline{\mathbb{Y}}$.

We will use the following multi-index notation: for $a = (a_1, \ldots, a_s) \in \mathbb{Z}^s$, set $t^a = t_1^{a_1} \cdots t_s^{a_s}$. We call $t^a$ a *Laurent monomial*. If $a_i \geq 0$ for all $i$, $t^a$ is called a *monomial* of $S$. A *binomial* of $S$ is an element of the form $f = t^a - t^b$, for some $a, b$ in $\mathbb{N}^s$. An ideal $I \subset S$ generated by binomials is called a *binomial ideal*. A binomial ideal $I \subset S$ with the property that $t_i$ is not a zero-divisor of $S/I$ for all $i$ is called a *lattice ideal*.

In this chapter we classify binomial vanishing ideals in algebraic and geometric terms. There are some reasons to study vanishing ideals. They are used in algebraic geometry [34] and algebraic coding theory [29, 43]. They are also used in polynomial interpolation problems [19, 36, 63].

The set $\mathcal{S} = \mathbb{P}^{s-1} \cup \{[0]\}$ is a monoid under componentwise multiplication, that is, given $[\alpha] = [(\alpha_1, \ldots, \alpha_s)]$ and $[\beta] = [(\beta_1, \ldots, \beta_s)]$ in $\mathcal{S}$, the product operation is given by

$$[\alpha] \cdot [\beta] = [\alpha \cdot \beta] = [(\alpha_1\beta_1, \ldots, \alpha_s\beta_s)],$$

where $[\mathbf{1}] = [(1, \ldots, 1)]$ is the identity element. Accordingly the affine space $\mathbb{A}^s$ is also a monoid under componentwise multiplication.

The contents of this chapter are as follows. Let $\mathbb{Y}$ be a subset of $\mathbb{P}^{s-1}$. If $\mathbb{Y} \cup \{[0]\}$ is a submonoid of $\mathbb{P}^{s-1} \cup \{[0]\}$, we show that $I(\mathbb{Y})$ is a binomial ideal (Theorem 4.2.1). The same type of result holds if $Y$ is a subset of $\mathbb{A}^s$ (Remark 4.2.3). Then we show that $I(\mathbb{Y})$ is a binomial ideal if and only if $V(I(\mathbb{Y})) \cup \{[0]\}$ is a monoid under componentwise multiplication (Theorem 4.2.4). As a result if $\mathbb{Y}$ is finite, then $I(\mathbb{Y})$ is a binomial ideal if and only if $\mathbb{Y} \cup \{0\}$ is a monoid (Corollary 4.2.5). This essentially classifies all graded binomial vanishing ideals of dimension 1 (Corollary 4.2.6)

If $Y$ is a submonoid of an affine torus (see Definition 4.2.7), then $I(Y)$ is a non-graded lattice ideal [16, Proposition 2.3]. We give a graded version of this result, namely, if $\mathbb{Y}$ is a submonoid of a projective torus, then $I(\mathbb{Y})$ is a lattice ideal (Corollary 4.2.8).

Let $I(\mathbb{Y})$ be a vanishing ideal of dimension 1. According to [49, Proposition 6.7(a)] $I(\mathbb{Y})$ is a lattice ideal if and only if $\mathbb{Y}$ is a finite subgroup of a projective torus. We complement this result by showing that—over an algebraically closed field—$\mathbb{Y}$ is a finite subgroup of a projective torus if and only if there is a finite subgroup $H$ of $K^* = K \setminus \{0\}$ and Laurent monomials $y^{v_1}, \ldots, y^{v_s}$ that parameterize $\mathbb{Y}$ relative to $H$ (Proposition 4.2.10). For finite fields, this result was shown in [49, Proposition 6.7(b)].

Finally, we classify the graded lattice ideals of dimension 1 over an algebraically closed field of characteristic zero. It turns out that they are the vanishing ideals of finite subgroups of projective tori (Proposition 4.2.13).

**Contents of Chapter 5** Let $R = K[\mathbf{y}] = K[y_1, \ldots, y_n]$ be a polynomial ring over a finite field $K = \mathbb{F}_q$ and let $y^{v_1}, \ldots, y^{v_s}$ be a finite set of monomials in $K[\mathbf{y}]$. As usual we denote the affine and projective spaces over the field $K$ of dimensions $s$ and $s-1$ by $\mathbb{A}^s$ and $\mathbb{P}^{s-1}$, respectively. Points of the projective space $\mathbb{P}^{s-1}$ are denoted by $[\alpha]$, where $0 \neq \alpha \in \mathbb{A}^s$.

We consider a set $\mathbb{X}$, in the projective space $\mathbb{P}^{s-1}$, parameterized by $y^{v_1}, \ldots, y^{v_s}$. The set $\mathbb{X}$ consists of all points $[(x^{v_1}, \ldots, x^{v_s})]$ in $\mathbb{P}^{s-1}$ that are well defined, i.e., $x \in K^n$ and $x^{v_i} \neq 0$ for some $i$. The set $\mathbb{X}$ is called of *clutter type* if $\operatorname{supp}(y^{v_i}) \not\subset \operatorname{supp}(y^{v_j})$ for $i \neq j$, where $\operatorname{supp}(y^{v_i})$ is the *support* of the monomial $y^{v_i}$ consisting of the variables that occur in $y^{v_i}$. In this case we say that the set of monomials $y^{v_1}, \ldots, y^{v_s}$ is of *clutter type*. This terminology comes from the fact that the condition $\operatorname{supp}(y^{v_i}) \not\subset \operatorname{supp}(y^{v_j})$ for $i \neq j$ means that there is a *clutter* $\mathcal{C}$, in the sense of [55], with vertex set $V(\mathcal{C}) = \{y_1, \ldots, y_n\}$ and edge set

$$E(\mathcal{C}) = \{\operatorname{supp}(y^{v_1}), \ldots, \operatorname{supp}(y^{v_s})\}.$$

A clutter is also called a *simple hypergraph*, see Definition 5.2.7.

Let $S = K[t_1, \ldots, t_s] = \oplus_{d=0}^{\infty} S_d$ be a polynomial ring over the field $K$ with the standard grading. The graded ideal $I(\mathbb{X})$ generated by the homogeneous polynomials of $S$ that vanish at all points of $\mathbb{X}$ is called the *vanishing ideal* of $\mathbb{X}$.

There are good reasons to study vanishing ideals over finite fields. They are used in algebraic coding theory [29] and in polynomial interpolation problems [19, 63]. The Reed-Muller-type codes arising from vanishing ideals on monomial parameterizations have received a lot of attention [7, 10, 21, 29, 43, 52, 55, 59].

The vanishing ideal $I(\mathbb{X})$ is a *complete intersection* if $I(\mathbb{X})$ is generated by $s-1$ homogeneous polynomials. Notice that $s-1$ is the height of $I(\mathbb{X})$ in the sense of [47]. The interest in complete intersection vanishing ideals over finite fields comes from information and communication theory, and algebraic coding theory [12, 23, 33].

Let $T$ be a projective torus in $\mathbb{P}^{s-1}$ (see Definition 4.2.7) and let $\mathbb{X}$ be the set in $\mathbb{P}^{s-1}$ parameterized by a clutter $\mathcal{C}$ (see Definition 5.2.8). Consider the set $X = \mathbb{X} \cap T$. In [55] it is shown that $I(X)$ is a complete intersection if and only if $X$ is a projective torus in $\mathbb{P}^{s-1}$ . If the clutter $\mathcal{C}$ has all its edges of the same cardinality, in [56] a classification of the complete intersection property of $I(X)$ is given using linear algebra.

The main result of this chapter is a classification of the complete intersection property of $I(\mathbb{X})$ when $\mathbb{X}$ is of clutter type (Theorem 5.2.17). Using the techniques of [52], this classification can be used to study the *basic parameters* [46, 66] of the Reed-Muller-type codes associated to $\mathbb{X}$.

**Contents of Chapter 6** In this chapter we present a number of problems on vanishing ideals for future works.

**Main references** For all unexplained terminology and for additional information, we refer to [13, 15, 41, 62] (for computational commutative algebra), [9, 60] (for Hilbert functions), [9, 34] (for Gröbner bases, algebraic geometry, and vanishing ideals), [5, 34, 47] (for commutative algebra), [13, Appendix 2] (for multilinear algebra), [16, 51, 70] (for binomial and lattice ideals), and [46, 52, 66] (for vanishing ideals and coding theory).

# Contents

# Chapter 1

# Preliminaries

In this chapter, we present some of the results that will be needed throughout this work and introduce some notation. The main topics are graded modules, Gröbner bases, projective closure, vanishing ideals, and Hilbert functions. The family of Reed-Muller-type codes is introduced here, and its relation to Hilbert functions and vanishing ideals is discussed. All results of this section are well-known.

## 1.1 Noetherian rings and modules

Let $S$ be a commutative ring with unit and let $M$ be an $S$-module. Recall that $M$ is called *Noetherian* if every submodule $N$ of $M$ is finitely generated, that is, $N = Sf_1 + \cdots + Sf_s$, for some $f_1, \ldots, f_s$ in $N$.

**Theorem 1.1.1.** *The following conditions are equivalent:*

(a) *$M$ is Noetherian.*

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

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

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

(c) *Any family $\mathcal{F}$ of submodules of $M$ partially ordered by inclusion has a maximal element, i.e., there is $N \in \mathcal{F}$ such that if $N \subset N_i$ and $N_i \in \mathcal{F}$, then $N = N_i$.*

**Proof.** (a)⇒(b): Consider the submodule $N = \cup_{i \geq 0} N_i$. By hypothesis there are $m_1, \ldots, m_r$ such that $N = Sm_1 + \cdots + Sm_r$. Then, there is $k$ such that $m_i \in N_k$ for all $i$. It follows that $N_i = N_k$ for all $i \geq k$.

(b)⇒(c): Let $N_1 \in \mathcal{F}$. If $N_1$ is not maximal, there is $N_2 \in \mathcal{F}$ such that $N_1 \subsetneq N_2$. If $N_2$ is not maximal, there is $N_3 \in \mathcal{F}$ such that $N_2 \subsetneq N_3$. Applying this argument repeatedly we get that $\mathcal{F}$ has a maximal element.

(c)$\Rightarrow$(a): Let $N$ be a submodule of $M$ and let $\mathcal{F}$ be the family of submodules of $N$ that are finitely generated. By hypothesis $\mathcal{F}$ has a maximal element $N'$. It follows that $N = N'$. □

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

$$I = \{a_1 f_1 + \cdots + a_s f_s |\ a_i \in S, \forall\, i\}\,.$$

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

**Theorem 1.1.2.** (Hilbert's basis theorem [2, Theorem 7.5]) *A polynomial ring $S[t]$ over a Noetherian ring $S$ is Noetherian.*

One of the important examples of a Noetherian ring is a polynomial ring over a field $k$. Often we will denote a polynomial ring in several variables by $k[\mathbf{t}]$ and a polynomial ring in one variable by $k[t]$. The letters $k$ and $K$ will always denote fields.

## 1.2 Graded modules

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

$$S = \bigoplus_{a \in H} S_a \quad \text{(as a } \mathbb{Z}\text{-module)},$$

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

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

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

such that $S_a M_b \subset M_{a+b}$ 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 $S_a$ 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 $f_a \neq 0$.

**Definition 1.2.1.** Let $M = \oplus_{a \in H} M_a$ be an $H$-graded module. A submodule $N \subset M$ is called a *graded submodule* if $N$ is generated over $S$ by homogeneous elements.

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*. Then $M/N$ is an $H$-graded $S$-module with $(M/N)_a = M_a / N \cap M_a$ for $a \in H$, $S_0 \subset S$ is a subring and $M_a$ is an $S_0$-module for $a \in H$.

**Proposition 1.2.2.** *Let $M = \oplus_{a\in H} M_a$ be an $H$-graded module and $N \subset M$ a submodule. Then the following three conditions are equivalent.*

(g$_1$) *$N$ is generated over $S$ by homogeneous elements.*

(g$_2$) *$N$ is graded with the induced grading. $N = \oplus_{a\in H} N \cap M_a$.*

(g$_3$) *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 $N$.*

Let $S = K[t_1, \ldots, t_s]$ be a polynomial ring over a field $K$ and let $d_1, \ldots, d_s$ be a sequence in $\mathbb{N}_+$. For $a = (a_i)$ in $\mathbb{N}^s$ we set $t^a = t_1^{a_1} \cdots t_s^{a_s}$ and $|a| = \sum_{i=1}^s a_i d_i$. The *induced* $\mathbb{N}$-*grading* on $S$ is given by:

$$S = \bigoplus_{i=0}^{\infty} S_i, \text{ where } S_i = \bigoplus_{|a|=i} K t^a.$$

Notice that $\deg(t_i) = d_i$ for all $i$. The induced grading extends to a $\mathbb{Z}$-grading by setting $S_i = 0$ for $i < 0$. The homogeneous elements of $S$ are called *quasi-homogeneous polynomials*. Let $I$ be a *homogeneous* ideal of $S$ 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

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

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

**Definition 1.2.3.** The *standard grading* or *usual grading* of a polynomial ring $K[t_1, \ldots, t_s]$ is the $\mathbb{N}$-grading induced by setting $\deg(t_i) = 1$ for all $i$.

## 1.3 Gröbner bases

In this section we review some basic facts and definitions on Gröbner bases. Our main references are [9, 17].

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

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

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

**Definition 1.3.1.** 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* $t^{\alpha_1}$ of $f$ is denoted by $\mathrm{in}_\prec(f)$ or $\mathrm{lm}_\prec(f)$, or simply by $\mathrm{in}(f)$. The *leading coefficient* $\lambda_1$ 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 1.3.2.** 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 1.3.3** (Dickson). *If $\{t^{\alpha_i}\}_{i=1}^{\infty}$ is a sequence in $\mathbb{M}_s$, then there is an integer $k$ so that $t^{\alpha_i}$ 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 1.1.2). 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 $t^{\alpha_i}$ is a multiple of $t^{\alpha_j}$. □

**Definition 1.3.4.** Let $f$, $g$ be two polynomials in $S$ and 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 $f \to_{\mathcal{F}} g$ , 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 $\lambda$.

**Proposition 1.3.5.** *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 $i$th 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 1.3.6.** (Division algorithm [17, Theorem 2.11]) *If $f, f_1, \ldots, f_s$ are polynomials in $S$, then $f$ can be written as*

$$f = a_1 f_1 + \cdots + a_s f_s + r,$$

*where $a_i, r \in S$ and either $r = 0$ or $r \neq 0$ and no term of $r$ is divisible by one of* $\mathrm{in}(f_1), \ldots, \mathrm{in}(f_s)$*. Furthermore if $a_i f_i \neq 0$, then* $\mathrm{in}(f) \succeq \mathrm{in}(a_i f_i)$.

**Definition 1.3.7.** The polynomial $r$ in the division algorithm is called a *remainder* of $f$ with respect to $\mathcal{F} = \{f_1, \ldots, f_s\}$.

**Definition 1.3.8.** 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

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

**Definition 1.3.9.** A Gröbner basis $\mathcal{G} = \{g_1, \ldots, g_r\}$ of an ideal $I$ is called a *reduced Gröbner basis* for $I$ if:

(i) $\mathrm{lc}(g_i) = 1\ \forall i$, and

(ii) none of the terms occurring in $g_i$ belongs to $\mathrm{in}_\prec(\mathcal{G} \setminus \{g_i\})\ \forall i$.

**Theorem 1.3.10.** [17, Theorem 2.17] *Each ideal $I$ has a unique reduced Gröbner basis.*

**Definition 1.3.11.** Let $f, g \in S \setminus \{0\}$ and let $[t^a, t^b] = \mathrm{lcm}(t^a, t^b)$ be the least common multiple of the monomials $t^a$ and $t^b$. The S-*polynomial* of $f$ and $g$ is given by

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

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

**Theorem 1.3.12.** (Buchberger [6]) If $\mathcal{F} = \{f_1, \ldots, f_s\}$ 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: $\mathcal{G} := \mathcal{F}$,   $B := \{\{f_i, f_j\} \mid f_i \neq f_j \in \mathcal{G}\}$
while $B \neq \emptyset$ do
  pick any $\{f, g\} \in B$
  $B := B \setminus \{\{f, g\}\}$
  $r :=$ remainder of $\mathrm{S}(f, g)$ with respect to $\mathcal{G}$
  if $r \neq 0$ then
    $B := B \cup \{\{r, h\} \mid h \in \mathcal{G}\}$
    $\mathcal{G} := \mathcal{G} \cup \{r\}$
```

**Proposition 1.3.13.** *Let $I$ be an ideal of $S$ and let $\mathcal{F} = \{f_1, \ldots, f_s\}$ be a Gröbner basis of $I$. If*

$$\mathcal{B} = \{\overline{u} \mid u \in \mathbb{M}_n \text{ and } u \notin (\mathrm{in}(f_1), \ldots, \mathrm{in}(f_s))\},$$

*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 "$\longrightarrow_{\mathcal{F}}$" is Noetherian, we can write $f = \sum_{i=1}^{s} a_i f_i + \sum_{i=1}^{r} \lambda_i u_i$, where $\lambda_i \in K^*$ and such that every $u_i$ is a term which is not a multiple of any of the terms $\mathrm{in}(f_j)$. 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 $h = \sum_{i=1}^{s} \lambda_i u_i \in I$, where $\overline{u}_i \in \mathcal{B}$ and $\lambda_i \in K$. We must show $\lambda_i = 0$, for all $i$. If not, then we can label the $u_i$'s so that $u_1 \succ \cdots \succ u_s$ and $\lambda_1 \neq 0$. Hence $\mathrm{in}(h) = u_1 \in \mathrm{in}(I)$, but this is a clear contradiction because $\mathrm{in}(I) = (\mathrm{in}(f_1), \ldots, \mathrm{in}(f_s))$. Therefore $\lambda_i = 0$, for all $i$, as required. □

**Definition 1.3.14.** A monomial in $\mathcal{B}$ is called a *standard monomial* with respect to $f_1, \ldots, f_s$.

**Corollary 1.3.15** (Macaulay)**.** *If $I$ is a graded ideal of $S$, then $S/I$ and $S/\mathrm{in}_{\prec}(I)$ have the same Hilbert function.*

**Lemma 1.3.16.** [17, Proposition 2.15] *Let $f$, $g$ be polynomials in $S$ and let $\mathcal{F} = \{f, g\}$. If $\mathrm{in}(f)$ and $\mathrm{in}(g)$ are relatively prime, then $\mathrm{S}(f, g) \to_{\mathcal{F}} 0$.*

**Theorem 1.3.17.** [6] *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*

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

**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 1.3.18.** *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 $\mathrm{in}(I^c)$, there is $f \in I^c$ with $\mathrm{lm}(f) = M$. Hence $M = m\,\mathrm{lm}(g)$ 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 $\alpha$ and $\beta$ we obtain $g \in \mathcal{G} \cap S$, that is, $M \in (\mathrm{in}(\mathcal{G} \cap S))$. Thus $\mathrm{in}(I^c) = (\mathrm{in}(\mathcal{G} \cap S))$, as required. □

**Example 1.3.19.** Let $\prec$ be the *elimination order* with respect to $x_1, \ldots, x_4$. Using *Macaulay*2 [30], 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 1.3.18, it follows that $I \cap K[t_1, \ldots, t_6] = (t_3t_4 - t_1t_6, t_2t_5 - t_1t_6)$.

**Definition 1.3.20.** Let $I$ and $J$ be two ideals of a ring $S$. The ideal

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

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 1.3.21.** 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 1.3.22.** *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

$$gf^m = b_1 f_1 + \cdots + b_s f_s,$$

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 $g \in (I, 1 - tf) \cap S$. □

**Definition 1.3.23.** A *binomial* of $S$ is a polynomial of the form $t^a - t^b$ for some $a, b \in \mathbb{N}^s$. An ideal of $S$ generated by binomials is called a *binomial ideal.*

**Lemma 1.3.24.** *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 1.3.12) 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 1.3.18) $\mathcal{G} \cap K[\mathbf{t}]$ is a Gröbner basis of $I \cap K[\mathbf{t}]$. Hence $I \cap K[\mathbf{t}]$ is a binomial ideal. □

## 1.4 Hilbert functions

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 $\binom{d+s-1}{s-1}$. Let $I$ be an ideal on S. 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.

According to [31, Remark 5.3.16, p. 330], there are unique polynomials

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

of degrees $k$ and $k-1$, respectively, such that $k$ is the *Krull dimension* of the affine ring $S/I$, $h_I^a(i) = H_I^a(i)$, and $h_I(i) = H_I(i)$ for $i \gg 0$. The polynomials $h_I^a$ and $h_I$ are called the *affine Hilbert polynomial* and the *Hilbert polynomial* of $S/I$. By convention, the zero polynomial has degree $-1$. The Krull dimension of the ring $S/I$ is denoted by $\dim(S/I)$. The *height* of $I$, denoted $\mathrm{ht}(I)$, is $\dim(S)-\dim(S/I)$. By the *dimension* of an ideal $I \subset S$ we mean the dimension of $S/I$.

**Definition 1.4.1.** The integer $a_k(k!)$, denoted by $\deg(S/I)$, is called the *degree* of $S/I$.

**Remark 1.4.2.** 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 1.4.3.** 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 $d \geq r$.

If $S$ has the standard grading and $I$ is a graded Cohen-Macaulay ideal of $S$ of dimension 1, then $\mathrm{reg}(S/I)$, the Castelnuovo-Mumford regularity of $S/I$ in the sense of [14], is equal to the regularity index of $S/I$ (see [14]). In this case we call $\mathrm{ri}(S/I)$ (resp. $\mathrm{ri}^a(S/I)$) the regularity (resp. affine regularity) of $S/I$ and denote this number by $\mathrm{reg}(S/I)$ (resp. $\mathrm{reg}^a(S/I)$). If $I$ is graded its regularity is related to the degrees of the polynomials in a minimal generating set of $I$ [14].

**Remark 1.4.4.** If $I$ is graded, we let $I_d := I \cap S_d$, denote the set of homogeneous polynomials in $I$ of total degree $d$, together with the zero polynomial. Note that $I_d$ is a vector subspace of $S_d$ and

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

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

**Definition 1.4.5.** 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 1.4.6.** (Hilbert-Serre [70, Theorem 5.1.4]) *Let $I \subset S$ be a graded ideal. Then there is a unique polynomial $h(t) \in \mathbb{Z}[t]$ such*

$$F_I(t) = \frac{h(t)}{(1-t)^{\rho}} \quad \textit{and} \quad h(1) \neq 0,$$

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

**Definition 1.4.7.** 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., $a(S/I) = \deg(h(t)) - \rho$.

**Lemma 1.4.8.** *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

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

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

**Lemma 1.4.9.** [70, Corollary 5.1.9] *Let $I \subset S$ be a graded ideal. Then* $\mathrm{ri}(S/I) = 0$ *if* $a(S/I) < 0$*, and* $\mathrm{ri}(S/I) = a(S/I) + 1$ *otherwise.*

**Lemma 1.4.10.** *Let $I \subset S$ be a graded ideal. If* $\dim(S/I) = 1$ *and* $\deg(S/I) \geq 2$*, then* $\mathrm{ri}(S/I) = \mathrm{ri}^a(S/I) + 1$.

**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 1.4.8 and 1.4.9 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. $\square$

**Proposition 1.4.11.** ([31, Lemma 5.3.11], [51]) *If $I$ is an ideal of $S$ and $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$ is a minimal primary decomposition, then*

$$\deg(S/I) = \sum_{\mathrm{ht}(\mathfrak{q}_i)=\mathrm{ht}(I)} \deg(S/\mathfrak{q}_i).$$

### Hilbert functions of vanishing ideals

**Definition 1.4.12.** Let $K$ be a field. We define the *projective space* of dimension $s-1$ over $K$, denoted by $\mathbb{P}_K^{s-1}$ or $\mathbb{P}^{s-1}$ if $K$ is understood, to be the quotient space

$$(K^s \setminus \{0\})/\sim$$

where two points $\alpha$, $\beta$ 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 $\alpha$ by $[\alpha]$.

**Definition 1.4.13.** An ideal $I \subset S$ is *graded* if $I$ is generated by homogeneous polynomials.

**Proposition 1.4.14.** [47, p. 92] *Let $I \subset S$ be an ideal. The following conditions are equivalent*:

(g$_1$) *$I$ is a graded ideal.*

(g$_2$) *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 $I$.*

For any set $\mathbb{Y} \subset \mathbb{P}^{s-1}$ define $I(\mathbb{Y})$, the *vanishing ideal* of $\mathbb{Y}$, as the graded 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*. In a similar way we can define affine varieties, vanishing ideals of subsets of the affine space $\mathbb{A}^s$, and the corresponding Zariski topology of $\mathbb{A}^s$. 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 1.4.15.** (a) [9, pp. 191–192] *Let $K$ be a field. If $Y \subset \mathbb{A}^s$ and $\mathbb{Y} \subset \mathbb{P}^{s-1}$, then $\overline{Y} = V(I(Y))$ and $\overline{\mathbb{Y}} = V(I(\mathbb{Y}))$.*

(b) *If $K$ is a finite field, then $Y = V(I(Y))$ and $\mathbb{Y} = V(I(\mathbb{Y}))$.*

**Proof.** Part (b) follows from (a) because $\overline{Y} = Y$ and $\overline{\mathbb{Y}} = \mathbb{Y}$, if $K$ is finite. □

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 1.4.16.** (The Dimension Theorem [9, p. 434]) *Let $K$ be an algebraically closed field. If $\mathbb{Y} = V(I)$ is a projective variety in $\mathbb{P}^{s-1}$ (resp. $Y = V(I)$ is an affine variety in $\mathbb{A}^s$), then* $\dim(\mathbb{Y}) = \dim(S/I) - 1$ *(resp.* $\dim(Y) = \dim(S/I)$*).*

**Corollary 1.4.17.** [22] *If $\mathbb{Y} \subset \mathbb{P}^{s-1}$ is a finite set, then* $\deg(S/I(\mathbb{Y})) = |\mathbb{Y}|$.

**Proof.** It follows from the additivity of the degree (see Proposition 1.4.11). □

**Proposition 1.4.18.** ([12], [22], [45]) *If $X$ is a finite set and* $r = \operatorname{reg}(S/I(X))$*, then*

$$1 = H_X(0) < H_X(1) < \cdots < H_X(r-1) < H_X(d) = |X|$$

*for $d \geq r$ and* $\deg(S/I(X)) = |X|$.

**Lemma 1.4.19.** *If $\emptyset \neq \mathbb{Y} \subset \mathbb{P}^{s-1}$ 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 1.4.11). Hence, by Corollary 1.4.17, $H_I(d) = a_0 + 1$ 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 Corollary 1.4.17 one has equality. □

**Projective closure and Gröbner bases.** We will use the following multi-index notation: for $a = (a_1, \ldots, a_s) \in \mathbb{Z}^s$, set $t^a = t_1^{a_1} \cdots t_s^{a_s}$. We call $t^a$ a *Laurent monomial*. If $a_i \geq 0$ for all $i$, $t^a$ is a *monomial* of $S$.

**Definition 1.4.20.** 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 $S$. Given an ideal $I \subset S$ and $f \in S$, we denote the initial ideal of $I$ (resp. leading monomial of $f$) by $\operatorname{in}_\prec(I)$ (resp. $\operatorname{in}_\prec(f)$). We refer to [9] for the theory of Gröbner bases. For $f \in S$ of degree $e$ define

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

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 and the degrees of $I$ and $I^h$ are nicely related.

**Proposition 1.4.21.** ([51, Lemma 2.4], [69, Proposition 2.4.26]) *Let $I$ be an ideal of $S$ and let $\succ$ be the GRevLex order on $S$ and $S[u]$, respectively.*

(a) *If $g_1, \ldots, g_r$ is a Gröbner basis of $I$, then $g_1^h, \ldots, g_r^h$ is a Gröbner basis of $I^h$.*

(b) *$H_I^a(d) = H_{I^h}(d)$ for $d \geq 0$.*

(c) $\deg(S/I) = \deg(S[u]/I^h)$.

**Definition 1.4.22.** Let $Y \subset \mathbb{A}^s$. The *projective closure* of $Y$ is defined as $\overline{\phi(Y)}$, where $\phi$ is the map $\phi\colon \mathbb{A}^s \to \mathbb{P}^s$, $\alpha \mapsto [(\alpha, 1)]$, and $\overline{\phi(Y)}$ is the closure of $\phi(Y)$ in the Zariski topology.

**Proposition 1.4.23.** *Let $Y \subset \mathbb{A}^s$ be a set, let $\overline{\phi(Y)} \subset \mathbb{P}^s$ be its projective closure and let $f_1, \ldots, f_r$ be a Gröbner basis of $I(Y)$. The following hold.*

(a) [69, Proposition 2.4.30] $I(\overline{\phi(Y)}) = I(Y)^h = (f_1^h, \ldots, f_r^h)$.

(b) [69, Corollary 2.4.31] *The height of $I(Y)$ in $S$ is equal to the height of $I(\overline{\phi(Y)})$ in $S[u]$.*

## 1.5 Reed-Muller-type codes

In this part we introduce the families of projective and affine Reed-Muller-type codes and its connection to vanishing ideals and Hilbert functions.

**Projective Reed-Muller-type codes.** Let $K = \mathbb{F}_q$ be a finite field as usual and let $\mathbb{Y} = \{P_1, \ldots, P_m\} \neq \emptyset$ a subset of $\mathbb{P}^{s-1}$ with $m = |\mathbb{Y}|$. Fix a degree $d \geq 1$. For each $i$ there is $f_i \in S_d$ such that $f_i(P_i) \neq 0$; we refer to Section 3.3 to see a convenient way to choose $f_1, \ldots, f_m$. There is a well-defined $K$-linear map:

$$\mathrm{ev}_d\colon S_d = K[t_1, \ldots, t_s]_d \to K^{|\mathbb{Y}|}, \qquad f \mapsto \left(\frac{f(P_1)}{f_1(P_1)}, \ldots, \frac{f(P_m)}{f_m(P_m)}\right). \tag{1.5.1}$$

The map $\mathrm{ev}_d$ is called an *evaluation map*. The image of $S_d$ under $\mathrm{ev}_d$, denoted by $C_{\mathbb{Y}}(d)$, is called a *projective Reed-Muller-type code* of degree $d$ over the set $\mathbb{Y}$ [12, 29]. It is also called an *evaluation code* associated to $\mathbb{Y}$ [23]. The kernel of the evaluation map $\mathrm{ev}_d$ is $I(\mathbb{Y})_d$. Hence there is an isomorphism of $K$-vector spaces $S_d/I(\mathbb{Y})_d \simeq C_{\mathbb{Y}}(d)$. If $\mathbb{Y}$ is a subset of $\mathbb{P}^{s-1}$ it is usual to denote the Hilbert function $S/I(\mathbb{Y})$ by $H_{\mathbb{Y}}$. Thus $H_{\mathbb{Y}}(d)$ is equal to $\dim_K C_{\mathbb{Y}}(d)$. By a *linear code* we mean a linear subspace of $K^m$ for some $m$ and for some finite field $K$.

**Definition 1.5.1.** Let $0 \neq v \in C_{\mathbb{Y}}(d)$. The *Hamming weight* of $v$, denoted 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

$$\delta_{\mathbb{Y}}(d) := \min\{\omega(v)\colon 0 \neq v \in C)\}.$$

**Definition 1.5.2.** 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 [59, Theorem 1]. If $\mathbb{Y}$ is a projective torus, $C_{\mathbb{Y}}(d)$ is the *generalized projective Reed–Solomon code*, and formulas for its basic parameters are given in [55, Theorem 3.5].

The following summarizes the well-known relation between projective Reed-Muller-type codes and the theory of Hilbert functions.

**Proposition 1.5.3.** ([29], [52]) *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 Cohen–Macaulay graded ring of dimension* 1.

(v) $C_{\mathbb{Y}}(d) \neq (0)$ *for* $d \geq 1$.

**Proof.** (i): The kernel of the evaluation map $\mathrm{ev}_d$, defined in Eq. (1.5.1), is precisely $I(\mathbb{Y})_d$. Hence there is an isomorphism of $K$-vector spaces $S_d/I(\mathbb{Y})_d \simeq C_{\mathbb{Y}}(d)$. Thus $H_{\mathbb{Y}}(d)$ is equal to $\dim_K C_{\mathbb{Y}}(d)$.

(ii): This follows readily from Proposition 1.4.18.

(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): Let $[P]$ be a point in $\mathbb{Y}$, with $P = (\alpha_1, \ldots, \alpha_s)$ and $\alpha_k \neq 0$ for some $k$, and let $I_{[P]}$ be the ideal generated by the homogeneous polynomials of $S$ that vanish at $[P]$. Then $I_{[P]}$ is a prime ideal of height $s-1$,

$$I_{[P]} = (\{\alpha_k t_i - \alpha_i t_k |\, k \neq i \in \{1, \ldots, s\}),\ I(\mathbb{Y}) = \bigcap_{[Q]\in\mathbb{Y}} I_{[Q]}, \tag{1.5.2}$$

and the latter is the primary decomposition of $I(\mathbb{Y})$. As $I_{[P]}$ has height $s-1$ for any $[P] \in \mathbb{Y}$, we get that the height of $I(\mathbb{Y})$ is $s-1$ and the dimension of $S/I(\mathbb{Y})$ is 1. Hence $\operatorname{depth}(S/I(\mathbb{Y})) \leq 1$. To complete the proof notice that, by Eq. (2.3.5), $\mathfrak{m} = (t_1, \ldots, t_s)$ 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): This follows readily from Proposition 1.4.18. □

**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*

$$\mathrm{ev}_d^a \colon S_{\leq d} \longrightarrow K^{|Y|}, \qquad f \mapsto (f(P_1), \ldots, f(P_m)),$$

defines a linear map of $K$-vector spaces. The image of $\mathrm{ev}_d^a$, denoted by $C_Y(d)$, defines a *linear code*. We call $C_Y(d)$ the *affine Reed-Muller-type code* of degree $d$ on $Y$ [66, p. 37]. The kernel of $\mathrm{ev}_d^a$ is $I(Y)_{\leq d}$. Thus $S_{\leq d}/I(Y)_{\leq d} \simeq C_Y(d)$. If $Y$ is a subset of $\mathbb{A}^s$ it is usual to denote the affine Hilbert function $S/I(Y)$ by $H_Y^a$. In our situation one has $H_Y^a(d) = \dim_K C_Y(d)$.

The linear code $C_Y(d)$ has the same basic parameters that $C_{\mathbb{Y}}(d)$, the projective Reed-Muller-type code of degree $d$ on $\mathbb{Y}$ (see [44, 43]). This means that affine Reed-Muller-type codes are a particular case of projective Reed-Muller-type codes and are somewhat easier to understand.

The following result reduces the computation of the algebraic invariants of $S/I(Y)$ to the computation of those of $S[u]/I(\mathbb{Y})$.

**Proposition 1.5.4.** (a) *$I(\mathbb{Y}) = I(Y)^h$,*

(b) *$|Y| = \deg\, S/I(Y) = \deg\, S[u]/I(\mathbb{Y}) = |\mathbb{Y}|$,*

(c) *$H_Y^a(d) = H_{\mathbb{Y}}(d)$ for $d \geq 0$,*

(d) *$\mathrm{reg}^a\, S/I(Y) = \mathrm{reg}\, S[u]/I(\mathbb{Y})$.*

**Proof.** This follows from Propositions 1.4.21 and 1.4.23. □

The computation of the regularity of $S[u]/I(\mathbb{Y})$ is important for applications to coding theory: for $d \geq \mathrm{reg}\, S[u]/I(\mathbb{Y})$ the linear code $C_Y(d)$ coincides with the underlying vector space $K^{|Y|}$ and has, accordingly, minimum distance equal to 1. Thus, potentially good codes $C_Y(d)$ can occur only if $1 \leq d < \mathrm{reg}(S[u]/I(\mathbb{Y}))$.

**Interpolation problems.** Let $K$ be an arbitrary field, let $Y = \{P_1, \ldots, P_m\}$ be a finite set of points in $\mathbb{A}^s$, and let $\mathbb{Y}$ be the projective closure of $Y$.

The regularity also plays an important role in interpolation problems.

*Interpolation Problem.* Given scalars $b_1, \ldots, b_m$ in $K$, i.e., given $(b_1, \ldots, b_m)$ in $\mathbb{A}^m$, can we find a polynomial $f \in S$ of degree at most $d$ such that $f(P_i) = b_i$ for all $i$?

The answer to this problem is positive if and only if $d \geq \mathrm{reg}\, S[u]/I(\mathbb{Y})$. Indeed the Hilbert function of $S[u]/I(\mathbb{Y})$ is strictly increasing for $i = 1, \ldots, r$, where $r$ is the regularity of $S[u]/I(\mathbb{Y})$, and $H_{\mathbb{Y}}(d) = |Y|$ for $d \geq r$ (see [12, 22]). Thus $C_Y(d) = K^m$ if and only if $H_Y^a(d) = m$, that is, $C_Y(d) = K^m$ if and only if $d \geq r$. Since the regularity of $S[u]/I(\mathbb{Y})$ is at most $m - 1$ the answer to this problem is positive if $d = m - 1$.

**Degree and regularity via Hilbert series.** The degree and regularity of $S[u]/I(\mathbb{Y})$ can be read off from its Hilbert series. Indeed, the Hilbert series can be written as

$$F_{\mathbb{Y}}(t) := \sum_{i=0}^{\infty} H_{\mathbb{Y}}(i)t^i = \sum_{i=0}^{\infty} \dim_K(S[u]/I(\mathbb{Y}))_i t^i = \frac{h_0 + h_1 t + \cdots + h_r t^r}{1-t},$$

where $h_0, \ldots, h_r$ are positive integers; see [60]. This follows from the fact that $I(\mathbb{Y})$ is a Cohen-Macaulay ideal of height $s$ [22]. The number $r$ is the regularity of $S[u]/I(\mathbb{Y})$ and $h_0 + \cdots + h_r$ is the degree of $S[u]/I(\mathbb{Y})$; see [69, Corollary 4.1.12].

# Chapter 2

# Vanishing Ideals over Rational Parameterizations

Let $K$ be a field and let $\mathbb{X}$ (resp. $\mathbb{X}^*$) be a subset of a projective space $\mathbb{P}^{s-1}$ (resp. affine space $\mathbb{A}^s$), over the field $K$, parameterized by rational functions. Recall that we consider the following sets parameterized by rational functions:

(i) $\mathbb{X}$ is the set of all points $[(f_1(x)/g_1(x),\ldots,f_s(x)/g_s(x))]$ in $\mathbb{P}^{s-1}$ that are well defined, i.e., $x \in K^n$, $f_i(x) \neq 0$ for some $i$, and $g_i(x) \neq 0$ for all $i$. We call $\mathbb{X}$ the *projective set parameterized* by $F$.

(ii) $X$ is the set of all points $[(f_1(x)/g_1(x),\ldots,f_s(x)/g_s(x))]$ in $\mathbb{P}^{s-1}$ such that $x \in K^n$ and $f_i(x)g_i(x) \neq 0$ for all $i$. We call $X$ the *projective algebraic set parameterized* by $F$.

(iii) $\mathbb{X}^*$ is the set of all points $(f_1(x)/g_1(x),\ldots,f_s(x)/g_s(x))$ in $\mathbb{A}^s$ such that $x \in K^n$ and $g_i(x) \neq 0$ for all $i$. We call $\mathbb{X}^*$ *the affine set parameterized* by $F$.

(iv) $X^*$ is the set of all points $(f_1(x)/g_1(x),\ldots,f_s(x)/g_s(x))$ in $\mathbb{A}^s$ such that $x \in K^n$ and $f_i(x)g_i(x) \neq 0$ for all $i$. We call $X^*$ the *affine algebraic set parameterized* by $F$.

(v) $\overline{\phi(\mathbb{X}^*)}$ (resp. $\overline{\phi(X^*)}$), is the *projective closure* of $\mathbb{X}^*$ (resp. $X^*$), where $\phi\colon \mathbb{A}^s \to \mathbb{P}^s$ is the map given by $\alpha \mapsto [(\alpha,1)]$.

Let $I(\mathbb{X})$ (resp. $I(\mathbb{X}^*)$) be the vanishing ideal of $\mathbb{X}$ (resp. $\mathbb{X}^*$). Some of the main contributions of this thesis are in determining formulas for $I(\mathbb{X})$ (resp. $I(\mathbb{X}^*)$) to compute their algebraic invariants using elimination theory and Gröbner bases. The formulas for vanishing ideals over finite fields that we give in this work were discovered by making experiments with *Macaulay*2; we are especially interested in this case because of its relation to algebraic coding theory. We also consider sets $X$ and $X^*$ in $\mathbb{P}^{s-1}$ and $\mathbb{A}^s$, respectively, parameterized by rational functions which are subject to some restrictions. Then we use our results to study: the degree and structure of vanishing ideals, the projective closure of

$\mathbb{X}^*$, and the basic parameters of affine and projective Reed-Muller-type codes. We recover some results for vanishing ideals over monomial parameterizations.

## 2.1 Presentation ideals of subrings generated by rational functions

In this section we give a formula for the presentation ideal of a subring generated by rational functions which is related to the rational implicitization problem [9].

Let $R = K[\mathbf{y}] = K[y_1, \ldots, y_n]$ be a polynomial ring over a field $K$, let $K(\mathbf{y})$ be the field of fractions of $K[\mathbf{y}]$ and let $F = \{f_1/g_1, \ldots, f_s/g_s\}$ be a set of rational functions. If $K[F]$ is the subring of $K(\mathbf{y})$ generated by $F$ over $K$, then there is an epimorphism of $K$-algebras:

$$\varphi\colon\ S = K[t_1, \ldots, t_s] \longrightarrow K[F] \longrightarrow 0, \text{ induced by } \varphi(t_i) = f_i/g_i,$$

where $S$ is a polynomial ring over the field $K$ with the standard grading $S = \oplus_{d=0}^{\infty} S_d$.

The kernel $P_F$ of $\varphi$ is called the *presentation ideal* of $K[F]$ with respect to $F$. An interesting case arises when $F$ consists of *Laurent monomials*, i.e., $f_i/g_i = y^{v_i}$ with $v_i \in \mathbb{Z}^n$ for all $i$. In this case $P_F$ is called the *toric ideal* of $K[F]$ with respect to $F$ and $K[F]$ is called the *monomial subring* spanned by $F$ [61, 69].

**Lemma 2.1.1.** *Let $f_1/g_1, \ldots, f_s/g_s$ be rational functions of $K(\mathbf{y})$ and let $f = f(t_1, \ldots, t_s)$ be a polynomial in $S$ of degree $d$. Then*

$$g_1^{d+1} \cdots g_s^{d+1} f = \sum_{i=1}^{s} g_1 \cdots g_s h_i (g_i t_i - f_i) + g_1^{d+1} \cdots g_s^{d+1} f(f_1/g_1, \ldots, f_s/g_s)$$

*for some $h_1, \ldots, h_s$ in the polynomial ring $K[y_1, \ldots, y_n, t_1, \ldots, t_s]$. If $f$ is homogeneous and $z$ is a new variable, then*

$$g_1^{d+1} \cdots g_s^{d+1} f = \sum_{i=1}^{s} g_1 \cdots g_s h_i (g_i t_i - f_i z) + g_1^{d+1} \cdots g_s^{d+1} z^d f(f_1/g_1, \ldots, f_s/g_s)$$

*for some $h_1, \ldots, h_s$ in the polynomial ring $K[y_1, \ldots, y_n, z, t_1, \ldots, t_s]$.*

**Proof.** We can write $f = \lambda_1 t^{m_1} + \cdots + \lambda_r t^{m_r}$ with $\lambda_i \in K^*$ and $m_i \in \mathbb{N}^s$ for all $i$. Write $m_i = (m_{i1}, \ldots, m_{is})$ for $1 \leq i \leq r$ and set $I = (\{g_i t_i - f_i\}_{i=1}^{s})$. By the binomial theorem, for all $i, j$, we can write

$$t_j^{m_{ij}} = [(t_j - (f_j/g_j)) + (f_j/g_j)]^{m_{ij}} = (h_{ij}/g_j^{m_{ij}}) + (f_j/g_j)^{m_{ij}},$$

for some $h_{ij} \in I$. Hence for any $i \in \{1, \ldots, r\}$ we can write

$$t^{m_i} = t_1^{m_{i1}} \cdots t_s^{m_{is}} = (G_i/g_1^{m_{i1}} \cdots g_s^{m_{is}}) + (f_1/g_1)^{m_{i1}} \cdots (f_s/g_s)^{m_{is}},$$

where $G_i \in I$. Notice that $m_{i_1} + \cdots + m_{is} \leq d$ for all $i$ because $f$ has degree $d$. Then substituting these expressions for $t^{m_1}, \ldots, t^{m_s}$ in $f = \lambda_1 t^{m_1} + \cdots + \lambda_r t^{m_r}$ and multiplying $f$ by $g_1^{d+1} \cdots g_s^{d+1}$, we obtain the required expression.

If $f$ is homogeneous of degree $d$, the required expression for $g_1^{d+1} \cdots g_s^{d+1} f$ follows from the first part by considering the rational functions $f_1 z/g_1, \ldots, f_s z/g_s$, i.e., by replacing $f_i$ by $f_i z$, and observing that $f(f_1 z, \ldots, f_s z) = z^d f(f_1, \ldots, f_s)$. □

The next result is related to rational implicitization in the sense of [9, Theorem 2, p. 131].

**Proposition 2.1.2.** *If $F = \{f_1/g_1, \ldots, f_s/g_s\}$ is a set of rational functions with $f_i, g_i \in R$ and $g_i \neq 0$ for all $i$, then the kernel of the homomorphism of $K$-algebras*

$$\varphi\colon\ S = K[t_1, \ldots, t_s] \longrightarrow K[F],\ \textit{induced by } \varphi(t_i) = f_i/g_i,$$

*is the ideal $(g_1 t_1 - f_1, \ldots, g_s t_s - f_s, y_0 g_1 \cdots g_s - 1) \cap S$, where $y_0$ is an extra variable.*

**Proof.** We set $I = (g_1 t_1 - f_1, \ldots, g_s t_s - f_s, y_0 g_1 \cdots g_s - 1)$ and $h_i = f_i/g_i$ for $i = 1, \ldots, s$. We first show the inclusion $\ker(\varphi) \subset I \cap S$. Let $f$ be a polynomial in $\ker(\varphi)$ of degree $d$. Then, by Lemma 2.1.1, one can write

$$g_1^d \cdots g_s^d f = \sum_{i=1}^{s} a_i(g_i t_i - f_i) + g_1^d \cdots g_s^d f(f_1/g_1, \ldots, f_s/g_s) = \sum_{i=1}^{s} a_i(g_i t_i - f_i) \qquad (2.1.1)$$

for some $a_1, \ldots, a_s$ in $B = K[y_1, \ldots, y_n, t_1, \ldots, t_s]$. Making $W = y_0 g_1 \cdots g_s - 1$, we get the equality $g_1 \cdots g_s = (W+1)/y_0$. Thus, from Eq. (2.1.1), we obtain that $(W+1)^d f \in I$. Hence $f \in I \cap S$. Conversely let $f \in I \cap S$. Then we can write

$$f = f(t_1, \ldots, t_s) = a_1(g_1 t_1 - f_1) + \cdots + a_s(g_s t_s - f_s) + b(g_1 \cdots g_s y_0 - 1).$$

for some $a_1, \ldots, a_s, b$ in $B[y_0]$. Hence $f(h_1, \ldots, h_s) = h(g_1 \cdots g_s y_0 - 1)$ for some $h$ in $B[y_0]$. The left-hand side of this equality does not depend on $y_0$. Thus making $y_0 = 1/g_1 \cdots g_s$, we obtain $f(h_1, \ldots, h_s) = 0$, i.e., $f \in \ker(\varphi)$. □

**Corollary 2.1.3.** [69, Proposition 7.1.9] *If $f_1, \ldots, f_s$ are in $R$, then the kernel of the homomorphism of $K$-algebras*

$$\varphi\colon\ S = K[t_1, \ldots, t_s] \longrightarrow K[f_1, \ldots, f_s],\ \textit{induced by } \varphi(t_i) = f_i,$$

*is the ideal $(t_1 - f_1, \ldots, t_s - f_s) \cap S$.*

**Proof.** By Proposition 2.1.2 it suffices to notice that any element of

$$(t_1 - f_1, \ldots, t_s - f_s, y_0 - 1) \cap S,$$

being independent of $y_0$, belongs to $(t_1 - f_1, \ldots, t_s - f_s) \cap S$. □

**Example 2.1.4.** If $F=\{y_1+4y_2+3y_3, y_1^2-y_2^2, y_1-y_2\}$, then using *Macaulay*2 and the procedure below we get that $P_F=(0)$ if $K=\mathbb{Q}$ and $P_F=(t_1t_3-t_2)$ if $K=\mathbb{F}_3$. Thus the degree of $\mathbb{Q}[F]$ is 1 and the degree of $\mathbb{F}_3[F]$ is 2, i.e., the degree of $K[F]$ depends on the field $K$.

```
R=K[y1,y2,y3,t1,t2,t3,MonomialOrder=>Eliminate 3];
f1=y1+4*y2+3*y3
f2=y1^2-y2^2
f3=y1-y2
I=ideal(t1-f1,t2-f2,t3-f3)
P=ideal selectInSubring(1,gens gb I)
degree P
```

Let $\mathcal{A}=\{\alpha_1,\ldots,\alpha_m\}$ be a set of lattice points of $\mathbb{Z}^n$ and let $\mathcal{P}=\operatorname{conv}(\mathcal{A})$ be the convex hull of $\mathcal{A}$. The set $\mathcal{P}$ is called a *lattice polytope*. We denote the *relative volume* of $\mathcal{P}$ by $\operatorname{vol}(\mathcal{P})$. A reference for relative volumes of lattice polytopes is [18].

**Definition 2.1.5.** If $r=\dim(\mathcal{P})$, the integer $r!\operatorname{vol}(\mathcal{P})$ is called the *normalized volume* of $\mathcal{P}$.

**Definition 2.1.6.** The torsion subgroup of an abelian group $(M,+)$, denoted by $T(M)$, is the set of all $x$ in $M$ such that $\ell x=0$ for some $\ell\in\mathbb{N}_+$.

The next result holds for any toric ideal.

**Theorem 2.1.7.** [51, Theorem 4.5] *Let $P_F$ be the toric ideal of $K[F]=K[y^{v_1},\ldots,y^{v_s}]$, let $A$ be the $n\times s$ matrix with column vectors $v_1,\ldots,v_s$. Then $\deg(S/P_F)=\deg(S[u]/P_F^h)$ and*

$$|T(\mathbb{Z}^n/\mathbb{Z}\{v_1,\ldots,v_s\})|\deg(S/P_F)=r!\operatorname{vol}(\operatorname{conv}(v_1,\ldots,v_s,0)),\ \textit{where } r=\operatorname{rank}(A).$$

**Remark 2.1.8.** The degree of $K[F]$ is independent of $K$ if $F$ is a set of monomials. Theorem 2.1.7 will allows us to compute the degree of vanishing ideals of affine sets parameterized by Laurent monomials over infinite fields without using Gröbner bases (see Theorem 2.2.11).

## 2.2 Rational parameterizations over infinite fields

In this section we study vanishing ideals over sets parameterized by rational functions over infinite fields.

**Theorem 2.2.1.** (Combinatorial Nullstellensatz [1]) *Let $S=K[t_1,\ldots,t_s]$ be a polynomial ring over a field $K$, let $f\in S$, and let $a=(a_i)\in\mathbb{N}^s$. Suppose that the coefficient of $t^a$ in $f$ is non-zero and $\deg(f)=a_1+\cdots+a_s$. If $A_1,\ldots,A_s$ are subsets of $K$, with $|A_i|>a_i$ for all $i$, then there are $x_1\in A_1,\ldots,x_s\in A_s$ such that $f(x_1,\ldots,x_s)\neq 0$.*

**Lemma 2.2.2.** *Let $K$ be a field and let $A_1,\ldots,A_s$ be a collection of non-empty finite subsets of $K$. If $Y := A_1\times\cdots\times A_s \subset \mathbb{A}^s$, $g\in I(Y)$ and $\deg_{t_i}(g) < |A_i|$ for $i=1,\ldots,s$, then $g=0$. In particular if $g$ is a polynomial of $S$ that vanishes at all points of $\mathbb{A}^s$, then $g=0$.*

**Proof.** We proceed by contradiction. Assume that $g$ is not zero. Then, there is a monomial $t^a = t_1^{a_1}\cdots t_s^{a_s}$ of $g$ with $\deg(g) = a_1+\cdots+a_s$ and $a=(a_1,\ldots,a_s)\neq 0$. As $\deg_{t_i}(g) < |A_i|$ for all $i$, then $a_i < |A_i|$ for all $i$. Thus, by Theorem 2.2.1, there are $x_1,\ldots,x_s$ with $x_i\in A_i$ for all $i$ such that $g(x_1,\ldots,x_s)\neq 0$, a contradiction to the assumption that $g$ vanishes on $Y$. □

**Example 2.2.3.** If $K=\mathbb{F}_2$ and $g = t_1t_2+t_1+t_2+1$, then $g$ vanishes on $K^2\setminus\{(0,0)\}$ and $\deg_{t_i}(g) < 1$ for $i=1,2$ but $g\neq 0$.

**Lemma 2.2.4.** *Let $K$ be an infinite field. Then the following hold.*

(a) $\mathbb{X}^*\neq\emptyset$.

(b) *$X\neq\emptyset$ and $X^*\neq\emptyset$ (resp. $\mathbb{X}\neq\emptyset$) if and only if $f_i\neq 0$ for all $i$ (resp. $f_i\neq 0$ for some $i$).*

**Proof.** (a) The affine set $\mathbb{X}^*$ is always non-empty because there are no restrictions on $f_1,\ldots,f_s$ and the non-zero polynomial $g_1\cdots g_s$ does not vanish at all points of $K^n$ by Lemma 2.2.2.

(b) Assume that $f_i\neq 0$ for all $i$. Consider the non-zero polynomial $f_1\cdots f_s g_1\cdots g_s$. As $K$ is infinite this polynomial does not vanish at all points of $K^n$ by Lemma 2.2.2. Thus there is $x\in K^n$ such that $f_i(x)g_i(x)\neq 0$ for all $i$. Then $X\neq\emptyset$ and $X^*\neq\emptyset$. The reverse implication is clear. □

**Theorem 2.2.5.** *Let $B=K[y_0,y_1,\ldots,y_n,z,t_1,\ldots,t_s]$ be a polynomial ring over an infinite field $K$. If $\mathbb{X}$ is a projective set parameterized by rational functions $f_1/g_1,\ldots,f_s/g_s$ in $K(\mathbf{y})$ not all of them zero, then*

$$I(\mathbb{X}) = (\{g_it_i - f_iz\}_{i=1}^s, y_0g_1\cdots g_s - 1)\cap S$$

*and $I(\mathbb{X})$ is the presentation ideal of $K[f_1z/g_1,\ldots,f_sz/g_s]$.*

**Proof.** We denote by $I = (\{g_it_i - f_iz\}_{i=1}^s, y_0g_1\cdots g_s - 1)$. First we show the inclusion $I(\mathbb{X})\subset I\cap S$. Take a homogeneous polynomial $f=f(t_1,\ldots,t_s)$ of degree $d$ that vanishes at all points of $\mathbb{X}$. Setting $W = y_0g_1\cdots g_s - 1$, by Lemma 2.1.1, we can write

$$(W+1)^{d+1}f = \sum_{i=1}^{s} y_0^{d+1}g_1\cdots g_sh_i(g_it_i - f_iz) + z^dy_0^{d+1}g_1^{d+1}\cdots g_s^{d+1}f(f_1/g_1,\ldots,f_s/g_s), \tag{2.2.1}$$

where $h_1,\ldots,h_s$ are in $K[y_1,\ldots,y_n,z,t_1,\ldots,t_s]$. We only need to show that

$$H = g_1^{d+1}\cdots g_s^{d+1} f(f_1/g_1,\ldots,f_s/g_s)$$

is equal to zero. It is not hard to see that $H$ is a polynomial in $K[\mathbf{y}]$. Thus we only need to show that $H$ vanishes at all points of $K^n$. Take a point $x \in K^n$. If $g_i(x) = 0$ for some $i$, then clearly $H(x) = 0$ because $g_1\cdots g_s$ divides $H$. Thus we may assume that $g_i(x) \neq 0$ for all $i$. If $f_i(x) \neq 0$ for some $i$, then by definition of $\mathbb{X}$, we get that $f(f_1(x)/g_1(x),\ldots,f_s(x)/g_s(x)) = 0$ and by Eq. (2.2.1) or directly from the definition of $H$ it is seen that $H(x) = 0$. If $f_i(x) = 0$ for all $i$, as $f$ is homogeneous, it follows that $H(x) = 0$. Thus $H = 0$ and $f \in I \cap S$.

Next we show the inclusion $I(\mathbb{X}) \supset I \cap S$. By Proposition 2.1.2 we get that $I \cap S$ is the presentation ideal of $K[f_1z/g_1,\ldots,f_sz/g_s]$. Therefore, using Proposition 1.4.14, it follows that $I \cap S$ is graded. Let $f$ be a homogeneous polynomial of $I \cap S$. Then we can write

$$f = f(t_1,\ldots,t_s) = h_1(g_1t_1 - f_1z) + \cdots + h_s(g_st_s - f_sz) + h(g_1\cdots g_sy_0 - 1). \qquad (2.2.2)$$

for some $h_1,\ldots,h_s,h$ in $B$. Take a point $[P]$ in $\mathbb{X}$ with $P = (f_1(x)/g_1(x),\ldots,f_s(x)/g_s(x))$, and $x = (x_1,\ldots,x_n) \in K^n$. From Eq. (2.2.2), making $t_i = f_i(x)/g_i(x)$, $y_j = x_j$, $z = 1$ and $y_0 = 1/g_1(x)\cdots g_s(x)$ for all $i,j$, it follows that $f(P) = 0$. Thus $f$ vanishes on $\mathbb{X}$. □

**Example 2.2.6.** If $\mathbb{X}$ is the projective set parameterized by $F = \{y_2/y_1, y_3/y_2, y_1/y_3, 1\}$ over the field $\mathbb{Q}$ of rational numbers. Using *Macaulay*2 [30] and Theorem 2.2.5 we get

$$I(\mathbb{X}) = (y_1t_1 - y_2z,\ y_2t_2 - y_3z,\ y_3t_3 - y_1z, t_4 - z, y_0y_1y_2y_3 - 1) \cap S = (t_1t_2t_3 - t_4^3).$$

Notice that $(y_1t_1 - y_2z,\ y_2t_2 - y_3z,\ y_3t_3 - y_1z, t_4 - z) \cap S = (0)$. This means that the variable $y_0$ is essential to compute $I(\mathbb{X})$.

**Definition 2.2.7.** Let $S = K[t_1,\ldots,t_s]$ be a polynomial ring over a field $K$. A *binomial* of $S$ is an element of the form $f = t^a - t^b$, for some $a, b$ in $\mathbb{N}^s$. An ideal generated by binomials is called a *binomial ideal*.

The next lemma is well known, see for instance [69, Corollary 7.1.5] and its proof.

**Corollary 2.2.8.** *Let $K$ be an infinite field and let $I \subset S$ be a graded ideal. Then $I$ is the vanishing ideal of a projective set in $\mathbb{P}^{s-1}$ parameterized by Laurent monomials if and only if $I$ is a prime ideal generated by binomials.*

**Proof.** $\Rightarrow$) By Theorem 2.2.5 and Lemma 1.3.24 we get that $I$ is a prime ideal generated by binomials.

$\Leftarrow$) By [48, Theorem 7.4] it follows that $I$ is a toric ideal, that is, there are $y^{v_1},\ldots,y^{v_s}$ in $K(\mathbf{y})$ and an epimorphism of $K$-algebras

$$\varphi\colon\ S = K[t_1,\ldots,t_s] \longrightarrow K[y^{v_1},\ldots,y^{v_s}],\ \text{induced by } \varphi(t_i) = y^{v_i},$$

such that $I=\ker(\varphi)$. Consider the epimorphism of $K$-algebras

$$\varphi_1\colon\ S=K[t_1,\ldots,t_s]\longrightarrow K[y^{v_1}z,\ldots,y^{v_s}z],\ \text{induced by } \varphi(t_i)=y^{v_i}z.$$

As $I$ and $\ker(\varphi_1)$ are graded binomial ideals in the standard grading of $S$ it is not hard to see that $I=\ker(\varphi_1)$. If $\mathbb{X}$ is the projective set parameterized by $y^{v_1},\ldots,y^{v_s}$, using Theorem 2.2.5 we get that $I(\mathbb{X})=\ker(\varphi_1)$. Thus $I=I(\mathbb{X})$ as required. □

**Example 2.2.9.** Let $K$ be an infinite field. If $\mathbb{Y}=\{[(1,0)],[(0,1)],[(1,1)]\}\subset\mathbb{P}^1$, then its vanishing ideal is generated by $t_1t_2(t_1-t_2)$. Notice that $\mathbb{Y}$ cannot be parameterized by Laurent monomials because $I(\mathbb{Y})$ is not a prime ideal (see Corollary 2.2.8).

**Theorem 2.2.10.** *Let $B=K[y_0,y_1,\ldots,y_n,z,t_1,\ldots,t_s]$ be a polynomial ring over an infinite field $K$. If $X$ is a projective algebraic set parameterized by rational functions $f_1/g_1,\ldots,f_s/g_s$ in $K(\mathbf{y})$ with $f_i\neq 0$ for all $i$, then*

$$I(X)=(\{g_it_i-f_iz\}_{i=1}^s,y_0g_1\cdots g_s-1)\cap S$$

*and $I(X)$ is the presentation ideal of $K[f_1z/g_1,\ldots,f_sz/g_s]$.*

**Proof.** We set $I=(\{f_ig_it_i-f_i^2z\}_{i=1}^s,y_0f_1\cdots f_sg_1\cdots g_s-1)$. As $f_i\neq 0$ for all $i$, by Proposition 2.1.2, one has the equality

$$(\{g_it_i-f_iz\}_{i=1}^s,y_0g_1\cdots g_s-1)\cap S=(\{f_ig_it_i-f_i^2z\}_{i=1}^s,y_0f_1\cdots f_sg_1\cdots g_s-1)\cap S$$

and $(\{g_it_i-f_iz\}_{i=1}^s,y_0g_1\cdots g_s-1)\cap S$ is the presentation ideal of $K[f_1z/g_1,\ldots,f_sz/g_s]$. Using Proposition 1.4.14, it follows that $I\cap S$ is graded.

First we are going to show the inclusion $I(X)\subset I\cap S$. Take a homogeneous polynomial $f=f(t_1,\ldots,t_s)$ of degree $d$ that vanishes at all points of $X$. Now setting $W=y_0f_1\cdots f_sg_1\cdots g_s-1$, by Lemma 2.1.1, we can write

$$(W+1)^{d+1}f=\sum_{i=1}^{s}y_0^{d+1}f_1\cdots f_sg_1\cdots g_sh_i(f_ig_it_i-f_i^2z)+z^d(W+1)^{d+1}f(f_1/g_1,\ldots,f_s/g_s),\tag{2.2.3}$$

where $h_1,\ldots,h_s$ are in $B$. We only need to show that

$$H=(f_1\cdots f_sg_1\cdots g_s)^{d+1}f(f_1/g_1,\ldots,f_s/g_s)$$

is equal to zero. It is not hard to see that $H$ is a polynomial in $K[\mathbf{y}]$. Thus we only need to show that $H$ vanishes at all points of $K^n$. Take a point $x\in K^n$. If $g_i(x)=0$ for some $i$ or $f_i(x)=0$ for some $i$, then clearly $H(x)=0$ because $f_1\cdots f_sg_1\cdots g_s$ divides $H$. Thus we may assume that $f_i(x)g_i(x)\neq 0$ for all $i$ and, by definition of $X$, we get that $f(f_1(x)/g_1(x),\ldots,f_s(x)/g_s(x))=0$. Hence by Eq. (2.2.3) or directly from the definition of $H$ it is seen that $H(x)=0$.

Next we show the inclusion $I(X)\supset I\cap S$. We proceed as in the second part of the proof of Theorem 2.2.5. Let $f$ be a homogeneous polynomial of $I\cap S$. Take a point $[P]$

in $X$ with $P = (f_1(x)/g_1(x), \ldots, f_s(x)/g_s(x))$ and $f_i(x)g_i(x) \neq 0$ for all $i$. Then $f$ is a linear combination of $\{f_ig_it_i - f_i^2z\}_{i=1}^s \cup \{y_0f_1 \cdots f_sg_1 \cdots g_s - 1\}$ with coefficients in $B$. Making $t_i = f_i(x)/g_i(x)$, $z = 1$, $y_j = x_j$, and $y_0 = 1/f_1(x) \cdots f_s(x)g_1(x) \cdots g_s(x)$ for all $i, j$, it follows that $f(P) = 0$. Thus $f$ vanishes on $X$. □

**Theorem 2.2.11.** *Let $B = K[y_0, y_1, \ldots, y_n, t_1, \ldots, t_s]$ be a polynomial ring over an infinite field $K$. If $\mathbb{X}^*$ is the affine set parameterized by rational functions $f_1/g_1, \ldots, f_s/g_s$ in $K(\mathbf{y})$, then*

$$I(\mathbb{X}^*) = (\{g_it_i - f_i\}_{i=1}^s, y_0g_1 \cdots g_s - 1) \cap S$$

*and $I(\mathbb{X}^*)$ is the presentation ideal of $K[f_1/g_1, \ldots, f_s/g_s]$.*

**Proof.** We set $I = (\{g_it_i - f_i\}_{i=1}^s, y_0g_1 \cdots g_s - 1)$. First we show the inclusion $I(\mathbb{X}^*) \subset I \cap S$. Take a polynomial $f = f(t_1, \ldots, t_s)$ of degree $d$ that vanishes at all points of $\mathbb{X}^*$. Setting $W = y_0g_1 \cdots g_s - 1$, by Lemma 2.1.1, we can write

$$(W+1)^{d+1}f = \sum_{i=1}^{s} y_0^{d+1}g_1 \cdots g_sh_i(g_it_i - f_i) + y_0^{d+1}g_1^{d+1} \cdots g_s^{d+1}f(f_1/g_1, \ldots, f_s/g_s), \quad (2.2.4)$$

where $h_1, \ldots, h_s$ are in $B$. We only need to show that $H = g_1^{d+1} \cdots g_s^{d+1}f(f_1/g_1, \ldots, f_s/g_s)$ is equal to zero. It is not hard to see that $H$ is a polynomial in $K[\mathbf{y}]$. Thus we need only show that $H$ vanishes at all points of $K^n$. Take a point $x \in K^n$. If $g_i(x) = 0$ for some $i$, then clearly $H(x) = 0$ because $g_1 \cdots g_s$ divides $H$. Thus we may assume that $g_i(x) \neq 0$ for all $i$. Then, by definition of $\mathbb{X}^*$, we get that $f(f_1(x)/g_1(x), \ldots, f_s(x)/g_s(x)) = 0$ and by Eq. (2.2.4) or directly from the definition of $H$ it is seen that $H(x) = 0$.

Next we show the inclusion $I(\mathbb{X}^*) \supset I \cap S$. Take $f$ in $I \cap S$. Let $P$ be any point in $\mathbb{X}^*$ with $P = (f_1(x)/g_1(x), \ldots, f_s(x)/g_s(x))$. Then $f$ is a linear combination of

$$\{g_it_i - f_i\}_{i=1}^s \cup \{y_0g_1 \cdots g_s - 1\}$$

with coefficients in $B$. Making $t_i = f_i(x)/g_i(x)$, $y_j = x_j$, and $y_0 = 1/g_1(x) \cdots g_s(x)$ for all $i, j$, it follows that $f(P) = 0$. Thus $f$ vanishes on $\mathbb{X}^*$. By Proposition 2.1.2 we get that $I \cap S$ is the presentation ideal of $K[f_1/g_1, \ldots, f_s/g_s]$. □

**Corollary 2.2.12.** *If $K$ is infinite, $f_i \neq 0$ for all $i$ and $\mathbb{Y} = \phi(X^*)$, then $I(\mathbb{Y})$ is equal to the presentation ideal of $K[f_1z/g_1, \ldots, f_sz/g_s, z]$.*

**Proof.** Notice that $\mathbb{Y}$ is the projective algebraic set parameterized by $f_1/g_1, \ldots, f_s/g_s, 1$. Hence the result follows from Theorem 2.2.10. □

**Theorem 2.2.13.** *Let $B = K[y_0, y_1, \ldots, y_n, t_1, \ldots, t_s]$ be a polynomial ring over an infinite field $K$. If $X^*$ is the affine algebraic set parameterized by rational functions $f_1/g_1, \ldots, f_s/g_s$ in $K(\mathbf{y})$ and $f_i \neq 0$ for all $i$, then*

$$I(X^*) = (\{g_it_i - f_i\}_{i=1}^s, y_0g_1 \cdots g_s - 1) \cap S$$

*and $I(X^*)$ is the presentation ideal of $K[f_1/g_1, \ldots, f_s/g_s]$.*

**Proof.** We set $I = (\{f_ig_it_i - f_i^2\}_{i=1}^s, y_0f_1\cdots f_sg_1\cdots g_s - 1)$. Because $f_i \neq 0$ for all $i$, by Proposition 2.1.2, one has

$$(\{g_it_i - f_i\}_{i=1}^s, y_0g_1\cdots g_s - 1) \cap S = (\{f_ig_it_i - f_i^2\}_{i=1}^s, y_0f_1\cdots f_sg_1\cdots g_s - 1) \cap S$$

and $(\{g_it_i - f_i\}_{i=1}^s, y_0g_1\cdots g_s - 1) \cap S$ is the presentation ideal of $K[f_1/g_1, \ldots, f_s/g_s]$.

First we show the inclusion $I(X^*) \subset I \cap S$. Take a polynomial $f = f(t_1, \ldots, t_s)$ of degree $d$ that vanishes at all points of $X^*$. Setting $W = y_0f_1\cdots f_sg_1\cdots g_s - 1$, by Lemma 2.1.1, we can write

$$(W+1)^{d+1}f = \sum_{i=1}^{s} y_0^{d+1}f_1\cdots f_sg_1\cdots g_sh_i(f_ig_it_i - f_i^2) + (W+1)^{d+1}f(f_1/g_1, \ldots, f_s/g_s), \tag{2.2.5}$$

where $h_1, \ldots, h_s$ are in $B$. We only need to show that

$$H = (f_1\cdots f_sg_1\cdots g_s)^{d+1}f(f_1/g_1, \ldots, f_s/g_s)$$

is equal to zero. It is not hard to see that $H$ is a polynomial in $K[\mathbf{y}]$. Thus we only need to show that $H$ vanishes at all points of $K^n$. Take a point $x \in K^n$. If $g_i(x) = 0$ for some $i$ or $f_i(x) = 0$ for some $i$, then clearly $H(x) = 0$ because $f_1\cdots f_sg_1\cdots g_s$ divides $H$. Thus we may assume that $f_i(x)g_i(x) \neq 0$ for all $i$ and, by definition of $X$, we get that $f(f_1(x)/g_1(x), \ldots, f_s(x)/g_s(x)) = 0$. Hence by Eq. (2.2.5) or directly from the definition of $H$ it is seen that $H(x) = 0$.

Next we show the inclusion $I(X^*) \supset I \cap S$. Let $f$ be a polynomial of $I \cap S$. Take a point $P$ in $X^*$ with $P = (f_1(x)/g_1(x), \ldots, f_s(x)/g_s(x))$ and $f_i(x)g_i(x) \neq 0$ for all $i$. Then $f$ is a linear combination of $\{f_ig_it_i - f_i^2\}_{i=1}^s \cup \{y_0f_1\cdots f_sg_1\cdots g_s - 1\}$ with coefficients in $B$. Making $t_i = f_i(x)/g_i(x)$, $y_j = x_j$, and $y_0 = 1/f_1(x)\cdots f_s(x)g_1(x)\cdots g_s(x)$ for all $i, j$, it follows that $f(P) = 0$. Thus $f$ vanishes on $X^*$. □

**The Zariski closure of an affine set.** Here we examine the Zariski closure of an affine set $\mathbb{X}^*$ parameterized by Laurent monomials.

**Theorem 2.2.14.** [39, 40] *Let $F = \{y^{v_1}, \ldots, y^{v_s}\}$ be a set of Laurent monomials such that $K$ is algebraically closed or $K[F]$ is normal. Then there exists an affine set $\mathbb{X}_H^*$ parameterized by $H = \{y^{u_1}, \ldots, y^{u_s}\}$ with $u_i \in \mathbb{Z}^n$ such that $V(P_F) = \mathbb{X}_H^*$ and $P_F = P_H$, where $P_F$ and $P_H$ are the toric ideals of $K[F]$ and $K[H]$, respectively.*

**Corollary 2.2.15.** *If $F = \{y^{v_1}, \ldots, y^{v_s}\}$ is a set of monomials with $v_1, \ldots, v_s$ in $\mathbb{Z}^n$ and $K$ is an algebraically closed field, then there exists a set of monomials $H = \{y^{u_1}, \ldots, y^{u_s}\}$ with $u_1, \ldots, u_s$ in $\mathbb{Z}^n$ such that $\overline{\mathbb{X}^*}$ is the affine set $\mathbb{X}_H^*$ parameterized by $H$.*

**Proof.** Let $P_F$ be the presentation ideal of $K[F]$. By Theorem 2.2.14 the affine variety $V(P_F)$ is parameterized by a set $H = \{y^{u_1}, \ldots, y^{u_s}\}$ of monomials with $u_1, \ldots, u_s$ in

$\mathbb{Z}^n$, and by Theorem 2.2.11 the vanishing ideal of $\mathbb{X}^*$ is equal to $P_F$. Therefore, by Lemma 1.4.15, we get

$$\mathbb{X}_H^* = V(P_F) = V(I(\mathbb{X}^*)) = \overline{\mathbb{X}^*},$$

as required. □

**Lemma 2.2.16.** *Let $K$ be a field. If $Y$ is a subset of $\mathbb{A}^s$ or a subset of $\mathbb{P}^s$ and we have that $Z = V(I(Y))$, then $I(Z) = I(Y)$. In particular $I(Y) = I(\overline{Y})$.*

**Proof.** Since $Y \subset Z$, we get $I(Z) \subset I(Y)$. As $I(Z) = I(V(I(Y))) \supset I(Y)$, one has equality. By Lemma 1.4.15 one has $\overline{Y} = V(I(Y))$. Thus $I(Y) = I(\overline{Y})$. □

**Corollary 2.2.17.** *Let $F = \{y^{v_1}, \ldots, y^{v_s}\}$, $H = \{y^{u_1}, \ldots, y^{u_s}\}$ be sets of Laurent monomials and let $\mathbb{X}_H^*$ be the affine set parameterized by $H$. If $K$ is infinite and $V(P_F) = \mathbb{X}_H^*$, then $P_F = P_H$.*

**Proof.** Let $\mathbb{X}_F^*$ be the affine set parameterized by $F$. By Theorem 2.2.11 we have that $P_F = I(\mathbb{X}_F^*)$ and $P_H = I(\mathbb{X}_H^*)$. Thus, by Lemma 1.4.15, one has

$$\mathbb{X}_H^* = V(P_F) = V(I(\mathbb{X}_F^*)) = \overline{\mathbb{X}_F^*}.$$

Then, by Lemma 2.2.16, we get $I(\mathbb{X}_H^*) = I(\overline{\mathbb{X}_F^*}) = I(\mathbb{X}_F^*)$. Hence $P_H = P_F$. □

**Definition 2.2.18.** If $F = \{y_1^{-1}, \ldots, y_n^{-1}\}$, the projective algebraic set parameterized by $F$, denoted by $T$, is called a *projective torus* in $\mathbb{P}^{n-1}$, and the affine algebraic set parameterized by $F$, denoted by $T^*$, is called an *affine torus* in $\mathbb{A}^n$.

**Remark 2.2.19.** If $T^*$ is an affine torus in $\mathbb{A}^n$ and $K$ is infinite, then $\overline{T^*} = \mathbb{A}^n$ because $T^*$ is equal to the open set $\mathbb{A}^n \setminus V(y_1 \cdots y_n)$. Thus $T^*$ has to be dense in $\mathbb{A}^n$ because $K$ is an infinite field (see for instance [70, Exercise 3.2.20]).

**Example 2.2.20.** If $F = \{y_1, y_1^{-1}, \ldots, y_n, y_n^{-1}\}$ and $K$ is an infinite field, then we have $I(\mathbb{X}^*) = P_F$, $P_F = (t_1t_2 - 1, \ldots, t_{2n-1}t_{2n} - 1)$ and $V(I(\mathbb{X}^*)) = \mathbb{X}^* = X^*$.

**The degree of the projective closure.** In this part we study the projective closure of an affine set $\mathbb{X}^*$ parameterized by rational functions.

For use below recall that $\phi$ is the map $\phi\colon \mathbb{A}^s \to \mathbb{P}^s$, $\alpha \mapsto [(\alpha, 1)]$.

**Corollary 2.2.21.** *If $K$ is an infinite field and $\mathbb{Y} = \phi(\mathbb{X}^*)$, then $I(\mathbb{Y}) = I(\overline{\mathbb{Y}}) = I(\mathbb{X}^*)^h$,*

$$\deg\, S[u]/I(\overline{\mathbb{Y}}) = \deg\, S[u]/I(\mathbb{Y}) = \deg\, S/I(\mathbb{X}^*) = \deg\, S[u]/I(\mathbb{X}^*)^h,$$

*and $I(\mathbb{Y})$ is equal to the presentation ideal of $K[f_1z/g_1, \ldots, f_sz/g_s, z]$.*

**Proof.** By Lemma 1.4.15 and Proposition 1.4.23 one has that $V(I(\mathbb{Y})) = \overline{\mathbb{Y}}$ and that $I(\overline{\mathbb{Y}}) = I(\mathbb{X}^*)^h$, and by Lemma 2.2.16 one has the equality $I(\mathbb{Y}) = I(\overline{\mathbb{Y}})$. Hence, by Proposition 1.4.21, we get

$$\deg\, S/I(\mathbb{X}^*) = \deg\, S[u]/I(\mathbb{X}^*)^h = \deg\, S[u]/I(\overline{\mathbb{Y}}) = \deg\, S[u]/I(\mathbb{Y}).$$

The set $\mathbb{Y}$ is the projective set parameterized by $f_1/g_1, \ldots, f_s/g_s, 1$. As a consequence, by Theorem 2.2.5, $I(\mathbb{Y})$ is the presentation ideal of $K[f_1z/g_1, \ldots, f_sz/g_s, z]$. □

**Remark 2.2.22.** This result, together with Theorems 2.1.7 and 2.2.11, can be used to compute the degree—without using Göbner bases—of the projective closure of any affine set $\mathbb{X}^*$ parameterized by Laurent monomials, i.e., we can compute the degree of $S/I(\overline{\phi(\mathbb{X}^*)})$.

As an application we recover the following known description of the projective closure of a monomial curve (see [69, Proposition 10.1.17]) and compute its degree.

**Corollary 2.2.23.** *Let $\mathbb{X}^* = \{(x_1^{d_1}, \ldots, x_1^{d_s}) |\, x_1 \in K\}$ be a monomial curve in the affine space $\mathbb{A}^s$. If $d_1 > d_2 > \cdots > d_s$ and $K = \mathbb{C}$, then the projective closure $\overline{\phi(\mathbb{X}^*)}$ of $\mathbb{X}^*$ is a projective toric variety in $\mathbb{P}^s$ of degree $d_s/\gcd(d_1, \ldots, d_s)$ and dimension $1$ given by*

$$\overline{\phi(\mathbb{X}^*)} = \left\{[(x_1^{d_1}, x_1^{d_2}u_1^{d_1-d_2}, \ldots, x_1^{d_s}u_1^{d_1-d_s}, u_1^{d_1})] \in \mathbb{P}^s \middle|\, u_1, x_1 \in K\right\},$$

*and its vanishing ideal is $I(\overline{\phi(\mathbb{X}^*)}) = I(\mathbb{X}^*)^h = (\{t_i - y_1^{d_i}z\}_{i=1}^{s+1}) \cap K[t_1, \ldots, t_{s+1}]$, where $d_{s+1} = 0$.*

**Proof.** Setting $\mathbb{Y} = \phi(\mathbb{X}^*)$ and $F = \{y_1^{d_1}z, \ldots, y_1^{d_s}z, z\}$, by Corollary 2.2.21, $I(\mathbb{Y})$ is the toric ideal $P_F$ of $K[F]$. Consider the $2 \times (s+1)$ matrix $A$ with rows $\alpha_1 = (d_1, \ldots, d_s, 0)$ and $\alpha_2 = (1, \ldots, 1)$. The matrix $A$ is row equivalent over $\mathbb{Q}$ to the $2 \times (s+1)$ matrix with rows $\beta_1 = (d_1, d_2, \ldots, d_s, 0)$ and $\beta_2 = (0, d_1 - d_2, \ldots, d_1 - d_s, d_1)$. Hence, setting $H = \{y_1^{d_1}, y_1^{d_2}u^{d_1-d_2}, \ldots, y_1^{d_s}u^{d_1-d_s}, u^{d_1}\}$, it follows that the toric ideal $P_H$ of $K[H]$ is the toric ideal $P_F$ of $K[F]$. . By Theorem 2.2.5, we get $P_H = I(\mathbb{X}_H)$, where $\mathbb{X}_H$ is the projective set parameterized by $H$. All together one has:

$$I(\mathbb{X}_H) = P_H = P_F = I(\mathbb{Y}).$$

Notice that $V(I(\mathbb{X}_H)) = \mathbb{X}_H$. This equality follows by observing that $t_i^{d_1} - t_1^{d_i}t_{s+1}^{d_1-d_i}$ is in $P_H$ for $i = 1, \ldots, s+1$, where $d_{s+1} = 0$. Applying Lemma 1.4.15 we obtain

$$\overline{\mathbb{Y}} = V(I(\mathbb{Y})) = V(I(\mathbb{X}_H)) = \mathbb{X}_H.$$

Thus $\overline{\mathbb{Y}}$ is the projective set parameterized by $H$, as required. Next we compute the degree of $S[u]/I(\overline{\mathbb{Y}})$. By Corollary 2.2.21 one has

$$\deg\, S[u]/I(\overline{\mathbb{Y}}) = \deg\, S/I(\mathbb{X}^*).$$

On the other hand by Theorems 2.1.7 and 2.2.11 we get

$$|T(\mathbb{Z}/\mathbb{Z}\{d_1,\ldots,d_s\})|\deg(S/I(\mathbb{X}^*)) = \mathrm{vol}(\mathrm{conv}(d_1,\ldots,d_s,0)).$$

Since $|T(\mathbb{Z}/\mathbb{Z}\{d_1,\ldots,d_s\})| = \gcd(d_1,\ldots,d_s)$ and $\mathrm{vol}(\mathrm{conv}(d_1,\ldots,d_s,0)) = d_s$, we get that the degree of $S[u]/I(\overline{\mathbb{Y}})$ is $d_s/\gcd(d_1,\ldots,d_s)$. Finally notice that by Corollary 2.2.21 one has that $I(\mathbb{X}^*)^h$ is the toric ideal of $K[y_1^{d_1}z,\ldots,y_1^{d_s}z,z]$. Thus the formula for $I(\mathbb{X}^*)^h$ follows at once from Corollary 2.1.3. □

**Example 2.2.24.** Let $\mathbb{X}^* = \{(x_1^3,x_1^2,x_1)|\, x_1 \in K\} \subset \mathbb{A}^3$ be a monomial curve and let $\overline{\phi(\mathbb{X}^*)}$ be its projective closure. If $K = \mathbb{Q}$ and $\mathbb{Y} = \phi(\mathbb{X}^*)$, then using *Macaulay*2 [30], with the procedure below, and Corollary 2.2.23, we get

$$\overline{\mathbb{Y}} = \{[(x_1^3, x_1^2u_1, x_1u_1^2, u_1^3)] \in \mathbb{P}^3|\, u_1, x_1 \in \mathbb{Q}\},$$

$\deg S[u]/I(\overline{\mathbb{Y}}) = 3$, and

$$I(\overline{\mathbb{Y}}) = I(\mathbb{Y}) = (t_3^2 - t_2u, t_2t_3 - t_1u, t_2^2 - t_1t_3) = I(\mathbb{X}^*)^h, \quad \text{where} \quad u = t_4.$$

```
R=QQ[y1,z,t1,t2,t3,t4,MonomialOrder=>Eliminate 2]
I=ideal(t1-y1^3*z,t2-y1^2*z,t3-y1*z,t4-z)
Ixxac= ideal selectInSubring(1,gens gb I)
```

**Polynomial parameterizations over infinite fields.** In this part we specialize our results to polynomial parameterizations over infinite fields.

Let $R = K[y_1,\ldots,y_n]$ be a polynomial ring over a field $K$ and let $F = \{f_1,\ldots,f_s\}$ be a finite set of polynomials of $R$. Consider the following polynomial parameterizations:

(i) $\mathbb{X} := \{[(f_1(x),\ldots,f_s(x))]\,|\, x \in K^n$ and $f_i(x) \neq 0$ for some $i\} \subset \mathbb{P}^{s-1}$, the *projective set parameterized* by $F$,

(ii) $X := \{[(f_1(x),\ldots,f_s(x))]\,|\, x \in K^n$ and $f_i(x) \neq 0$ for all $i\} \subset \mathbb{P}^{s-1}$, the *projective algebraic set parameterized* by $F$,

(iii) $\mathbb{X}^* := \{(f_1(x),\ldots,f_s(x))\,|\, x \in K^n\} \subset \mathbb{A}^s$, *the affine set parameterized* by $F$,

(iv) $X^* := \{(f_1(x),\ldots,f_s(x))\,|\, x \in K^n$ and $f_i(x) \neq 0$ for all $i\} \subset \mathbb{A}^s$, the *affine algebraic set parameterized* by $F$, and

(v) $\overline{\mathbb{X}^*}$ (resp. $\overline{X^*}$), the *projective closure* of $\mathbb{X}^*$ (resp. $X^*$).

**Theorem 2.2.25.** *Let $K$ be an infinite field, let $F = \{f_1,\ldots,f_s\}$ be a set of polynomials of $R$ and let $\mathbb{X}$, $X$, $\mathbb{X}^*$ and $X^*$ be the corresponding sets parameterized by $F$. Then the following holds.*

(i) *If $\mathbb{X} \neq \emptyset$, then $I(\mathbb{X}) = (\{t_i - f_iz\}_{i=1}^s) \cap S$.*

(ii) *If $X \neq \emptyset$, then $I(X) = (\{t_i - f_i z\}_{i=1}^{s}) \cap S$.*

(iii) [69, Corollary 7.1.12] $I(\mathbb{X}^*) = (\{t_i - f_i\}_{i=1}^{s}) \cap S$.

(iv) If $X^* \neq \emptyset$, then $I(X^*) = (\{t_i - f_i\}_{i=1}^{s}) \cap S$.

**Proof.** (i): By Theorem 2.2.5, making $g_i = 1$ for all $i$, we get

$$I(\mathbb{X}) = (\{t_i - f_i z\}_{i=1}^{s}, y_0 - 1) \cap S$$

and $I(\mathbb{X})$ is the presentation ideal of $K[f_1 z, \ldots, f_s z]$. Since $t_i - f_i z$ is independent of $y_0$ it follows readily that $(\{t_i - f_i z\}_{i=1}^{s}, y_0 - 1) \cap S$ is equal to $(\{t_i - f_i z\}_{i=1}^{s}) \cap S$.

(ii): Making $g_i = 1$ for $i = 1, \ldots, s$ in Theorem 2.2.10, we get

$$I(X) = (\{t_i - f_i z\}_{i=1}^{s}, y_0 - 1) \cap S$$

and $I(X)$ is the presentation ideal of $K[f_1 z, \ldots, f_s z]$. Since $t_i - f_i z$ is independent of $y_0$ it follows readily that $(\{t_i - f_i z\}_{i=1}^{s}, y_0 - 1) \cap S$ is equal to $(\{t_i - f_i z\}_{i=1}^{s}) \cap S$.

(iii) and (iv): The two assertions follow by the arguments above and by a direct application of Theorems 2.2.11 and 2.2.13 respectively. □

**Corollary 2.2.26.** *Let $K$ be an infinite field. The following hold for polynomial parameterizations.*

(a) [9, Theorem 1, p. 128] $\overline{\mathbb{X}^*} = V((\{t_i - f_i\}_{i=1}^{s}) \cap S)$.

(b) If $\mathbb{X} \neq \emptyset$ and $X^* \neq \emptyset$, then $I(X) = I(\mathbb{X})$ and $I(X^*) = I(\mathbb{X}^*)$.

(c) If $\mathbb{X} \neq \emptyset$ and $X^* \neq \emptyset$, then $\overline{X} = \overline{\mathbb{X}}$ and $\overline{X^*} = \overline{\mathbb{X}^*}$.

**Proof.** Notice that $\overline{X^*} = V(I(X^*))$ and $\overline{\mathbb{X}^*} = V(I(\mathbb{X}^*))$ (see Lemma 1.4.15) and that similar formulas hold for $X$ and $\mathbb{X}$. Thus the result follows from Theorem 2.2.25. □

Next we recover a result of [49].

**Corollary 2.2.27.** [49, Theorem 6.9] *If $K$ is an infinite field and $X$ is a projective algebraic set parameterized by monomials $y^{v_1}, \ldots, y^{v_s}$ in $R$, then $I(X) = (\{t_i - y^{v_i} z\}_{i=1}^{s}) \cap S$ and $I(X)$ is the presentation ideal of $K[y^{v_1} z, \ldots, y^{v_s} z]$.*

**Proof.** It follows at once from Theorem 2.2.25(ii). □

## 2.3 Rational parameterizations over finite fields

Throughout this section $K = \mathbb{F}_q$ is a finite field and $\mathbb{X}$, $\mathbb{X}^*$, $X$ and $X^*$, are the sets parameterized by rational functions $F = \{f_1/g_1, \ldots, f_s/g_s\}$ in $K(\mathbf{y})$.

**Proposition 2.3.1.** [37, pp. 136–137] *Let $K = \mathbb{F}_q$ be a finite field and let $\mathbb{A}^s$ be the affine space of dimension $s$ over $K$. Then $I(\mathbb{A}^s) = (\{t_i^q - t_i\}_{i=1}^s)$.*

**Proof.** The inclusion "$\supset$" is clear. To show the inclusion "$\subset$" take $f \in I(\mathbb{A}^s)$. Consider the GRevLex order $\prec$ on $S$. By the division algorithm [9, Theorem 3, p. 63] the residue of dividing $f$ by $\{t_i^q - t_i\}_{i=1}^s$, denoted by $g$, satisfies that $\deg_{t_i}(g) < q$ for all $i$. Thus, by Lemma 2.2.2, $g = 0$. Hence $f \in (\{t_i^q - t_i\}_{i=1}^s)$. □

**Lemma 2.3.2.** *Let $K = \mathbb{F}_q$ be a finite field. The following conditions are equivalent:*

(a) *$g_1 \cdots g_s$ vanishes at all points of $K^n$.*

(b) *$g_1 \cdots g_s \in (\{y_i^q - y_i\}_{i=1}^n)$.*

(c) *$(\{g_i t_i - f_i z\}_{i=1}^s, \{y_i^q - y_i\}_{i=1}^n, y_0 g_1 \cdots g_s - 1) \cap S = S$.*

(d) *$\mathbb{X}^* = \emptyset$.*

**Proof.** (a) $\Leftrightarrow$ (b)): This follows at once from Proposition 2.3.1.

(a) $\Leftrightarrow$ (d)): This follows from the definition of $\mathbb{X}^*$.

(c) $\Rightarrow$ (a)): We can write $1 = \sum_{i=1}^s a_i(g_i t_i - f_i z) + \sum_{j=1}^n b_j(y_j^q - y_j) + h(y_0 g_1 \cdots g_s - 1)$, where the $a_i$'s, $b_j$'s and $h$ are polynomials in the variables $y_j$'s, $t_i$'s, $y_0$ and $z$. Take an arbitrary point $x = (x_i)$ in $K^n$. In the equality above, making $y_i = x_i$ for all $i$, $z = 0$ and $t_i = 0$ for all $i$, we get that $1 = h_1(y_0 g_1(x) \cdots g_s(x) - 1)$ for some $h_1$. If $(g_1 \cdots g_s)(x) \neq 0$, then $h_1(y_0 g_1(x) \cdots g_s(x) - 1)$ is a polynomial in $y_0$ of positive degree, a contradiction. Thus $(g_1 \cdots g_s)(x) = 0$.

(b) $\Rightarrow$ (c)): Writing $g_1 \cdots g_s = \sum_{j=1}^n b_j(y_j^q - y_j)$, we get

$$y_0 g_1 \cdots g_s - 1 = -1 + \sum_{j=1}^n y_0 b_j(y_j^q - y_j)$$

Thus 1 is in the ideal $(\{g_i t_i - f_i z\}_{i=1}^s, \{y_i^q - y_i\}_{i=1}^n, y_0 g_1 \cdots g_s - 1)$. □

**Example 2.3.3.** If $K = \mathbb{F}_3$, $f_1 = y_2 y_3$, $f_2 = y_1 y_3$, $g_1 = y_1^3 - y_1$ and $g_2 = 1$, then clearly $\mathbb{X}^* = \emptyset$. Thus $(g_1 t_1 - f_1 z, g_2 t_2 - f_2 z, y_1^3 - y_1, y_2^3 - y_2, y_3^3 - y_3, g_1 g_2 y_0 - 1) \cap S = S$.

**Lemma 2.3.4.** *Let $K = \mathbb{F}_q$ be a finite field. The following conditions are equivalent:*

(a) *$(\{g_i t_i - f_i z\}_{i=1}^s, \{y_i^q - y_i\}_{i=1}^n, y_0 g_1 \cdots g_s - 1) \cap S = (t_1, \ldots, t_s)$.*

(b) *$\mathbb{X}^* = \{0\}$.*

**Proof.** (a) $\Rightarrow$ (b)): By Lemma 2.3.2, $\mathbb{X}^* \neq \emptyset$. Take a point $P$ in $\mathbb{X}^*$, i.e., there is $x = (x_i) \in \mathbb{A}^s$ such that $g_i(x) \neq 0$ for all $i$ and $P = (f_1(x)/g_1(x), \ldots, f_s(x)/g_s(x))$. By hypothesis, for each $t_k$, we can write

$$t_k = \sum_{i=1}^s a_i(g_i t_i - f_i z) + \sum_{j=1}^n b_j(y_j^q - y_j) + h(y_0 g_1 \cdots g_s - 1), \tag{2.3.1}$$

where the $a_i$'s, $b_j$'s and $h$ are polynomials in the variables $y_j$'s, $t_i$'s, $y_0$ and $z$. From Eq. (2.3.1), making $y_i = x_i$ for all $i$, $y_0 = 1/g_1(x)\cdots g_s(x)$, $t_i = f_i(x)/g_i(x)$ for all $i$, and $z = 1$, we get that $f_k(x)/g_k(x) = 0$. Thus $P = 0$.

(b) $\Rightarrow$ (a)): Setting $I = (\{g_it_i - f_iz\}_{i=1}^s, \{y_i^q - y_i\}_{i=1}^n, y_0g_1\cdots g_s - 1)$, by Lemma 2.3.2 one has that $I \cap S \subsetneq S$. Thus it suffices to show that $t_k \in I \cap S$ for all $k$. Notice that $g_1\cdots g_sf_k$ vanishes at all points of $\mathbb{A}^n$ because $\mathbb{X}^* = \{0\}$. Hence, thanks to Proposition 2.3.1, $g_1\cdots g_sf_k$ is in $(\{y_i^q - y_i\}_{i=1}^n)$. Setting $W = y_0g_1\cdots g_s - 1$, and applying Lemma 2.1.1 with $f = t_k$, we can write

$$(W+1)^2t_k = \sum_{i=1}^s y_0^2g_1\cdots g_sh_i(g_it_i - f_iz) + y_0^2g_1^2\cdots g_s^2z(f_k/g_k).$$

Therefore $(W+1)^2t_k \in I$. Thus $t_k \in I \cap S$. $\Box$

**Example 2.3.5.** Using *Macaulay*2 [30], and the procedure below, we get that

$$I \cap S = (t_1, \ldots, t_s),$$

i.e., $\mathbb{X}^* = \{0\}$ in concordance with Lemma 2.3.4.

```
B=GF(3)[y0,y1,y2,y3,y4,y5,z,t1,t2,t3,t4,t5,t6,MonomialOrder=>Eliminate 7];
f1=y1*y3, f2=y1*y4, f3=y1*y5, f4=y2*y3, f5=y2*y4, f6=y2*y5,
g1=y2^2-1, g2=y3^2-1, g3=y1^3-1, g4=y1^3-1, g5=y4^2-1 ,g6=y1^2-1, q=3
I=ideal(g1*t1-f1*z,g2*t2-f2*z,g3*t3-f3*z,g4*t4-f4*z,g5*t5-f5*z,g6*t6-f6*z,
y1^q-y1,y2^q-y2,y3^q-y3,y4^q-y4,y5^q-y5,g1*g2*g3*g4*g5*g6*y0-1)
Ixx=ideal selectInSubring(1,gens gb Ia)
mingens Ixx
```

**Lemma 2.3.6.** *If* $I = (\{g_it_i - f_iz\}_{i=1}^s, \{y_i^q - y_i\}_{i=1}^n, y_0g_1\cdots g_s - 1)$ *and* $\mathfrak{m} = (t_1, \ldots, t_s)$ *is the irrelevant maximal ideal of* $S$*, then*

(a) $I \cap S$ *is graded, and*

(b) $\mathbb{X} \neq \emptyset$ *if and only if* $I \cap S \subsetneq \mathfrak{m}$.

**Proof.** (a): We set $B = K[y_0, y_1, \ldots, y_n, z, t_1, \ldots, t_s]$. Take $0 \neq f \in I \cap S$ and write it as $f = f_1 + \cdots + f_r$, where $f_i$ is a homogeneous polynomial of degree $d_i$ and $d_1 < \cdots < d_r$. By induction, using Proposition 1.4.14, it suffices to show that $f_r \in I \cap S$. We can write

$$f = \sum_{i=1}^s a_i(g_it_i - f_iz) + \sum_{i=1}^n c_i(y_i^q - y_i) + c(y_0g_1\cdots g_s - 1),$$

where the $a_i$'s, $c_i$'s, and $c$ are in $B$. Making the substitution $t_i \to t_iv$, $z \to zv$, with $v$ an extra variable, and regarding $f(t_1v, \ldots, t_sv)$ as a polynomial in $v$ it follows readily that $v^{d_r}f_r$ is in the ideal generated by $\mathcal{B} = \{g_it_iv - f_izv\}_{i=1}^s \cup \{y_i^q - y_i\}_{i=1}^n \cup \{y_0g_1\cdots g_s - 1\}$.

Writing $v^{d_r}f_r$ as a linear combination of $\mathcal{B}$, with coefficients in $B$, and making $v=1$, we get that $f_r\in I\cap S$.

(b): $\Rightarrow$) If $\mathbb{X}\neq\emptyset$, by Lemma 2.3.2, we get that $I\cap S\neq S$. By part (a) the ideal $I\cap S$ is graded. Hence $I\cap S\subsetneq\mathfrak{m}$.

$\Leftarrow$) If $I\cap S\subsetneq\mathfrak{m}$, by Lemmas 2.3.2 and 2.3.4, we get $\mathbb{X}^*\neq\emptyset$ and $\mathbb{X}^*\neq\{0\}$. Thus $\mathbb{X}\neq\emptyset$. □

**Theorem 2.3.7.** *Let $B=K[y_0,y_1,\ldots,y_n,z,t_1,\ldots,t_s]$ be a polynomial ring over a finite field $K=\mathbb{F}_q$. If $\mathbb{X}$ is a projective set parameterized by rational functions $f_1/g_1,\ldots,f_s/g_s$ in $K(\mathbf{y})$ and $\mathbb{X}\neq\emptyset$, then*

$$I(\mathbb{X})=(\{g_it_i-f_iz\}_{i=1}^s,\{y_i^q-y_i\}_{i=1}^n,y_0g_1\cdots g_s-1)\cap S.$$

**Proof.** We set $I=(\{g_it_i-f_iz\}_{i=1}^s,\{y_i^q-y_i\}_{i=1}^n,y_0g_1\cdots g_s-1)$. First we show the inclusion $I(\mathbb{X})\subset I\cap S$. Take a homogeneous polynomial $f=f(t_1,\ldots,t_s)$ of degree $d$ that vanishes at all points of $\mathbb{X}$. Setting $W=y_0g_1\cdots g_s-1$, by Lemma 2.1.1, we can write

$$(W+1)^{d+1}f=\sum_{i=1}^s y_0^{d+1}g_1\cdots g_sa_i(g_it_i-f_iz)+z^dy_0^{d+1}g_1^{d+1}\cdots g_s^{d+1}f(f_1/g_1,\ldots,f_s/g_s),\tag{2.3.2}$$

where $a_1,\ldots,a_s$ are in $B$. We set $H=g_1^{d+1}\cdots g_s^{d+1}f(f_1/g_1,\ldots,f_s/g_s)$. This is a polynomial in $K[\mathbf{y}]$. Thus, by the division algorithm in $K[\mathbf{y}]$ (see [9, Theorem 3, p. 63]), we can write

$$H=H(y_1,\ldots,y_n)=\sum_{i=1}^n h_i(y_i^q-y_i)+G(y_1,\ldots,y_n)\tag{2.3.3}$$

for some $h_1,\ldots,h_n$ in $K[\mathbf{y}]$, where the monomials that occur in $G=G(y_1,\ldots,y_n)$ are not divisible by any of the monomials $y_1^q,\ldots,y_n^q$, i.e., $\deg_{y_i}(G)<q$ for $i=1,\ldots,n$. Therefore, using Eqs. (2.3.2) and (2.3.3), we obtain the equality

$$(W+1)^{d+1}f=\sum_{i=1}^s y_0^{d+1}g_1\cdots g_sa_i(g_it_i-f_iz)+z^dy_0^{d+1}\sum_{i=1}^n h_i(y_i^q-y_i)+z^dy_0^{d+1}G(y_1,\ldots,y_n).\tag{2.3.4}$$

Thus to show that $f\in I\cap S$ we only need to show that $G=0$. We claim that $G$ vanishes on $K^n$. Notice that $y_i^q-y_i$ vanishes at all points of $K^n$ because $(K^*,\,\cdot\,)$ is a group of order $q-1$. Take an arbitrary sequence $x_1,\ldots,x_n$ of elements of $K$, i.e., $x=(x_i)\in K^n$.

Case (I): $g_i(x)=0$ for some $i$. Making $y_j=x_j$ for all $j$ in Eq. (2.3.4) we get $G(x)=0$.

Case (II): $f_i(x)=0$ and $g_i(x)\neq 0$ for all $i$. Making $y_k=x_k$ and $t_j=f_j(x)/g_j(x)$ for all $k,j$ in Eq. (2.3.4) and using that $f$ is homogeneous, we obtain that $G(x)=0$.

Case (III): $f_i(x)\neq 0$ for some $i$ and $g_\ell(x)\neq 0$ for all $\ell$. In this case, making $y_k=x_k$, $t_j=f_j(x)/g_j(x)$ and $z=1$ in Eq. (2.3.4) and using that $f$ vanishes on $[(f_1(x)/g_1(x),\ldots,f_s(x)/g_s(x))]$, we get that $G(x)=0$. This completes the proof of the claim.

Therefore $G$ vanishes at all points of $K^n$ and $\deg_{y_i}(G) < q$ for all $i$. Hence, by Lemma 2.2.2, we get that $G = 0$.

Next we show the inclusion $I(\mathbb{X}) \supset I \cap S$. By Lemma 2.3.6 we have that the ideal $I \cap S$ is graded. Let $f$ be a homogeneous polynomial of $I \cap S$. Take a point $[P]$ in $\mathbb{X}$ with $P = (f_1(x)/g_1(x), \ldots, f_s(x)/g_s(x))$. Writing $f$ as a linear combination of the elements $\{g_it_i - f_iz\}_{i=1}^s, \{y_i^q - y_i\}_{i=1}^n, y_0g_1 \cdots g_s - 1$, with coefficients in $K$, and making $t_i = f_i(x)/g_i(x)$, $y_j = x_j$, $z = 1$ and $y_0 = 1/g_1(x) \cdots g_s(x)$ for all $i, j$ it follows that $f(P) = 0$. Thus $f$ vanishes on $\mathbb{X}$. $\Box$

**Lemma 2.3.8.** *If* $I := (\{g_it_i - f_iz\}_{i=1}^s, \{y_i^q - y_i\}_{i=1}^n, y_0g_1 \cdots g_s - 1, wf_1 \cdots f_s - 1)$ *and* $K = \mathbb{F}_q$ *is a finite field, then the following conditions are equivalent*:

(a) $g_1 \cdots g_s f_1 \cdots f_s$ *vanishes at all points of* $K^n$,

(b) $g_1 \cdots g_s f_1 \cdots f_s \in (\{y_i^q - y_i\}_{i=1}^n)$,

(c) $I \cap S = S$,

(d) $X = \emptyset$.

**Proof.** (a) $\Leftrightarrow$ (b)): This follows at once from Proposition 2.3.1.

(a) $\Leftrightarrow$ (d)): This follows from the definition of $X$.

(c) $\Rightarrow$ (a)): Writing

$$1 = \sum_i^s a_i(g_it_i - f_iz) + \sum_j^n b_j(y_j^q - y_j) + h(y_0g_1 \cdots g_s - 1) + h_1(f_1 \cdots f_sw - 1),$$

where the $a_i$'s, $b_j$'s, $h$ and $h_1$ are polynomials in the variables $y_j$'s, $t_i$'s, $y_0$, $w$ and $z$. We proceed by contradiction assuming there is a point $x = (x_1, \ldots, x_n)$ in $K^n$ such that $(g_1 \cdots g_s f_1 \cdots g_s)(x) \neq 0$. Making $y_i = x_i$ for all $i$, $z = 0$, $t_i = 0$, for all $i$, $y_0 = 1/(g_1 \cdots g_s)(x)$, and $w = 1/(f_1 \cdots f_s)(x)$, in the equation above we get that $1 = 0$, a contradiction.

(b) $\Rightarrow$ (c)): Since $wf_1 \cdots f_s(y_0g_1 \cdots g_s - 1) + (wf_1 \cdots f_s - 1) + 1 = wy_0f_1 \cdots f_sg_1 \cdots g_s$, we get that $1 \in I \cap S$. $\Box$

The ideal $I(X)$ can be computed from $I(\mathbb{X})$ using the colon operation.

**Proposition 2.3.9.** *If* $X \neq \emptyset$, *then* $(I(\mathbb{X}) \colon t_1 \cdots t_s) = I(X)$.

**Proof.** Since $X \subset \mathbb{X}$, one has $I(\mathbb{X}) \subset I(X)$. Consequently $(I(\mathbb{X}) \colon t_1 \cdots t_s) \subset I(X)$ because $t_i$ is not a zero-divisor of $S/I(X)$ for all $i$. To show the reverse inclusion take a homogeneous polynomial $f$ in $I(X)$. Let $[P]$ be a point in $\mathbb{X}$, with $P = (\alpha_1, \ldots, \alpha_s)$ and $\alpha_k \neq 0$ for some $k$, and let $I_{[P]}$ be the ideal generated by the homogeneous polynomials of $S$ that vanish at $[P]$. Then $I_{[P]}$ is a prime ideal of height $s - 1$,

$$I_{[P]} = (\{\alpha_kt_i - \alpha_it_k |\, k \neq i \in \{1, \ldots, s\}),\ I(\mathbb{X}) = \bigcap_{[Q] \in \mathbb{X}} I_{[Q]}, \tag{2.3.5}$$

and the latter is the primary decomposition of $I(\mathbb{X})$. Noticing that $t_i \in I_{[P]}$ if and only if $\alpha_i = 0$, it follows that $t_1 \cdots t_s f \in I(\mathbb{X})$. Indeed if $[P]$ has at least one entry equal to zero, then $t_1 \cdots t_s \in I_{[P]}$ and if all entries of $P$ are not zero, then $f \in I(X) \subset I_{[P]}$. In either case $t_1 \cdots t_s f \in I(\mathbb{X})$. Hence $f \in (I(\mathbb{X})\colon t_1 \cdots t_s)$. □

Next we present some other means to compute the vanishing ideal $I(X)$.

**Theorem 2.3.10.** *Let $B = K[y_0, w, y_1, \ldots, y_n, z, t_1, \ldots, t_s]$ be a polynomial ring over a finite field $K = \mathbb{F}_q$. If $X$ is a projective algebraic set parameterized by rational functions $f_1/g_1, \ldots, f_s/g_s$ in $K(\mathbf{y})$ and $X \neq \emptyset$, then*

$$I(X) = (\{g_i t_i - f_i z\}_{i=1}^s, \{y_i^q - y_i\}_{i=1}^n, y_0 g_1 \cdots g_s - 1, w f_1 \cdots f_s - 1) \cap S.$$

**Proof.** We set $I = (\{g_i t_i - f_i z\}_{i=1}^s, \{y_i^q - y_i\}_{i=1}^n, y_0 g_1 \cdots g_s - 1, w f_1 \cdots f_s - 1)$. First we show the inclusion $I(X) \subset I \cap S$. Take a homogeneous polynomial $f = f(t_1, \ldots, t_s)$ of degree $d$ that vanishes at all points of $X$. Setting $W_1 = y_0 g_1 \cdots g_s - 1$ and $W_2 = w f_1 \cdots f_s - 1$, by Lemma 2.1.1, we can write

$$(W_1 + 1)^{d+1}(W_2 + 1)f = \sum_{i=1}^{s} y_0^{d+1} g_1 \cdots g_s (W_2 + 1) a_i (g_i t_i - f_i z) + w z^d y_0^{d+1} H, \qquad (2.3.6)$$

where $a_1, \ldots, a_s$ are in $B$ and $H = f_1 \cdots f_s g_1^{d+1} \cdots g_s^{d+1} f(f_1/g_1, \ldots, f_s/g_s)$. As $H$ is a polynomial in $K[\mathbf{y}]$, by the division algorithm in $K[\mathbf{y}]$ (see [9, Theorem 3, p. 63]), we can write

$$H = H(y_1, \ldots, y_n) = \sum_{i=1}^{n} h_i (y_i^q - y_i) + G(y_1, \ldots, y_n) \qquad (2.3.7)$$

for some $h_1, \ldots, h_n$ in $K[\mathbf{y}]$, where the monomials that occur in $G = G(y_1, \ldots, y_n)$ are not divisible by any of the monomials $y_1^q, \ldots, y_n^q$, i.e., $\deg_{y_i}(G) < q$ for $i = 1, \ldots, n$. Therefore, setting $F = (W_1 + 1)^{d+1}(W_2 + 1)f$ and using Eqs. (2.3.6) and (2.3.7), we obtain the equality

$$F = \sum_{i=1}^{s} y_0^{d+1} g_1 \cdots g_s (W_2 + 1) a_i (g_i t_i - f_i z) + w z^d y_0^{d+1} \sum_{i=1}^{n} h_i (y_i^q - y_i) + w z^d y_0^{d+1} G. \quad (2.3.8)$$

Thus to show that $f \in I \cap S$ we only need to show that $G = 0$. By Lemma 2.2.2 it suffices to show that $G$ vanishes on all points of $K^n$ because $\deg_{y_i}(G) < q$ for all $i$. Notice that $y_i^q - y_i$ vanishes at all points of $K^n$ because $(K^*, \cdot\,)$ is a group of order $q - 1$. Take an arbitrary sequence $x_1, \ldots, x_n$ of elements of $K$, i.e., $x = (x_i) \in K^n$.

Case (I): Assume that $f_i(x) = 0$ or $g_i(x) = 0$ for some $i$. Using Eq. (2.3.8), we obtain that $G(x) = 0$.

Case (II): Assume that $f_i(x) g_i(x) \neq 0$ for all $i$. Making $y_i = x_i$, $t_i = f_i(x)/g_i(x)$ and $z = 1$ in Eq. (2.3.8) and using that $f$ vanishes on $[(f_1(x)/g_1(x), \ldots, f_s(x)/g_s(x))]$, we get that $G(x) = 0$.

Next we show the inclusion $I(X) \supset I \cap S$. One can proceed as in the proof of Lemma 2.3.6 to show that $I \cap S$ is graded. Let $f$ be a homogeneous polynomial of $I \cap S$.

Take a point $[P]$ in the set $X$ with $P=(f_1(x)/g_1(x),\ldots,f_s(x)/g_s(x))$. Writing $f$ as a linear combination of

$$\{g_it_i-f_iz\}_{i=1}^s,\{y_i^q-y_i\}_{i=1}^n,y_0g_1\cdots g_s-1,wf_1\cdots f_s-1$$

with coefficients in $B$, and making $t_i=f_i(x)/g_i(x)$, $y_j=x_j$, $z=1$, $y_0=1/g_1(x)\cdots g_s(x)$, and $w=1/f_1(x)\cdots f_s(x)$ for all $i,j$ it follows that $f(P)=0$. Thus $f$ vanishes on $X$. □

**Remark 2.3.11.** The vanishing ideal $I(X)$ can also be computed using the following formula:

$$I(X)=(\{g_it_i-f_iz\}_{i=1}^s,\{y_i^q-y_i\}_{i=1}^n,\{f_i^{q-1}-1\}_{i=1}^s,y_0g_1\cdots g_s-1)\cap S.$$

To show this we can proceed essentially as in the proof of Theorem 2.3.10 by considering the polynomial $F=(W_0+1)^{d+1}(W_1+1)\cdots(W_s+1)$, where $W_0=g_1\cdots g_sy_0-1$ and $W_i=f_i^{q-1}-1$ for $i=1,\ldots,s$.

**Theorem 2.3.12.** *Let $B=K[y_0,y_1,\ldots,y_n,t_1,\ldots,t_s]$ be a polynomial ring over a finite field $K=\mathbb{F}_q$. If $\mathbb{X}^*$ is an affine set parameterized by rational functions $f_1/g_1,\ldots,f_s/g_s$ in $K(\mathbf{y})$, then*

$$I(\mathbb{X}^*)=(\{g_it_i-f_i\}_{i=1}^s,\{y_i^q-y_i\}_{i=1}^n,y_0g_1\cdots g_s-1)\cap S.$$

**Proof.** We set $I=(\{g_it_i-f_i\}_{i=1}^s,\{y_i^q-y_i\}_{i=1}^n,y_0g_1\cdots g_s-1)\cap S$. First we show the inclusion $I(\mathbb{X}^*)\subset I\cap S$. Take a polynomial $f=f(t_1,\ldots,t_s)$ of degree $d$ that vanishes at all points of $\mathbb{X}^*$. Setting $W=y_0g_1\cdots g_s-1$, by Lemma 2.1.1 and using the division algorithm in $K[\mathbf{y}]$ (see the proof of Theorem 2.3.7), we obtain the equality

$$(W+1)^{d+1}f=\sum_{i=1}^{s}y_0^{d+1}g_1\cdots g_sa_i(g_it_i-f_i)+y_0^{d+1}\sum_{i=1}^{n}h_i(y_i^q-y_i)+y_0^{d+1}G(y_1,\ldots,y_n),\tag{2.3.9}$$

where $a_1,\ldots,a_s,h_1,\ldots,h_n$ are in $B$, $G=G(y_1,\ldots,y_n)$ is a polynomial in $K[\mathbf{y}]$ such that $\deg_{y_i}(G)<q$ for $i=1,\ldots,n$. Thus to show that $f\in I\cap S$ we only need to show that $G=0$. By Lemma 2.2.1 it suffices to show that $G$ vanishes on $K^n$. Take an arbitrary sequence $x_1,\ldots,x_n$ of elements of $K$ and set $x=(x_1,\ldots,x_n)$.

Case (I): $g_i(x)=0$ for some $i$. Making $y_j=x_j$ for all $j$ in Eq. (2.3.9) we get $G(x)=0$.

Case (II): $g_i(x)\neq 0$ for all $i$. Making $y_k=x_k$, $t_j=f_j(x)/g_j(x)$ in Eq. (2.3.9) and using that $f$ vanishes on $(f_1(x)/g_1(x),\ldots,f_s(x)/g_s(x))$, we get that $G(x)=0$.

Next we show the inclusion $I(\mathbb{X}^*)\supset I\cap S$. Let $f$ be a polynomial of $I\cap S$. Take a point $P$ in $\mathbb{X}^*$ with $P=(f_1(x)/g_1(x),\ldots,f_s(x)/g_s(x))$. Making $t_i=f_i(x)/g_i(x)$, $y_j=x_j$, and $y_0=1/g_1(x)\cdots g_s(x)$ for all $i,j$, it follows that $f(P)=0$. Thus $f$ vanishes on $\mathbb{X}^*$. □

The ideal $I(X^*)$ can be computed from $I(\mathbb{X}^*)$ using the colon operation.

**Proposition 2.3.13.** $(I(\mathbb{X}^*)\colon t_1\cdots t_s)=I(X^*)$.

**Proof.** This follows adapting the proof of Proposition 2.3.9. □

Next we present some other means to compute the vanishing ideal $I(X^*)$.

**Theorem 2.3.14.** *Let $B = K[y_0, w, y_1, \ldots, y_n, z, t_1, \ldots, t_s]$ be a polynomial ring over a finite field $K = \mathbb{F}_q$. If $X^*$ is an affine algebraic set parameterized by rational functions $f_1/g_1, \ldots, f_s/g_s$ in $K(\mathbf{y})$ with $f_i \neq 0$ for all $i$, then*

$$I(X^*) = (\{g_it_i - f_i\}_{i=1}^s, \{y_i^q - y_i\}_{i=1}^n, y_0g_1 \cdots g_s - 1, wf_1 \cdots f_s - 1) \cap S.$$

**Proof.** This follows adapting the proof of Theorem 2.3.10. □

**Remark 2.3.15.** The vanishing ideal $I(X^*)$ can also be computed using the following formula:

$$I(X^*) = (\{g_it_i - f_i\}_{i=1}^s, \{y_i^q - y_i\}_{i=1}^n, \{f_i^{q-1} - 1\}_{i=1}^s, y_0g_1 \cdots g_s - 1) \cap S.$$

To show this we can proceed essentially as in the proof of Theorem 2.3.10 by considering the polynomial $F = (W_0 + 1)^{d+1}(W_1 + 1) \cdots (W_s + 1)$, where $W_0 = g_1 \cdots g_s y_0 - 1$ and $W_i = f_i^{q-1} - 1$ for $i = 1, \ldots, s$.

**Corollary 2.3.16.** *Let $B = K[t_1, \ldots, t_s, y_1, \ldots, y_n, z]$ be a polynomial ring over the finite field $K = \mathbb{F}_q$ and let $f_1, \ldots, f_s$ be polynomials of $R$. The following hold:*

(a) *If $\mathbb{X} \neq \emptyset$, then $I(\mathbb{X}) = (\{t_i - f_iz\}_{i=1}^s \cup \{y_i^q - y_i\}_{i=1}^n) \cap S$.*

(b) *If $X \neq \emptyset$, then $I(X) = (\{t_i - f_iz\}_{i=1}^s \cup \{y_i^q - y_i\}_{i=1}^n \cup \{f_i^{q-1} - 1\}_{i=1}^s) \cap S$.*

(c) *$I(\mathbb{X}^*) = (\{t_i - f_i\}_{i=1}^s \cup \{y_i^q - y_i\}_{i=1}^n) \cap S$.*

(d) *$I(X^*) = (\{t_i - f_i\}_{i=1}^s \cup \{y_i^q - y_i\}_{i=1}^n \cup \{f_i^{q-1} - 1\}_{i=1}^s) \cap S$.*

**Proof.** The result follows readily by adapting the proof of Theorem 2.2.25, and using Theorem 2.3.7, Remark 2.3.11, Theorem 2.3.12, and Remark 2.3.15, respectively. □

The formula for $I(X)$ given in (b) can be slightly simplified if the $f_i$'s are Laurent monomials (see [52, Theorems 2.1 and 2.13]).

**Example 2.3.17.** Let $f_1 = y_1 + 1$, $f_2 = y_2 + 1$, $f_3 = y_1y_2$ and let $K = \mathbb{F}_5$ be a field with 5 elements. Using Proposition 1.5.4, Corollary 2.3.16, and *Macaulay*2 [30], we get

$$\begin{array}{llll} \deg S/I(\mathbb{X}) = 19, & \deg S/I(X) = 6, & \deg S/I(\mathbb{X}^*) = 25, & \deg S/I(X^*) = 9, \\ \operatorname{reg} S/I(\mathbb{X}) = 5, & \operatorname{reg} S/I(X) = 2, & \operatorname{reg}^a S/I(\mathbb{X}^*) = 4, & \operatorname{reg}^a S/I(X^*) = 2. \end{array}$$

For convenience we present the following procedure for *Macaulay*2 [30] that we used to compute the degree and the regularity:

```
R=GF(5)[z,y1,y2,t1,t2,t3,MonomialOrder=>Eliminate 3];
f1=y1+1,f2=y2+1,f3=y1*y2,q=5
I=ideal(t1-f1*z,t2-f2*z,t3-f3*z,y1^q-y1,y2^q-y2)
Jxx=ideal selectInSubring(1,gens gb I)
I=ideal(t1-f1*z,t2-f2*z,t3-f3*z,y1^q-y1,y2^q-y2,
f1^(q-1)-1,f2^(q-1)-1,f3^(q-1)-1)
Jx=ideal selectInSubring(1,gens gb I)
I=ideal(t1-f1,t2-f2,t3-f3,y1^q-y1,y2^q-y2)
Jxxa=ideal selectInSubring(1,gens gb I)
I=ideal(t1-f1,t2-f2,t3-f3,y1^q-y1,y2^q-y2,
f1^(q-1)-1,f2^(q-1)-1,f3^(q-1)-1)
Jxa=ideal selectInSubring(1,gens gb I)
S=ZZ/5[t1,t2,t3]
Ixx=sub(Jxx,S),Mxx=coker gens Ixx
degree Ixx, regularity Mxx
Ix=sub(Jx,S),Mx=coker gens Ix
degree Ix, regularity Mx
Su=ZZ/5[t1,t2,t3,u]
Ixxa=sub(Jxxa,Su),K=ideal(gens gb Ixxa),Ixxah=homogenize(K,u)
Mxxah=coker gens Ixxah
degree Mxxah, regularity Mxxah
Ixa=sub(Jxa,Su),K=ideal(gens gb Ixa),Ixah=homogenize(K,u)
Mxah=coker gens Ixah
degree Mxah, regularity Mxah
```

**Example 2.3.18.** Let $f_1 = y_1 + 1$, $f_2 = y_2 + 1$, $f_3 = y_1y_2$ and let $K = \mathbb{F}_5$ be a field with 5 elements. Using Proposition 1.5.3, Corollary 2.3.16 and *Macaulay*2 [30], we get

| $d$ | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| $\|\mathbb{X}\|$ | 19 | 19 | 19 | 19 | 19 |
| $\dim C_{\mathbb{X}}(d)$ | 3 | 6 | 10 | 15 | 19 |

| $d$ | 1 | 2 |
|---|---|---|
| $\|X\|$ | 6 | 6 |
| $\dim C_X(d)$ | 3 | 6 |

The $d$th column of these tables represent the length and the dimension of the projective Reed-Muller-type codes $C_{\mathbb{X}}(d)$ and $C_X(d)$, respectively (see Chapter 1). Using Proposition 1.5.4, Corollary 2.3.16 and *Macaulay*2 [30], we get

| $d$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| $\|\mathbb{X}^*\|$ | 25 | 25 | 25 | 25 |
| $\dim C_{\mathbb{X}^*}(d)$ | 4 | 9 | 16 | 25 |

| $d$ | 1 | 2 |
|---|---|---|
| $\|X^*\|$ | 9 | 9 |
| $\dim C_{X^*}(d)$ | 4 | 9 |

Continuing with the *Macaulay*2 procedure of Example 2.3.17 we can compute these four tables as follows:

```
degree Ixx, regularity Mxx
```

```
hilbertFunction(1,Ixx),hilbertFunction(2,Ixx),hilbertFunction(3,Ixx),
hilbertFunction(4,Ixx),hilbertFunction(5,Ixx)
degree Ix, regularity Mx
hilbertFunction(1,Ix),hilbertFunction(2,Ix)
degree Mxxah, regularity Mxxah
hilbertFunction(1,Ixxa),hilbertFunction(2,Ixxa)
hilbertFunction(3,Ixxa), hilbertFunction(4,Ixxa)
degree Mxah, regularity Mxah
hilbertFunction(1,Ixa),hilbertFunction(2,Ixa)
```

**Remark 2.3.19.** Let $K = \mathbb{F}_q$ be a finite field and let $h_1, \ldots, h_m$ be polynomials that generate $I(\mathbb{X}^*)$. The system of polynomial equations $f_i(y) = b_i$ for $i = 1, \ldots, s$ has a solution in the affine space $\mathbb{A}^n$ if and only if $h_i(b) = 0$ for all $i$, where $b = (b_1, \ldots, b_s)$. This follows from Lemma 1.4.15.

Our results are useful to compute a finite set of generators for vanishing ideals over finite fields and are interesting from a theoretical point of view. Let us give some application to vanishing ideals over monomial parameterizations.

**Corollary 2.3.20.** *Let $K = \mathbb{F}_q$ be a finite field. If $\mathbb{X}$, $X$, $\mathbb{X}^*$, $X^*$ are parameterized by Laurent monomials, then $I(\mathbb{X})$, $I(X)$, $I(\mathbb{X}^*)$, $I(X^*)$ are binomial ideals.*

**Proof.** The result follows from Lemma 1.3.24 and applying Theorems 2.3.7, 2.3.10, 2.3.12, and 2.3.14. □

**Corollary 2.3.21.** *Let $K = \mathbb{F}_q$ be a finite field. If $\mathbb{X}$ is parameterized by Laurent monomials, then $I(\mathbb{X})$ is a radical Cohen-Macaulay binomial ideal of dimension* 1.

**Proof.** By Corollary 2.3.20, $I(\mathbb{X})$ is a binomial ideal. That $I(\mathbb{X})$ is a radical ideal of dimension 1 is well known and follows from Eq. (2.3.5) (see the proof of Proposition 2.3.9). Recall that $\operatorname{depth} S/I(\mathbb{X}) \leq \dim S/I(\mathbb{X}) = 1$. From Eq. (2.3.5) one has that $\mathfrak{m} = (t_1, \ldots, t_s)$ is not an associated prime of $I(\mathbb{X})$. Thus $\operatorname{depth} S/I(\mathbb{X}) > 0$ and $\operatorname{depth} S/I(\mathbb{X}) = \dim S/I(\mathbb{X}) = 1$, i.e., $I(\mathbb{X})$ is Cohen-Macaulay. □

**Corollary 2.3.22.** [52, Theorem 2.1] *Let $K = \mathbb{F}_q$ be a finite field and let $X$ be a projective algebraic set parameterized by Laurent monomials. Then $I(X)$ is a Cohen-Macaulay lattice ideal and* $\dim S/I(X) = 1$.

**Proof.** It follows from Proposition 2.3.9, Theorem 2.3.10 and Lemma 1.3.24. □

**Binomial vanishing ideals.** Let $K$ be a field. The projective space $\mathbb{P}^{s-1} \cup \{[0]\})$ together with the zero vector $[0]$ is a monoid under componentwise multiplication, where $[\mathbf{1}] = [(1, \ldots, 1)]$ is the identity of $\mathbb{P}^{s-1} \cup \{[0]\}$. Recall that monoids always have an identity element.

**Lemma 2.3.23.** *Let $K = \mathbb{F}_q$ be a finite field and let $\mathbb{Y}$ be a subset of $\mathbb{P}^{s-1}$. If $\mathbb{Y} \cup \{[0]\}$ is a submonoid of $\mathbb{P}^{s-1} \cup \{[0]\}$ such that each element of $\mathbb{Y}$ is of the form $[\alpha]$ with $\alpha \in \{0,1\}^s$, then $\mathbb{Y}$ is parameterized by Laurent monomials.*

**Proof.** The set $\mathbb{Y}$ can be written as $\mathbb{Y} = \{[\alpha_1], \ldots, [\alpha_m]\}$, where $\alpha_i = (\alpha_{i1}, \ldots, \alpha_{is})$ and $\alpha_{ij} = 0$ or $\alpha_{ik} = 1$ for all $i, k$. Consider variables $y_1, \ldots, y_s$ and $z_1, \ldots, z_s$. For each $\alpha_{ik}$ define $h_{ik} = y_i^{q-1}$ if $\alpha_{ik} = 1$ and $h_{ik} = z_i^{q-1}/y_i^{q-1}$ if $\alpha_{ik} = 0$. Setting $h_i = (h_{i1}, \ldots, h_{is})$ for $i = 1, \ldots, m$ and $F_i = h_{1i} \cdots h_{mi}$ for $i = 1, \ldots, s$, we get

$$h_1 h_2 \cdots h_m = (h_{11} \cdots h_{m1}, \ldots, h_{1s} \cdots h_{ms}) = (F_1, \ldots, F_s).$$

It is not hard to see that $\mathbb{Y}$ is parameterized by $F_1, \ldots, F_s$. □

**Example 2.3.24.** Let $K$ be the field $\mathbb{F}_3$ and let $\mathbb{Y} = \{[(1,1,0)], [0,1,1], [0,1,0], [1,1,1]\}$. With the notation above, we get that $\mathbb{Y}$ is the projective set parameterized by

$$F_1 = (y_1 z_2 z_3)^2/(y_2 y_3)^2,\ F_2 = (y_1 y_2 y_3)^2,\ F_3 = (y_2 z_1 z_3)^2/(y_1 y_3)^2.$$

The next result gives a family of ideals where the converse of Corollary 2.3.21 is true.

**Proposition 2.3.25.** *Let $K = \mathbb{F}_q$ be a finite field. If $\mathbb{Y}$ is a subset of $\mathbb{P}^{s-1}$ such that each element of $\mathbb{Y}$ is of the form $[\alpha]$ with $\alpha \in \{0,1\}^s$ and $I(\mathbb{Y})$ is a binomial ideal, then $\mathbb{Y}$ is a projective set parameterized by Laurent monomials.*

**Proof.** Since $\mathbb{Y}$ is finite, one has that $\mathbb{Y} = \overline{\mathbb{Y}} = V(I(\mathbb{Y}))$. Hence, as $I(\mathbb{Y})$ is generated by binomials, we get that $\mathbb{Y} \cup \{[0]\}$ is a submonoid of $\mathbb{P}^{s-1} \cup \{[0]\}$. Thus, by Lemma 2.3.23, $\mathbb{Y}$ is parameterized by Laurent monomials. □

This leads us to pose the following conjecture.

**Conjecture 2.3.26.** Let $K = \mathbb{F}_q$ be a finite field and let $\mathbb{Y}$ be a subset of $\mathbb{P}^{s-1}$. If $I(\mathbb{Y})$ is a binomial ideal, then $\mathbb{Y}$ is a projective set parameterized by Laurent monomials.

In particular from Proposition 2.3.25 this conjecture is true for $q = 2$.

**Computing degrees using group actions.** Let $K = \mathbb{F}_q$ be a finite field, let $y^{v_1}, \ldots, y^{v_s}$ be Laurent monomials in $K(\mathbf{y})$ and let $X$ and $\mathbb{X}$ be the projective sets parameterized by these monomials. By the exponent laws it is not hard to show that $X$ is a multiplicative group under componentwise multiplication. The group $X$ acts on $\mathbb{X}$ by componentwise multiplication

$$X \times \mathbb{X} \to \mathbb{X}, \quad ([\alpha], [\gamma]) \mapsto [\alpha] \cdot [\gamma], \tag{2.3.10}$$

where $[\alpha] = [(\alpha_1 \ldots, \alpha_s)]$, $[\gamma] = [(\gamma_1, \ldots, \gamma_s)]$ and $[\alpha] \cdot [\gamma] = [(\alpha_1 \gamma_1, \ldots, \alpha_s \gamma_s)]$. One can use this action to study $\mathbb{X}$ as is seen in the next result. Recall that $\mathbb{X}$ decomposes as a disjoint union of the orbits of the action $X \times \mathbb{X} \to \mathbb{X}$, where an orbit of this action is a subset of $\mathbb{X}$ of the form $X \cdot [\gamma] = \{[\alpha] \cdot [\gamma] \mid [\alpha] \in X\}$ for some $[\gamma]$ in $\mathbb{X}$ and where two orbits are either equal or disjoint.

**Proposition 2.3.27.** *Let $G$ be a complete graph with vertices $y_1, \ldots, y_n$, $n \geq 2$, and let $\mathbb{X}_G \subset \mathbb{P}^{s-1}$ be the projective set parameterized by the set of all monomials $y_iy_j$ such that $\{y_i, y_j\}$ is an edge of $G$, where $s = n(n-1)/2$. Then*

$$\deg(S/I(\mathbb{X}_G)) = |\mathbb{X}_G| = \frac{q^n - 1}{q-1} + \binom{n}{2} - n - \binom{n}{2}(q-1).$$

**Proof.** Let $V \subset \{y_1, \ldots, y_n\}$ be a set of vertices of $G$ and let $G_V$ be its induced subgraph which is again a complete graph with vertex set $V$. Consider the algebraic projective set $X_{G_V}$ parameterized by $G_V$. As $G_V$ is a subgraph of $G$, $X_{G_V}$ embeds in $\mathbb{X}_G$, we denote the embedding of $X_{G_V}$ by $\mathbb{X}_{G_V}$. By [52, Corollary 3.8], one has that $|\mathbb{X}_{G_V}| = (q-1)^{|V|-1}$ if $|V| \geq 3$ and $|\mathbb{X}_{G_V}| = 1$ if $|V| = 2$. It is not hard to see that the orbits of the action $X \times \mathbb{X} \to \mathbb{X}$ are precisely the sets $\mathbb{X}_{G_V}$. For each $2 \leq k \leq n$ there are $\binom{n}{k}$ induced subgraphs with $k$ vertices. Hence

$$|\mathbb{X}_G| = \binom{n}{2} + \sum_{k=3}^{n} \binom{n}{k}(q-1)^{k-1} = \binom{n}{2} + \frac{1}{(q-1)} \sum_{k=3}^{n} \binom{n}{k}(q-1)^k.$$

Since $q^n = [(q-1)+1]^n = \sum_{k=0}^{n} \binom{n}{k}(q-1)^k$, the required equality follows readily. □

The next result also follows from the results of Chapter 3.

**Proposition 2.3.28.** *Let $G$ be a complete bipartite graph with bipartition $(V_1, V_2)$, with $m_i = |V_i|$ for $i = 1, 2$, and let $\mathbb{X}_G$ be the projective set parameterized by the monomials corresponding to the edges of $G$. Then*

$$|\mathbb{X}_G| = \frac{q^{m_1} - 1}{q-1} \cdot \frac{q^{m_2} - 1}{q-1}.$$

**Proof.** It follows adapting the proof of Proposition 2.3.27, and using that the group $X_G$ acts on $\mathbb{X}_G$ by componentwise multiplication. □

**Problem 2.3.29.** Let $G$ be a graph. Find a formula for the degree of $S/I(\mathbb{X}_G)$ in terms of the graph invariants of $G$ and the combinatorics of the graph.

If $X_G$ is the algebraic projective set parameterized by the edges of $G$, then a formula for the degree of $S/X_G$ is given in [50, Theorem 3.2].

# Chapter 3

# Direct Products in Projective Segre Codes

Let $K=\mathbb{F}_q$ be a finite field. We introduce a family of projective Reed-Muller-type codes called *projective Segre codes*. Using commutative algebra and linear algebra methods, we study their basic parameters and show that they are direct products of projective Reed-Muller-type codes. As a consequence we recover some results on projective Reed-Muller-type codes over the Segre variety and over projective tori.

## 3.1 Linear codes and direct products

In this section we study direct product codes, and some of their properties and characterizations.

**Generalized Hamming weights.** Let $K=\mathbb{F}_q$ be a finite field and let $C$ be a $[s,k]$ *linear code* of *length* $s$ and *dimension* $k$, that is, $C$ is a linear subspace of $K^s$ 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,

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

The $r$th *generalized Hamming weight* of $C$, denoted $\delta_r(C)$, is the size of the smallest support of an $r$-dimensional subcode, that is,

$$\delta_r(C):=\min\{|\chi(D)|:\; D \text{ is a linear subcode of } C \text{ with } \dim_K(D)=r\}.$$

Let $0\neq v\in C$. The *Hamming weight* of $v$, denoted by $\omega(v)$, is the number of non-zero entries of $v$. If $\delta(C)$ is the *minimum distance* of $C$, that is,

$$\delta(C):=\min\{\omega(v)\colon\, 0\neq v\in C)\},$$

then note that $\delta_1(C) = \delta(C)$. The *weight hierarchy* of $C$ is the sequence $(\delta_1(C), \ldots, \delta_k(C))$. According to [71, Theorem 1] the weight hierarchy is an increasing sequence

$$1 \leq \delta_1(C) < \delta_2(C) < \cdots < \delta_r(C) \leq s,$$

and $\delta_r(C) \leq s - k + r$ for $r = 1, \ldots, k$. For $r = 1$ this is the Singleton bound for the minimum distance. Generalized Hamming weights have received a lot of attention; see [7, 20, 58, 71, 72] and the references therein.

**Direct product codes and tensor products.** Let $C_1 \subset K^{s_1}$ and $C_2 \subset K^{s_2}$ be two linear codes over the finite field $K = \mathbb{F}_q$ and let $M_{s_1 \times s_2}(K)$ be the $K$-vector space of all matrices of size $s_1 \times s_2$ with entries in $K$.

The *direct product* (also called *Kronecker product*) of $C_1$ and $C_2$, denoted by $C_1 \underline{\otimes} C_2$, is defined to be the linear code consisting of all $s_1 \times s_2$ matrices in which the rows belong to $C_2$ and the columns to $C_1$; see [66, p. 44]. The direct product codes usually have poor minimum distance but are easy to decode and can be useful in certain applications; see [46, Chapter 18].

We denote the tensor product of $C_1$ and $C_2$—in the sense of multilinear algebra [13, p. 573]—by $C_1 \otimes_K C_2$. As is shown in Lemma 3.1.4 another way to see the direct product of $C_1$ and $C_2$ is as a tensor product.

**Theorem 3.1.1.** [67, Theorems 2.5.2 and 2.5.3] *Let $C_i \subset K^{s_i}$ be a linear code of length $s_i$, dimension $k_i$, and minimum distance $\delta(C_i)$ for $i = 1, 2$. Then $C_1 \underline{\otimes} C_2$ has length $s_1 s_2$, dimension $k_1 k_2$, and minimum distance $\delta(C_1)\delta(C_2)$.*

**Theorem 3.1.2.** [72, Theorem 3(d)] *Let $C_1 \subset K^{s_1}$ and $C_2 \subset K^{s_2}$ be two linear codes and let $C = C_1 \underline{\otimes} C_2$ be their direct product. Then*

$$\delta_2(C) = \min\{\delta_1(C_1)\delta_2(C_2), \delta_2(C_1)\delta_1(C_2)\}.$$

**Proof.** Let $V_1$ and $V_2$ be subcodes of $C_1$ and $C_2$ of dimensions 2 and 1, respectively. Setting $V = V_1 \underline{\otimes} V_2$, $\chi(V_1) = \{j_1, \ldots, j_r\}$, and $\chi(V_2) = \{i_1, \ldots, i_m\}$, one has

$$\begin{aligned} \chi(V) &= \{(i,j) \mid \exists\, \alpha \in V \text{ whose } (i,j)\text{-entry is not } 0\} \\ &= \{(i_k, j_\ell) \mid 1 \leq k \leq m,\ 1 \leq \ell \leq r\} \\ &= \chi(V_2) \times \chi(V_1). \end{aligned}$$

Therefore, using that $\dim(V) = 2$ (see Theorem 3.1.1), we get

$$\delta_2(C) \leq |\chi(V)| = |\chi(V_2)||\chi(V_1)|.$$

Hence $\delta_2(C) \leq \delta_1(C_2)\delta_2(C_1)$. By a similar argument, considering subcodes $V_1$ and $V_2$ of $C_1$ and $C_2$ of dimensions 1 and 2, respectively, we get that $\delta_2(C) \leq \delta_1(C_1)\delta_2(C_2)$. Thus

$$\delta_2(C) \leq \min\{\delta_1(C_1)\delta_2(C_2), \delta_2(C_1)\delta_1(C_2)\}.$$

Next we show the reverse inequality. Let $V$ be an arbitrary subcode of $C$ of dimension 2. Consider the subcode $W_2$ of $C_2$ generated by the rows of all matrices in $V$ and the subcode $W_1$ of $C_1$ generated by the columns of all matrices in $V$. Since $V \subset W_1 \underline{\otimes} W_2$, by Theorem 3.1.1, we get that $\dim_K(W_1)\dim_K(W_2) \geq 2$. If $\dim_K(W_2) \geq 2$, then $|\chi(W_2)| \geq \delta_2(C_2)$. We set $\chi(W_2) = \{j_1, \ldots, j_r\}$. For $\alpha \in C$ denote the $(i,j)$-entry of $\alpha$ by $\alpha_{i,j}$. Recall that

$$\chi(V) = \{(i,j) | \, \exists\, \alpha \in V \text{ with } \alpha_{i,j} \neq 0\}.$$

Let $R_1, \ldots, R_m$ be the list of all rows of matrices in $V$, i.e., the $R_i$'s form a generating set for $W_2$. For each $j_i \in \chi(W_2)$ there exists $\gamma = (\gamma_1, \ldots, \gamma_{s_2})$ with $\gamma_{j_i} \neq 0$. We can write

$$\gamma = \mu_1 R_1 + \mu_2 R_2 + \cdots + \mu_m R_m$$

for some $\mu_i$'s in $K$. Clearly there is $\ell$ such that the $j_i$-entry of $R_\ell$ is not zero. Hence there is $\alpha \in V$ whose $(k, j_i)$-entry is not zero for some $k$. Therefore there are at least $\delta_1(C_1)$ non-zero entries in the column $j_i$ of $\alpha$. Hence, as $j_1, \ldots, j_r$ are distinct, we get

$$|\chi(V)| \geq |\chi(W_2)|\delta_1(C_1) \geq \delta_2(C_2)\delta_1(C_1).$$

If $\dim(W_1) \geq 2$, a similar argument (with $W_1$ playing the role of $W_2$) shows that

$$|\chi(V)| \geq \delta_2(C_1)\delta_1(C_2).$$

Therefore $\delta_2(C) \geq \min\{\delta_1(C_1)\delta_2(C_2), \delta_2(C_1)\delta_1(C_2)\}$. □

Recall that there is a natural isomorphism $\operatorname{vec}\colon M_{s_1 \times s_2}(K) \to K^{s_1 s_2}$ of $K$-vector spaces given by $\operatorname{vec}(A) = (F_1, \ldots, F_{s_1})$, where $F_1, \ldots, F_{s_1}$ are the rows of $A$. Consider the bilinear map $\psi_0$ given by

$$\begin{array}{rcl} \psi_0\colon K^{s_1} \times K^{s_2} & \longrightarrow & M_{s_1 \times s_2}(K) \\ ((a_1, \ldots, a_{s_1}), (b_1, \ldots, b_{s_2})) & \longmapsto & \begin{bmatrix} a_1 b_1 & a_1 b_2 & \ldots & a_1 b_{s_2} \\ a_2 b_1 & a_2 b_2 & \ldots & a_2 b_{s_2} \\ \vdots & \vdots & & \vdots \\ a_{s_1} b_1 & a_{s_1} b_2 & \ldots & a_{s_1} b_{s_2} \end{bmatrix}. \end{array}$$

**Definition 3.1.3.** The *Segre embedding* is given by

$$\psi([a],[b]) := [(\operatorname{vec} \circ \psi_0)(a,b)].$$

The map $\psi$ is well-defined and injective [35, p. 13].

The next lemma is not hard to prove and is probably known in some equivalent formulation; but we could not find a reference with the corresponding proof.

**Lemma 3.1.4.** *There is an isomorphism $T\colon C_1 \otimes_K C_2 \to C_1 \underline{\otimes} C_2$ of $K$-vector spaces such that $T(a \otimes b) = \psi_0(a,b)$ for $a \in C_1$ and $b \in C_2$.*

**Proof.** We set $k_i = \dim_K(C_i)$ for $i = 1, 2$. Using the universal property of the tensor product [13, p. 573], we get that the bilinear map $\psi_0$ induces a linear map

$$\begin{array}{rcl} T\colon C_1 \otimes_K C_2 & \longrightarrow & C_1 \underline{\otimes} C_2, \text{ such that,} \\ a \otimes b & \longmapsto & \psi_0(a, b) \end{array}$$

for $a \in C_1$ and $b \in C_2$. By [47, Formula 5, p. 267] and Theorem 3.1.1, one has that $C_1 \otimes_K C_2$ and $C_1 \underline{\otimes} C_2$ have dimension $k_1k_2$. Thus to prove that $T$ is an isomorphism it suffices to prove that $T$ is a one-to-one linear map. Fix bases $\{\alpha_1, \ldots, \alpha_{k_1}\}$ and $\{\beta_1, \ldots, \beta_{k_2}\}$ of $C_1$ and $C_2$, respectively. Take any element $\gamma$ in the kernel of $T$. We can write

$$\gamma = \sum \lambda_{i,j}\alpha_i \otimes \beta_j$$

with $\lambda_{i,j}$ in $K$ for all $i, j$. Then

$$\begin{array}{rcl} T(\gamma) & = & \lambda_{1,1}T(\alpha_1 \otimes \beta_1) + \cdots + \lambda_{1,k_2}T(\alpha_1 \otimes \beta_{k_2}) + \\ & & \lambda_{2,1}T(\alpha_2 \otimes \beta_1) + \cdots + \lambda_{2,k_2}T(\alpha_2 \otimes \beta_{k_2}) + \\ & & \vdots \\ & & \lambda_{k_1,1}T(\alpha_{k_1} \otimes \beta_1) + \cdots + \lambda_{k_1,k_2}T(\alpha_{k_1} \otimes \beta_{k_2}). \end{array}$$

Setting $\alpha_i = (\alpha_{i,1}, \ldots, \alpha_{i,s_1})$, $\beta_j = (\beta_{j,1}, \ldots, \beta_{j,s_2})$ for $i = 1, \ldots, k_1$, $j = 1, \ldots, k_2$, we get

$$T(\gamma) = \begin{bmatrix} (\lambda_{1,1}\alpha_{1,1}\beta_1 + \cdots + \lambda_{1,k_2}\alpha_{1,1}\beta_{k_2}) + \cdots + (\lambda_{k_1,1}\alpha_{k_1,1}\beta_1 + \cdots + \lambda_{k_1,k_2}\alpha_{k_1,1}\beta_{k_2}) \\ (\lambda_{1,1}\alpha_{1,2}\beta_1 + \cdots + \lambda_{1,k_2}\alpha_{1,2}\beta_{k_2}) + \cdots + (\lambda_{k_1,1}\alpha_{k_1,2}\beta_1 + \cdots + \lambda_{k_1,k_2}\alpha_{k_1,2}\beta_{k_2}) \\ \vdots \\ (\lambda_{1,1}\alpha_{1,s_1}\beta_1 + \cdots + \lambda_{1,k_2}\alpha_{1,s_1}\beta_{k_2}) + \cdots + (\lambda_{k_1,1}\alpha_{k_1,s_1}\beta_1 + \cdots + \lambda_{k_1,k_2}\alpha_{k_1,s_1}\beta_{k_2}) \end{bmatrix}.$$

Since $T(\gamma) = (0)$, using that the $\beta_i$'s are linearly independent, we get

$$\lambda_{1,j}\alpha_1^\top + \cdots + \lambda_{k_1,j}\alpha_{k_1}^\top = 0 \text{ for } j = 1, \ldots, k_2.$$

Thus $\lambda_{i,j} = 0$ for all $i, j$ and $\gamma = 0$. □

## 3.2 Segre products of coordinate rings

In this section we study Segre products of standard graded algebras arising from vanishing ideals.

Let $K$ be an arbitrary field, let $a_1, a_2$ be two positive integers, let $\mathbb{P}^{a_1-1}$, $\mathbb{P}^{a_2-1}$ be projective spaces over the field $K$, and let $K[\mathbf{x}] = K[x_1, \ldots, x_{a_1}]$, $K[\mathbf{y}] = K[y_1, \ldots, y_{a_2}]$, $K[\mathbf{t}] = K[t_{1,1}, \ldots, t_{a_1,a_2}]$ be polynomial rings with the standard grading. If $d \in \mathbb{N}$, let $K[\mathbf{t}]_d$ denote the set of homogeneous polynomials of total degree $d$ in $K[\mathbf{t}]$, together with the zero polynomial. Thus $K[\mathbf{t}]_d$ is a $K$-linear space and $K[\mathbf{t}] = \oplus_{d=0}^{\infty} K[\mathbf{t}]_d$. In this grading each $t_{i,j}$ is homogeneous of degree one.

Given $\mathbb{X}_i \subset \mathbb{P}^{a_i-1}$, $i = 1, 2$, denote by $I(\mathbb{X}_1)$ (resp. $I(\mathbb{X}_2)$) the *vanishing ideal* of $\mathbb{X}_1$ (resp. $\mathbb{X}_2$) generated by the homogeneous polynomials of $K[\mathbf{x}]$ (resp. $K[\mathbf{y}]$) that vanish at all points of $\mathbb{X}_1$ (resp. $\mathbb{X}_2$).

The image of $\mathbb{X}_1 \times \mathbb{X}_2$ under the Segre embedding $\psi$ (see Definition 3.1.3), denoted by $\mathbb{X}$, is called the *Segre product* of $\mathbb{X}_1$ and $\mathbb{X}_2$. The vanishing ideal $I(\mathbb{X})$ of $\mathbb{X}$ is a graded ideal of $K[\mathbf{t}]$, where the $t_{i,j}$ variables are ordered as $t_{1,1}, \ldots, t_{1,a_2}, \ldots, t_{a_1,1}, \ldots, t_{a_1,a_2}$.

A *standard algebra* over an arbitrary field $K$ is a finitely generated graded $K$-algebra $A = \bigoplus_{d=0}^{\infty} A_d$ such that $A = K[A_1]$ and $A_0 = K$ (that is, $A$ is isomorphic to $K[\mathbf{x}]/I$, for some polynomial ring $K[\mathbf{x}]$ with the standard grading and for some graded ideal $I$).

**Definition 3.2.1.** [13, p. 304]} Let $A = \oplus_{d\geq 0} A_d$, $B = \oplus_{d\geq 0} B_d$ be two standard algebras over a field $K$. The *Segre product* of $A$ and $B$, denoted by $A \otimes_{\mathcal{S}} B$, is the graded algebra

$$A \otimes_{\mathcal{S}} B := (A_0 \otimes_K B_0) \oplus (A_1 \otimes_K B_1) \oplus \cdots \subset A \otimes_K B,$$

with the normalized grading $(A \otimes_{\mathcal{S}} B)_d := A_d \otimes_K B_d$ for $d \geq 0$. The tensor product algebra $A \otimes_K B$ is graded by

$$(A \otimes_K B)_p := \sum_{i+j=p} A_i \otimes_K B_j.$$

**Example 3.2.2.** [4, p. 161] The Segre product (resp. tensor product) of $K[\mathbf{x}]$ and $K[\mathbf{y}]$ is

$$K[\mathbf{x}] \otimes_{\mathcal{S}} K[\mathbf{y}] \simeq K[\{x_i y_j |\, 1 \leq i \leq a_1,\, 1 \leq j \leq a_2\}]$$

(resp. $K[\mathbf{x}] \otimes_K K[\mathbf{y}] \simeq K[\mathbf{x}, \mathbf{y}]$). Notice that the elements $x_i y_j$ have normalized degree 1 as elements of $K[\mathbf{x}] \otimes_{\mathcal{S}} K[\mathbf{y}]$ and total degree 2 as elements of $K[\mathbf{x}] \otimes_K K[\mathbf{y}]$.

The next result is well-known assuming that $\mathbb{X}_1$ and $\mathbb{X}_2$ are projective algebraic sets; see for instance [13, Excercise 13.14(d)]. However David Eisenbud pointed out to us that the result is valid in general. We give a proof of the general case.

**Theorem 3.2.3.** *Let $K$ be a field. If $\mathbb{X}_1$, $\mathbb{X}_2$ are subsets of the projective spaces $\mathbb{P}^{a_1-1}$, $\mathbb{P}^{a_2-1}$, respectively, and $\mathbb{X}$ is the Segre product of $\mathbb{X}_1$ and $\mathbb{X}_2$, then the following hold:*

(a) $(K[\mathbf{x}]/I(\mathbb{X}_1))_d \otimes_K (K[\mathbf{y}]/I(\mathbb{X}_2))_d \simeq (K[\mathbf{t}]/I(\mathbb{X}))_d$ *as $K$-vector spaces for $d \geq 0$.*

(b) $K[\mathbf{x}]/I(\mathbb{X}_1) \otimes_{\mathcal{S}} K[\mathbf{y}]/I(\mathbb{X}_2) \simeq K[\mathbf{t}]/I(\mathbb{X})$ *as standard graded algebras.*

(c) $H_{\mathbb{X}_1}(d) H_{\mathbb{X}_2}(d) = H_{\mathbb{X}}(d)$ *for $d \geq 0$.*

(d) $\operatorname{reg}(K[\mathbf{t}]/I(\mathbb{X})) = \max\{\operatorname{reg}(K[\mathbf{x}]/I(\mathbb{X}_1)), \operatorname{reg}(K[\mathbf{y}]/I(\mathbb{X}_2))\}$.

(e) *If* $\rho_1 = \dim(K[\mathbf{x}]/I(\mathbb{X}_1))$ *and* $\rho_2 = \dim(K[\mathbf{y}]/I(\mathbb{X}_2))$, *then*

$$\deg(K[\mathbf{t}]/I(\mathbb{X})) = \deg(K[\mathbf{x}]/I(\mathbb{X}_1))\deg(K[\mathbf{y}]/I(\mathbb{X}_2))\binom{\rho_1+\rho_2-2}{\rho_1-1}.$$

**Proof.** (a): Let $\sigma$ be the epimorphism of $K$-algebras

$$\sigma\colon K[\mathbf{t}] \to K[\{x_iy_j \mid i \in [\![1,a_1]\!],\ j \in [\![1,a_2]\!]\}]$$

induced by $t_{ij} \mapsto x_iy_j$, where $[\![1,a_i]\!] = \{1,\dots,a_i\}$. For each element $x^by^c$ with the property $\deg(x^b) = \deg(y^c) = d$ there is a unique $t^a \in K[\mathbf{t}]_d$ such that $t^a = t_{i_1,j_1}\cdots t_{i_d,j_d}$, $1 \leq i_1 \leq \cdots \leq i_d$, $1 \leq j_1 \leq \cdots \leq j_d$ and $\sigma(t^a) = x^by^c$. Notice that if $\sigma(t^\alpha) = x^by^c$ for some other monomial $t^\alpha \in K[\mathbf{t}]_d$, then $t^a - t^\alpha \in I(\mathbb{X})$. This is used below to ensure that the mapping of Eq. (3.2.1) is surjective. Setting $\varphi_0(x^b,y^c) = t^a$, gives a $K$-bilinear map

$$\varphi_0\colon K[\mathbf{x}]_d \times K[\mathbf{y}]_d \to K[\mathbf{t}]_d$$

induced by $\varphi_0(x^b,y^c) = t^a$. Notice that $\varphi_0(\sum \lambda_kx^{b_k}, \sum \mu_\ell y^{c_\ell}) = \sum \lambda_k\mu_\ell\varphi_0(x^{b_k},y^{c_\ell})$, where the $\lambda_k$'s and $\mu_\ell$'s are in $K$. To show that $\varphi_0$ induces a $K$-bilinear map

$$\varphi\colon (K[\mathbf{x}]_d/I(\mathbb{X}_1)_d) \times (K[\mathbf{y}]_d/I(\mathbb{X}_2)_d) \to K[\mathbf{t}]_d/I(\mathbb{X})_d,\quad (\overline{x^b},\overline{y^c}) \mapsto \overline{\varphi_0(x^b,y^c)}, \qquad (3.2.1)$$

which is a surjection, it suffices to show that for any $f \in K[\mathbf{x}]_d$ that vanish on $\mathbb{X}_1$ (resp. $g \in K[\mathbf{y}]_d$ that vanish on $\mathbb{X}_2$) one has that $\varphi_0(f,g)$ vanishes at all points of $\mathbb{X}$. Assume that $f = \lambda_1x^{b_1} + \cdots + \lambda_mx^{b_m}$ is a polynomial in $K[\mathbf{x}]_d$ that vanish on $\mathbb{X}_1$ and that $g = \mu_1y^{c_1} + \cdots + \mu_ry^{c_r}$ is a polynomial in $K[\mathbf{y}]_d$ with $\lambda_k$, $\mu_\ell$ in $K$ for all $k,\ell$. For each $x^{b_k}y^{c_\ell}$ there is $t^{a_{k\ell}} \in K[\mathbf{t}]$ such that $\sigma(t^{a_{k\ell}}) = x^{b_k}y^{c_\ell}$. Then

$$\begin{aligned}\varphi_0(f,g) &= \sum \lambda_k\mu_\ell\varphi_0(x^{b_k},y^{c_\ell}) = \sum \lambda_k\mu_\ell t^{a_{k\ell}}, \text{ and}\\ \varphi_0(f,g)(x_iy_j) &= (\lambda_1x^{b_1} + \cdots + \lambda_mx^{b_m})(\mu_1y^{c_1} + \cdots + \mu_ry^{c_r}),\end{aligned}$$

where we use $(x_iy_j)$ as a short hand for $(x_1y_1, x_1y_2, \dots, x_1y_{a_2}, \dots, x_{a_1}y_1, x_{a_1}y_2, \dots, x_{a_1}y_{a_2})$. Now if $[(\alpha_1,\dots,\alpha_{a_1})]$ is in $\mathbb{X}_1$ and $[(\beta_1,\dots,\beta_{a_2})]$ is in $\mathbb{X}_2$, making $x_i = \alpha_i$ and $y_j = \beta_j$ for all $i,j$ in the last equality, we get $\varphi_0(f,g)(\alpha_i\beta_j) = 0$. Therefore, by the universal property of the tensor product [13, p. 573], there is a surjective map $\overline{\varphi}$ that makes the following diagram commutative:

$$\begin{tikzcd}
(K[\mathbf{x}]_d/I(\mathbb{X}_1)_d) \times (K[\mathbf{y}]_d/I(\mathbb{X}_2)_d) \arrow[r, "\phi"] \arrow[d, "\varphi"] & (K[\mathbf{x}]_d/I(\mathbb{X}_1)_d) \otimes_K (K[\mathbf{y}]_d/I(\mathbb{X}_2)_d) \arrow[dl, "\overline{\varphi}"] \\
K[\mathbf{t}]_d/I(\mathbb{X})_d &
\end{tikzcd}$$

where $\phi$ is the canonical map, given by $\phi(\overline{f},\overline{g}) = \overline{f} \otimes \overline{g}$, and $\varphi = \overline{\varphi}\phi$.

For each $t^\alpha \in K[\mathbf{t}]_d$ there are unique monomials $x^b \in K[\mathbf{x}]_d$ and $y^c \in K[\mathbf{y}]_d$ such that $\sigma(t^\alpha) = x^b y^c$. We set $\sigma_1(t^\alpha) = x^b$ and $\sigma_2(t^\alpha) = y^c$. Thus we have a surjective $K$-linear map

$$\sigma_0^*\colon K[\mathbf{t}]_d \to K[\mathbf{x}]_d/I(\mathbb{X}_1)_d \otimes_K K[\mathbf{y}]_d/I(\mathbb{X}_2)_d$$

given by $\sigma_0^*(\sum \lambda_\alpha t^\alpha) = \sum \lambda_\alpha \overline{\sigma_1(t^\alpha)} \otimes \overline{\sigma_2(t^\alpha)}$, where the $\lambda_\alpha$'s are in $K$. Notice that the $K$-vector space on the right hand side is generated by all $\overline{x^b} \otimes \overline{y^c}$ such that $x^b \in K[\mathbf{x}]_d$ and $y^c \in K[\mathbf{y}]_d$. Take $f \in I(\mathbb{X})_d$, then $\sigma(f)(\alpha_i\beta_j) = 0$ for all $\alpha = [(\alpha_1, \ldots, \alpha_{a_1})] \in \mathbb{X}_1$ and all $\beta = [(\beta_1, \ldots, \beta_{a_2})] \in \mathbb{X}_2$. We can write $\sigma(f) = \sum_{\ell=1}^k f_\ell g_\ell$ with $f_\ell \in K[\mathbf{x}]_d$, $g_\ell \in K[\mathbf{y}]_d$ for $\ell = 1, \ldots, k$, and $\sigma_0^*(f) = \sum_{\ell=1}^k \overline{f_\ell} \otimes \overline{g_\ell}$. Next we show that $\sigma_0^*(f) = 0$, i.e., $f \in \ker(\sigma_0^*)$. If $k = 1$, we may assume that $f_1 \notin I(\mathbb{X}_1)$ otherwise $\overline{f_1} = \overline{0}$. Pick $\alpha \in \mathbb{X}_1$ such that $f_1(\alpha) \neq 0$. Then, as $f_1(\alpha)g_1(\beta) = 0$ for all $\beta \in \mathbb{X}_2$, one has $g_1 \in I(\mathbb{X}_2)$ and $\overline{g_1} = \overline{0}$. We may now assume that $k > 1$ and $\overline{f_k} \neq 0$. Pick $\alpha \in \mathbb{X}_1$ such that $f_k(\alpha) \neq 0$. By hypothesis the polynomial

$$f_1(\alpha)g_1 + \cdots + f_k(\alpha)g_k$$

is in $K[\mathbf{y}]_d$ and vanishes at all points of $\mathbb{X}_2$. Thus

$$\overline{g_k} = -(f_1(\alpha)/f_k(\alpha))\overline{g}_1 - \cdots - (f_{k-1}(\alpha)/f_k(\alpha))\overline{g}_{k-1}.$$

Therefore, setting $h_\ell = f_\ell - (f_\ell(\alpha)/f_k(\alpha))f_k$ for $\ell = 1, \ldots, k-1$, we get

$$\sigma_0^*(f) = \sum_{\ell=1}^{k} \overline{f_\ell} \otimes \overline{g}_\ell = \sum_{\ell=1}^{k-1} \overline{h}_\ell \otimes \overline{g}_\ell$$

and $\sum_{\ell=1}^{k-1} h_\ell(\gamma)g_\ell(\beta) = 0$ for all $\gamma \in \mathbb{X}_1$ and $\beta \in \mathbb{X}_2$. Repeating the same argument, with $h_\ell$ playing the role of $f_\ell$ and $k-1$ playing the role of $k$, as many times as necessary we conclude that $\sigma_0^*(f) = 0$. Hence $I(\mathbb{X})_d \subset \ker(\sigma_0^*)$. Therefore $\sigma_0^*$ induces a $K$-linear surjection

$$\sigma^*\colon K[\mathbf{t}]_d/I(\mathbb{X})_d \to (K[\mathbf{x}]_d/I(\mathbb{X}_1)_d) \otimes_K (K[\mathbf{y}]_d/I(\mathbb{X}_2)_d).$$

Altogether we get that the linear maps $\overline{\varphi}$ and $\sigma^*$ are bijective.

Items (b) to (e) follow directly from (a) and its proof. □

## 3.3 Projective Segre codes

In this section we study projective Segre codes and their basic parameters; including the second generalized Hamming weight. It is shown that direct product codes of projective Reed-Muller-type codes are projective Segre codes. Then some applications are given. We continue to employ the notations and definitions used in Sections 3.1 and 3.2.

In preparation for our main theorem, let $K = \mathbb{F}_q$ be a finite field, let $a_1, a_2$ be two positive integers with $a_1 \geq a_2$, and for $i = 1, 2$, let $\mathbb{X}_i$ be a non-empty subset of the projective space $\mathbb{P}^{a_i-1}$ over $K$. We set $s = a_1a_2$ and $s_i = |\mathbb{X}_i|$ for $i = 1, 2$. The *Segre embedding* is given by

$$\begin{aligned}
\psi\colon \mathbb{P}^{a_1-1} \times \mathbb{P}^{a_2-1} &\to \mathbb{P}^{a_1a_2-1} = \mathbb{P}^{s-1}\\
([\alpha_1, \ldots, \alpha_{a_1}], [\beta_1, \ldots, \beta_{a_2}]) &\to [(\alpha_1\beta_1, \alpha_1\beta_2, \ldots, \alpha_1\beta_{a_2},\\
&\qquad \alpha_2\beta_1, \alpha_2\beta_2, \ldots, \alpha_2\beta_{a_2},\\
&\qquad\qquad \vdots\\
&\qquad \alpha_{a_1}\beta_1, \alpha_{a_1}\beta_2, \ldots, \alpha_{a_1}\beta_{a_2})].
\end{aligned}$$

The image of $\mathbb{X}_1 \times \mathbb{X}_2$ under the map $\psi$, denoted by $\mathbb{X}$, is the *Segre product* of $\mathbb{X}_1$ and $\mathbb{X}_2$. As $\psi$ is injective, we get $|\mathbb{X}| = |\mathbb{X}_1||\mathbb{X}_2| = s_1s_2$. Then we can write $\mathbb{X}$, $\mathbb{X}_1$, and $\mathbb{X}_2$ as:

$$\begin{aligned}
\mathbb{X} = \{P_{1,1}, \ldots, P_{s_1,s_2}\} &= \{P_{1,1},\ P_{1,2}, \ldots,\ P_{1,s_2},\\
&\quad P_{2,1},\ P_{2,2}, \ldots,\ P_{2,s_2},\\
&\qquad\quad \vdots\\
&\quad P_{s_1,1}, P_{s_1,2}, \ldots, P_{s_1,s_2}\},
\end{aligned}$$

$\mathbb{X}_1 = \{Q_1, \ldots, Q_{s_1}\}$, and $\mathbb{X}_2 = \{R_1, \ldots, R_{s_2}\}$, respectively, where

$$Q_i = [(\alpha_{i,1}, \alpha_{i,2}, \ldots, \alpha_{i,a_1})] \ \text{ and } \ R_j = [(\beta_{j,1}, \beta_{j,2}, \ldots, \beta_{j,a_2})],$$

for $i = 1, \ldots, s_1$ and $j = 1, \ldots, s_2$. Because of the embedding $\psi$ each $P_{i,j} \in \mathbb{X}$ is of the form

$$\begin{aligned}
P_{i,j} = \psi(Q_i, R_j) &= [(\alpha_{i,1}\cdot\beta_{j,1}, \alpha_{i,1}\cdot\beta_{j,2}, \ldots, \alpha_{i,1}\cdot\beta_{j,a_2},\\
&\quad \alpha_{i,2}\cdot\beta_{j,1}, \alpha_{i,2}\cdot\beta_{j,2}, \ldots, \alpha_{i,2}\cdot\beta_{j,a_2},\\
&\qquad\quad \vdots\\
&\quad \alpha_{i,a_1}\cdot\beta_{j,1}, \alpha_{i,a_1}\cdot\beta_{j,2}, \ldots, \alpha_{i,a_1}\cdot\beta_{j,a_2})].
\end{aligned}$$

Given a positive integer $r$, we set $[\![1, r]\!] := \{1, \ldots, r\}$. For use below notice that for each $i \in [\![1, s_1]\!]$ and for each $j \in [\![1, s_2]\!]$ there are $k_i \in [\![1, a_1]\!]$ and $\ell_j \in [\![1, a_2]\!]$ such that $\alpha_{i,k_i} \neq 0$ and $\beta_{j,\ell_j} \neq 0$. In fact, choose $k_i$ to be the smallest $k \in [\![1, a_1]\!]$ such that $\alpha_{i,k} \neq 0$, and choose $\ell_j$ to be the smallest $\ell \in [\![1, a_2]\!]$ such that $\beta_{j,\ell} \neq 0$. Hence $\alpha_{i,k_i}\cdot\beta_{j,\ell_j} \neq 0$.

Setting $K[\mathbf{t}] = K[t_{1,1}, t_{1,2}\ldots, t_{1,a_1}, \ldots, t_{a_1,1}, t_{a_1,2}, \ldots, t_{a_1,a_2}]$, $s = a_1a_2$, and fixing an integer $d \geq 1$, define $f_{i,j}(t_{1,1}, \ldots, t_{a_1,a_2}) = (t_{k_i,\ell_j})^d$. Then $f_{i,j}(P_{i,j}) = (\alpha_{i,k_i}\cdot\beta_{j,\ell_j})^d \neq 0$. The evaluation map $\mathrm{ev}_d$ is defined as:

$$\begin{aligned}
\mathrm{ev}_d\colon K[\mathbf{t}]_d &\to K^{|\mathbb{X}|} = K^{s_1s_2},\\
f &\to \left(\frac{f(P_{1,1})}{f_{1,1}(P_{1,1})}, \frac{f(P_{1,2})}{f_{1,2}(P_{1,1})}, \ldots, \frac{f(P_{s_1,s_2})}{f_{s_1,s_2}(P_{s_1,s_2})}\right).
\end{aligned}$$

This is a linear map of $K$-vector spaces.

**Definition 3.3.1.** The image of $\mathrm{ev}_d$, denoted by $C_{\mathbb{X}}(d)$, defines a projective Reed-Muller-type linear code of degree $d$ that we call a *projective Segre code* of degree $d$.

For each $i \in [\![1, s_1]\!]$ and for each $j \in [\![1, s_2]\!]$, define the following polynomials:

$$g_i(x_1, \ldots, x_{a_1}) = x_{k_i}^d \in K[x_1, \ldots, x_{a_1}]_d \ \text{ and } \ h_j(y_1, \ldots, y_{a_2}) = y_{\ell_j}^d \in K[y_1, \ldots, y_{a_2}]_d.$$

Clearly $g_i(Q_i) = \alpha_{i,k_i}^d \neq 0$, $h_j(R_j) = \beta_{j,\ell_j}^d \neq 0$, $f_{i,j}(P_{i,j}) = (\alpha_{i,k_i})^d h_j(R_j) = g_i(Q_i)(\beta_{j,\ell_j})^d$. We also define the following two evaluation maps:

$$\begin{aligned}
\mathrm{ev}_d^1\colon K[x_1, \ldots, x_{a_1}]_d &\to K^{|\mathbb{X}_1|} = K^{s_1},\\
g &\to \left(\frac{g(Q_1)}{g_1(Q_1)}, \frac{g(Q_2)}{g_2(Q_2)}, \ldots, \frac{g(Q_{s_1})}{g_{s_1}(Q_{s_1})}\right), \text{ and}\\
\mathrm{ev}_d^2\colon K[y_1, \ldots, y_{a_2}]_d &\to K^{|\mathbb{X}_2|} = K^{s_2},\\
h &\to \left(\frac{h(R_1)}{h_1(R_1)}, \frac{h(R_2)}{h_2(R_2)}, \ldots, \frac{h(R_{s_2})}{h_{s_2}(R_{s_2})}\right),
\end{aligned}$$

and their corresponding Reed-Muller-type linear codes $C_{\mathbb{X}_i}(d) := \mathrm{im}(\mathrm{ev}_d^i)$ for $i = 1, 2$.

Let $C$ be a linear code. From Section 3.1 recall that $\delta_r(C)$ is the $r$th generalized Hamming weight of $C$ and that $\delta_1(C)$ is the minimum distance $\delta(C)$ of $C$. For $0 \neq v \in C$ its *Hamming weight*, denoted by $\omega(v)$, is the number of non-zero entries of $v$.

We come to the main result of this section.

**Theorem 3.3.2.** *Let $K = \mathbb{F}_q$ be a finite field, let $\mathbb{X}_i \subset \mathbb{P}^{a_i - 1}$ for $i = 1, 2$, and let $\mathbb{X}$ be the Segre product of $\mathbb{X}_1$ and $\mathbb{X}_2$. The following hold.*

(a) $|\mathbb{X}| = |\mathbb{X}_1||\mathbb{X}_2|$.

(b) $\dim_K(C_{\mathbb{X}}(d)) = \dim_K(C_{\mathbb{X}_1}(d)) \dim_K(C_{\mathbb{X}_2}(d))$ *for* $d \geq 1$.

(c) $\delta(C_{\mathbb{X}}(d)) = \delta(C_{\mathbb{X}_1}(d))\delta(C_{\mathbb{X}_2}(d))$ *for* $d \geq 1$.

(d) $C_{\mathbb{X}}(d)$ *is the direct product* $C_{\mathbb{X}_1}(d) \underline{\otimes} C_{\mathbb{X}_2}(d)$ *of* $C_{\mathbb{X}_1}(d)$ *and* $C_{\mathbb{X}_2}(d)$ *for* $d \geq 1$.

(e) $\delta_2(C_{\mathbb{X}}(d)) = \min\{\delta_1(C_{\mathbb{X}_1}(d))\delta_2(C_{\mathbb{X}_2}(d)), \delta_2(C_{\mathbb{X}_1}(d))\delta_1(C_{\mathbb{X}_2}(d))\}$ *for* $d \geq 1$.

(f) $\delta(C_{\mathbb{X}}(d)) = 1$ *for* $d \geq \max\{\mathrm{reg}(K[\mathbf{x}]/I(\mathbb{X}_1)), \mathrm{reg}(K[\mathbf{y}]/I(\mathbb{X}_2))\}$.

**Proof.** (a): This is clear because the Segre embedding is a one-to-one map.

(b): Since $K[\mathbf{x}]_d/I(\mathbb{X}_1)_d \simeq C_{\mathbb{X}_1}(d)$, $K[\mathbf{y}]_d/I(\mathbb{X}_2)_d \simeq C_{\mathbb{X}_2}(d)$, and $K[\mathbf{t}]_d/I(\mathbb{X})_d \simeq C_{\mathbb{X}}(d)$, the results follows at once from Theorem 3.2.3.

(c): We set $\delta_{\mathbb{X}}(d) = \delta(C_{\mathbb{X}}(d))$ and $\delta_{\mathbb{X}_i}(d) = \delta(C_{\mathbb{X}_i}(d))$ for $i = 1, 2$. Given $f \in K[\mathbf{t}]_d$, the entries of $\mathrm{ev}_d(f)$ can be arranged as:

$$\mathrm{ev}_d(f) \;=\; \begin{array}{ccccc} \Bigg(\dfrac{f(P_{1,1})}{f_{1,1}(P_{1,1})}, & \dfrac{f(P_{1,2})}{f_{1,2}(P_{1,2})}, & \ldots, & \dfrac{f(P_{1,s_2})}{f_{1,s_2}(P_{1,s_2})}\,, & \to \Gamma_1 \\ \dfrac{f(P_{2,1})}{f_{2,1}(P_{2,1})}, & \dfrac{f(P_{2,2})}{f_{2,2}(P_{2,2})}, & \ldots, & \dfrac{f(P_{2,s_2})}{f_{2,s_2}(P_{2,s_2})}, & \to \Gamma_2 \\ \vdots & \vdots & & \vdots & \vdots \\ \dfrac{f(P_{s_1,1})}{f_{s_1,1}(P_{s_1,1})}, & \dfrac{f(P_{s_1,2})}{f_{s_1,2}(P_{s_1,2})}, & \ldots, & \dfrac{f(P_{s_1,s_2})}{f_{s_1,s_2}(P_{s_1,s_2})}\Bigg) & \to \Gamma_{s_1} \\ \downarrow & \downarrow & & \downarrow & \\ \Lambda_1 & \Lambda_2 & \cdots & \Lambda_{s_2} & \end{array} \tag{3.3.1}$$

where $\Gamma_1, \ldots, \Gamma_{s_1}$ and $\Lambda_1, \ldots, \Lambda_{s_2}$ are row and column vectors, respectively. Thus $\mathrm{ev}_d(f)$ can be viewed as a matrix of size $s_1 \times s_2$. Below we show that $\Gamma_i \in C_{\mathbb{X}_2}(d)$ and $\Lambda_j^\top \in C_{\mathbb{X}_1}(d)$ for all $i, j$. Define the following polynomials

$$\begin{aligned} h_{Q_i} \;=\; & f(\alpha_{i,1} \cdot y_1, \alpha_{i,1} \cdot y_2, \ldots, \alpha_{i,1} \cdot y_{a_2}, \\ & \alpha_{i,2} \cdot y_1, \alpha_{i,2} \cdot y_2, \ldots, \alpha_{i,2} \cdot y_{a_2}, \\ & \qquad\qquad \vdots \\ & \alpha_{i,a_1} \cdot y_1, \alpha_{i,a_1} \cdot y_2, \ldots, \alpha_{i,a_1} \cdot y_{a_2}) \in K[y_1, \ldots, y_{a_2}]_d, \text{ and} \end{aligned}$$

$$\begin{aligned} g_{R_j} \;=\; & f(x_1 \cdot \beta_{j,1}, x_1 \cdot \beta_{j,2}, \ldots, x_1 \cdot \beta_{j,a_2}, \\ & x_2 \cdot \beta_{j,1}, x_2 \cdot \beta_{j,2}, \ldots, x_2 \cdot \beta_{j,a_2}, \\ & \qquad\qquad \vdots \\ & x_{a_1} \cdot \beta_{j,1}, x_{a_1} \cdot \beta_{j,2}, \ldots, x_{a_1} \cdot \beta_{j,a_2}) \in K[x_1, \ldots, x_{a_1}]_d. \end{aligned}$$

Observe that $f(P_{ij}) = h_{Q_i}(R_j) = g_{R_j}(Q_i)$.

First we show the inequality $\delta_{\mathbb{X}}(d) \geq \delta_{\mathbb{X}_1}(d)\delta_{\mathbb{X}_2}(d)$. Let $f \in K[\mathbf{t}]_d$ such that $\mathrm{ev}_d(f) \neq 0$. We want to prove that $\omega(\mathrm{ev}_d(f))$, the Hamming weight of $\mathrm{ev}_d(f)$, satisfies

$$\omega(\mathrm{ev}_d(f)) \geq \delta_{\mathbb{X}_1}(d)\delta_{\mathbb{X}_2}(d).$$

For simplicity, we set $\tau_f = \mathrm{ev}_d(f)$ and denote the Hamming weight of $\Gamma_i$ by $\omega(\Gamma_i)$. One has

$$\omega(\tau_f) = \omega(\Gamma_1) + \omega(\Gamma_2) + \cdots + \omega(\Gamma_{s_1}).$$

Notice that

$$\begin{aligned}\Gamma_i &= \left(\frac{f(P_{i1})}{f_{i1}(P_{i1})}, \frac{f(P_{i2})}{f_{i2}(P_{i2})}, \ldots, \frac{f(P_{is_2})}{f_{is_2}(P_{is_2})}\right) = \\ &\quad \left(\frac{h_{Q_i}(R_1)}{\alpha_{i,k_i}^d \cdot h_1(R_1)}, \frac{h_{Q_i}(R_2)}{\alpha_{i,k_i}^d \cdot h_2(R_2)}, \ldots, \frac{h_{Q_i}(R_{s_2})}{\alpha_{i,k_i}^d \cdot h_{s_2}(R_{s_2})}\right) = \frac{1}{(\alpha_{i,k_i})^d} \cdot \mathrm{ev}_d^2(h_{Q_i}), \text{ and} \\ \Lambda_j^\top &= \frac{1}{(\beta_{j,\ell_j})^d} \cdot \mathrm{ev}_d^1(g_{R_j}),\end{aligned}$$

for $i = 1, \ldots, s_1$ and $j = 1, \ldots, s_2$. Therefore $\omega(\Gamma_1)$, the number of non-zero entries of $\Gamma_1$, is the same as the number of non-zero entries of $\mathrm{ev}_d^2(h_{Q_1})$, and if $\Gamma_1 \neq 0$, then $\mathrm{ev}_d^2(h_{Q_1}) \neq 0$ and $\omega(\Gamma_1) \geq \delta_{\mathbb{X}_2}(d)$. Similarly, for any $i \in [\![1, s_1]\!]$ such that $\Gamma_i \neq 0$, $\omega(\Gamma_i) \geq \delta_{\mathbb{X}_2}(d)$. Setting $b = |\{i|\, \Gamma_i \neq 0\}|$, we get that

$$\omega(\tau_f) \geq b \cdot \delta_{\mathbb{X}_2}(d).$$

Now we want to prove that $b \geq \delta_{\mathbb{X}_1}(d)$. Suppose $b < \delta_{\mathbb{X}_1}(d)$. Choose $j \in [\![1, s_2]\!]$ such that $\Lambda_j \neq 0$. If $\omega(\Lambda_j)$ is the number of non-zero entries of $\Lambda_j$, we have $\omega(\Lambda_j) \leq b < \delta_{\mathbb{X}_1}(d)$ and $\omega(\Lambda_j)$ is equal to the number of non-zero entries of $\mathrm{ev}_d^1(g_{R_j})$. As $\mathrm{ev}_d^1(g_{R_j})$ is in $C_{\mathbb{X}_1}(d)$, we conclude that $\omega(\Lambda_j) \geq \delta_{\mathbb{X}_1}(d)$, a contradiction. Thus $b \geq \delta_{\mathbb{X}_1}(d)$ and

$$\omega(\mathrm{ev}_d(f)) \geq \delta_{\mathbb{X}_1}(d)\delta_{\mathbb{X}_2}(d).$$

As this holds for any $f \in K[\mathbf{t}]_d$ such that $\mathrm{ev}_d(f) \neq 0$, we obtain $\delta_{\mathbb{X}}(d) \geq \delta_{\mathbb{X}_1}(d)\delta_{\mathbb{X}_2}(d)$.

Next we prove that $\delta_{\mathbb{X}}(d) \leq \delta_{\mathbb{X}_1}(d)\delta_{\mathbb{X}_2}(d)$. It suffices to find a word in $C_{\mathbb{X}}(d)$ with Hamming weight equal to $\delta_{\mathbb{X}_1}(d)\delta_{\mathbb{X}_2}(d)$. Let $\overline{g} \in K[x_1, \ldots, x_{a_1}]_d$ be such that $\mathrm{ev}_d^1(\overline{g})$ is not zero and $\omega(\mathrm{ev}_d^1(\overline{g})) = \delta_{\mathbb{X}_1}(d)$ and let $\overline{h} \in K[y_1, \ldots, y_{a_2}]_d$ be such that $\mathrm{ev}_d^1(\overline{h}) \neq 0$ and $\omega(\mathrm{ev}_d^2(\overline{h})) = \delta_{\mathbb{X}_2}(d)$. Let $\delta_i = \delta_{\mathbb{X}_i}(d)$ for $i = 1, 2$. There are $Q_{i_1}, \ldots, Q_{i_{\delta_1}} \in \mathbb{X}_1$ such that

$$\overline{g}(Q_{i_1}) \neq 0, \ldots, \overline{g}(Q_{i_{\delta_1}}) \neq 0 \;\text{ and }\; \overline{g}(Q_i) = 0 \;\text{ for }\; Q_i \in \mathbb{X}_1 \setminus \{Q_{i_1}, \ldots, Q_{i_{\delta_1}}\},$$

and there are $R_{j_1}, \ldots, R_{j_{\delta_2}} \in \mathbb{X}_2$ such that

$$\overline{h}(R_{j_1}) \neq 0, \ldots, \overline{h}(R_{i_{\delta_2}}) \neq 0 \;\text{ and }\; \overline{h}(R_j) = 0 \;\text{ for }\; R_j \in \mathbb{X}_2 \setminus \{R_{j_1}, \ldots, R_{j_{\delta_2}}\}.$$

Notice that $\overline{g}$ (resp. $\overline{h}$) is a sum of monomials of degree $d$ in the variables $x_1, \ldots, x_{a_1}$ (resp. $y_1, \ldots, y_{a_2}$). Each monomial is a product of $d$ variables; the variables could be repeated. Therefore, $\overline{g}\cdot\overline{h} = \overline{g}(x_1, \ldots, x_{a_1})\cdot\overline{h}(y_1, \ldots, y_{a_2})$ is a sum of monomials, each one of these monomials is a product of $2d$ variables, $d$ variables among $x_1, \ldots, x_{a_1}$ and $d$ variables among $y_1, \ldots, y_{a_2}$; and again, variables could be repeated. Let $x_{\theta_1} \cdots x_{\theta_d} y_{\gamma_1} \cdots y_{\gamma_d}$ be a monomial of $\overline{g}\overline{h}$ with $\theta_1, \ldots, \theta_d \in [\![1, a_1]\!]$, $\gamma_1, \ldots, \gamma_d \in [\![1, a_2]\!]$. We can write

$$x_{\theta_1} \cdots x_{\theta_d} y_{\gamma_1} \cdots y_{\gamma_d} = (x_{\theta_1} y_{\gamma_1}) \cdots (x_{\theta_d} y_{\gamma_d}),$$

this is one possible way to match these $d$ $x$'s and these $d$ $y$'s in pairs; there are many other ways to do it. If, for each monomial of $\overline{g} \cdot \overline{h}$, we choose a way to match the $d$ $x$'s and the $d$ $y$'s in pairs, then we can see $\overline{g}\cdot\overline{h}$ as a polynomials in $(x_ky_\ell)$, $k\in[\![1,a_1]\!]$, $\ell\in[\![1,a_2]\!]$. Now, if in $\overline{g}\cdot\overline{h}$ we substitute $x_ky_\ell$ by the variable $t_{k,\ell}$, we obtain a polynomial

$$\overline{f}(t_{1,1},\ldots,t_{a_1,a_2})\in K[\mathbf{t}]_d=K[t_{1,1},\ldots,t_{a_1,a_2}]_d$$

such that $\overline{f}(P_{i,j})=\overline{g}(Q_i)\cdot\overline{h}(R_j)$, where $P_{i,j}=\psi(Q_i,R_j)$ for $i=1,\ldots,s_1$ and $j=1,\ldots,s_2$. Hence $\overline{f}(P_{i,j})\neq 0$ if and only if $\overline{g}(Q_i)\neq 0$ and $\overline{h}(R_j)\neq 0$. As a result $\mathrm{ev}_d(\overline{f})\neq 0$, and $\omega(\mathrm{ev}_d(\overline{f}))=\delta_1\delta_2=\delta_{\mathbb{X}_1}(d)\delta_{\mathbb{X}_2}(d)$. Hence $\delta_{\mathbb{X}}(d)\leq\delta_{\mathbb{X}_1}(d)\delta_{\mathbb{X}_2}(d)$.

(d): By part (b) and Theorem 3.1.1 the linear codes $C_{\mathbb{X}}(d)$ and $C_{\mathbb{X}_1}(d)\underline{\otimes}C_{\mathbb{X}_2}(d)$ have the same dimension. Using Eq. (3.3.1) it follows that $C_{\mathbb{X}}(d)$ can be regarded as a linear subspace of $C_{\mathbb{X}_1}(d)\underline{\otimes}C_{\mathbb{X}_2}(d)$. Hence these linear spaces must be equal.

(e): It follows at once from Theorem 3.1.2 and part (d).

(f): This follows from part (c), Proposition 1.5.3(iii), and Theorem 3.2.3(d). □

**Remark 3.3.3.** This result tells us that the direct product of projective Reed-Muller-type codes is again a projective Reed-Muller-type code.

**Definition 3.3.4.** If $K^*=K\setminus\{0\}$ and $\mathbb{X}_i$ is the image of $(\mathbb{K}^*)^{a_i}$, under the map $(K^*)^{a_i}\to\mathbb{P}^{a_i-1}$, $x\to[x]$, we call $\mathbb{X}_i$ a *projective torus* in $\mathbb{P}^{a_i-1}$.

Our main theorem gives a wide generalization of most of the main results of [24, 25, 26, 29].

**Remark 3.3.5.** If $\mathbb{X}_1=\mathbb{P}^{a_1-1}$ and $\mathbb{X}_2=\mathbb{P}^{a_2-1}$, using Theorem 3.3.2 we recover the formula for the minimum distance of $C_{\mathbb{X}}(d)$ given in [29, Theorem 5.1], and if $\mathbb{X}_i$ is a projective torus for $i=1,2$, using Theorem 3.3.2 we recover the formula for the minimum distance of $C_{\mathbb{X}}(d)$ given in [24, Theorem 5.5]. In these two cases formulas for the basic parameters of $C_{\mathbb{X}_i}(d)$, $i=1,2$, are given in [59, Theorem 1] and [55, Theorem 3.5], respectively. We also recover the formulas for the second generalized Hamming weight of some evaluation codes arising from complete bipartite graphs given in [25, Theorem 5.1] and [26, Theorem 3] (see Corollary 3.3.6).

It turns out that the formula given in Theorem 3.3.2(d) is a far reaching generalization of the following result.

**Corollary 3.3.6.** [25, Theorem 5.1] *Let $\mathbb{X}$ be the Segre product of two projective torus $\mathbb{X}_1$ and $\mathbb{X}_2$. Then the second generalized Hamming weight of $C_{\mathbb{X}}(d)$ is given by*

$$\delta_2(C_{\mathbb{X}}(d))=\min\{\delta_1(C_{\mathbb{X}_1}(d))\delta_2(C_{\mathbb{X}_2}(d)),\delta_2(C_{\mathbb{X}_1}(d))\delta_1(C_{\mathbb{X}_2}(d))\}.$$

**Remark 3.3.7.** The knowledge of the regularity of $K[\mathbf{t}]/I(\mathbb{X})$ is important for applications to coding theory: for $d\geq\mathrm{reg}(K[\mathbf{t}]/I(\mathbb{X}))$ the projective Segre code $C_{\mathbb{X}}(d)$ has minimum distance equal to 1 by Theorem 3.3.2(f). Thus, potentially good projective Segre codes $C_{\mathbb{X}}(d)$ can occur only if $1\leq d<\mathrm{reg}(K[\mathbf{t}]/I(\mathbb{X}))$.

**Definition 3.3.8.** If $\mathbb{X}$ is parameterized by monomials $z^{v_1}, \ldots, z^{v_s}$, we say that $C_{\mathbb{X}}(d)$ is a *parameterized projective code* of degree $d$.

**Corollary 3.3.9.** *If $C_{\mathbb{X}_i}(d)$ is a parameterized projective code of degree $d$ for $i = 1, 2$, then so is the corresponding projective Segre code $C_{\mathbb{X}}(d)$.*

**Proof.** It suffices to observe that if $\mathbb{X}_1$ and $\mathbb{X}_2$ are parameterized by $z^{v_1}, \ldots z^{v_s}$ and $w^{u_1}, \ldots w^{u_r}$, respectively, then $\mathbb{X}$ is parameterized by $z^{v_i}w^{u_j}$, $i = 1, \ldots, s$, $j = 1, \ldots, r$. $\square$

# Chapter 4

# Vanishing ideals generated by binomials

In this chapter we characterize, in algebraic and geometric terms, when a graded vanishing ideal is generated by binomials over any field $K$. Then we show some applications.

## 4.1 Monoids in affine and projective spaces

Let $(\mathcal{S}, \cdot, 1)$ be a monoid and let $K$ be a field. As usual we define a *character* $\chi$ of $\mathcal{S}$ in $K$ (or a $K$-*character* of $\mathcal{S}$) to be a homomorphism of $\mathcal{S}$ into the multiplicative monoid $(K, \cdot, 1)$. Thus $\chi$ is a map of $\mathcal{S}$ into $K$ such that $\chi(1) = 1$ and $\chi(\alpha\beta) = \chi(\alpha)\chi(\beta)$ for all $\alpha, \beta$ in $\mathcal{S}$.

**Theorem 4.1.1.** (Dedekind's Theorem [37, p. 291]) *If $\chi_1, \ldots, \chi_m$ are distinct characters of a monoid $\mathcal{S}$ into a field $K$, then the only elements $\lambda_1, \ldots, \lambda_m$ in $K$ such that*

$$\lambda_1\chi_1(\alpha) + \cdots + \lambda_m\chi_m(\alpha) = 0$$

*for all $\alpha \in \mathcal{S}$ are $\lambda_1 = \cdots = \lambda_m = 0$.*

Let $\mathbb{P}^{s-1}$ be a projective space over $K$. The set $\mathcal{S} = \mathbb{P}^{s-1} \cup \{[0]\}$ is a monoid under componentwise multiplication, i.e., given $[\alpha] = [(\alpha_1, \ldots, \alpha_s)]$ and $[\beta] = [(\beta_1, \ldots, \beta_s)]$ in $\mathcal{S}$, the product operation is given by

$$[\alpha] \cdot [\beta] = [\alpha \cdot \beta] = [(\alpha_1\beta_1, \ldots, \alpha_s\beta_s)],$$

where $[\mathbf{1}] = [(1, \ldots, 1)]$ is the identity element. Accordingly the affine space $\mathbb{A}^s$ is also a monoid under componentwise multiplication.

Let $S = K[t_1, \ldots, t_s]$ be a polynomial ring over a field $K$ with the standard grading induced by setting $\deg(t_i) = 1$ for all $i$. Given a set $\mathbb{Y} \subset \mathbb{P}^{s-1}$, recall that the *vanishing ideal* of $\mathbb{Y}$ is the graded ideal generated by the homogeneous polynomials in $S$ that vanish at all points of $\mathbb{Y}$.

**Lemma 4.1.2.** *Let $\mathbb{Y}$ and $Y$ be finite subsets of $\mathbb{P}^{s-1}$ and $\mathbb{A}^s$ respectively, let $P$ and $[P]$ be points in $\mathbb{Y}$ and $Y$, respectively, with $P = (\alpha_1, \ldots, \alpha_s)$, and let $I_{[P]}$ and $I_P$ be the vanishing ideal of $[P]$ and $P$, respectively. Then*

$$I_{[P]} = (\{\alpha_k t_i - \alpha_i t_k | \, k \neq i \in \{1, \ldots, s\}\}), \;\; I_P = (t_1 - \alpha_1, \ldots, t_s - \alpha_s), \qquad (4.1.1)$$

*where $\alpha_k \neq 0$ for some $k$. Furthermore $I(\mathbb{Y}) = \bigcap_{[Q]\in\mathbb{Y}} I_{[Q]}$, $I(Y) = \bigcap_{Q\in Y} I_Q$, $I_{[P]}$ is a prime ideal of height $s-1$ and $I_P$ is a prime ideal of height $s$.*

## 4.2 Binomial vanishing ideals

We continue to employ the notations and definitions used in Section 4.1. In this part we classify vanishing ideals generated by binomials.

**Theorem 4.2.1.** *If $\mathbb{Y}$ is a subset of $\mathbb{P}^{s-1}$ and $\mathbb{Y} \cup \{[0]\}$ is a submonoid of $\mathbb{P}^{s-1} \cup \{[0]\}$ under componentwise multiplication, then $I(\mathbb{Y})$ is a binomial ideal.*

**Proof.** The set $\mathcal{S} = \{x \in \mathbb{A}^s \,|\, [x] \in \mathbb{Y} \cup \{[0]\}\}$ is a submonoid of $\mathbb{A}^s$. Take a homogeneous polynomial $0 \neq f = \lambda_1 t^{a_1} + \cdots + \lambda_m t^{a_m}$ that vanishes at all points of $\mathbb{Y}$, where $\lambda_i \in K \setminus \{0\}$ for all $i$ and $a_1, \ldots, a_m$ are distinct non-zero vectors in $\mathbb{N}^s$. We set $a_i = (a_{i_1}, \ldots, a_{is})$ for all $i$. For each $i$ consider the $K$-character of $\mathcal{S}$ given by

$$\chi_i \colon \mathcal{S} \to K, \quad (\alpha_1, \ldots, \alpha_s) \mapsto \alpha_1^{a_{i1}} \cdots \alpha_s^{a_{is}}.$$

As $f \in I(\mathbb{Y})$, one has that $\lambda_1\chi_1 + \cdots + \lambda_m\chi_m = 0$. Hence, by Theorem 4.1.1, we get that $m \geqslant 2$ and $\chi_i = \chi_j$ for some $i \neq j$. Thus $t^{a_i} - t^{a_j}$ is in $I(\mathbb{Y})$. For simplicity of notation we assume that $i = 1$ and $j = 2$. Since $[\mathbf{1}] \in \mathbb{Y}$, we get that $\lambda_1 + \cdots + \lambda_m = 0$. Thus

$$f = \lambda_2(t^{a_2} - t^{a_1}) + \cdots + \lambda_m(t^{a_m} - t^{a_1}).$$

Since $f - \lambda_2(t^{a_2} - t^{a_1})$ is a homogeneous polynomial in $I(\mathbb{Y})$, by induction on $m$, we obtain that $f$ is a sum of homogeneous binomials in $I(\mathbb{Y})$. □

This result can be restated as:

**Theorem 4.2.2.** *Let $\mathbb{Y}$ be a subset of $\mathbb{P}^{s-1}$ such that $[\mathbf{1}] \in \mathbb{Y}$ and $[\alpha] \cdot [\beta] \in \mathbb{Y}$ for all $[\alpha]$, $[\beta]$ in $\mathbb{Y}$ with $\alpha \cdot \beta \neq 0$. Then $I(\mathbb{Y})$ is a binomial ideal.*

**Remark 4.2.3.** If $Y$ is a submonoid of $\mathbb{A}^s$, then $I(Y)$ is a binomial ideal. This follows by adapting the proof of Theorem 4.2.1

**Theorem 4.2.4.** *Let $K$ be a field and let $\mathbb{Y}$ be a subset of $\mathbb{P}^{s-1}$. Then $I(\mathbb{Y})$ is a binomial ideal if and only if $V(I(\mathbb{Y})) \cup \{[0]\}$ is a monoid under componentwise multiplication.*

**Proof.** $\Rightarrow$) Consider an arbitrary non-zero binomial $f = t^a - t^b$ in $I(\mathbb{Y})$ with $a = (a_i)$ and $b = (b_i)$ in $\mathbb{N}^s$. As $I(\mathbb{Y})$ is graded, $f$ is homogeneous. First notice that $[\mathbf{1}] \in V(I(\mathbb{Y}))$ because $f$ vanishes at $[\mathbf{1}]$. Take $[\alpha]$, $[\beta]$ in $V(I(\mathbb{Y}))$ with $\alpha = (\alpha_i)$, $\beta = (\beta_i)$. Then

$$\alpha_1^{a_1} \cdots \alpha_s^{a_s} = \alpha_1^{b_1} \cdots \alpha_s^{b_s} \text{ and } \beta_1^{a_1} \cdots \beta_s^{a_s} = \beta_1^{b_1} \cdots \beta_s^{b_s},$$

and consequently we have $(\alpha_1\beta_1)^{a_1} \cdots (\alpha_s\beta_s)^{a_s} = (\alpha_1\beta_1)^{b_1} \cdots (\alpha_s\beta_s)^{b_s}$, i.e., $f$ vanishes at $[\alpha] \cdot [\beta] = [\alpha \cdot \beta]$ if $\alpha \cdot \beta \neq 0$. Thus $[\alpha] \cdot [\beta] \in V(I(\mathbb{Y})) \cup \{[0]\}$.

$\Leftarrow$) Thanks to Theorem 4.2.1 one has that $I(V(I(\mathbb{Y})))$ is a binomial ideal. Recall that $V(I(\mathbb{Y}))$ is equal to $\overline{\mathbb{Y}}$ (see Lemma 1.4.15). On the other hand, by Lemma 2.2.16, $I(\mathbb{Y}) = I(\overline{\mathbb{Y}})$. Thus $I(\mathbb{Y})$ is a binomial ideal. □

**Corollary 4.2.5.** *If $\mathbb{Y}$ is a subset of $\mathbb{P}^{s-1}$ which is closed in the Zariski topology, then $I(\mathbb{Y})$ is a binomial ideal if and only if $\mathbb{Y} \cup \{[0]\}$ is a submonoid of $\mathbb{P}^{s-1} \cup \{[0]\}$.*

**Proof.** Thanks to Theorem 4.2.4 it suffices to recall that $V(I(\mathbb{Y}))$ is equal to $\overline{\mathbb{Y}}$ (see Lemma 1.4.15). □

**Corollary 4.2.6.** *If $\mathbb{Y}$ is a subset of $\mathbb{P}^{s-1}$ and $\dim(S/I(\mathbb{Y})) = 1$, then $I(\mathbb{Y})$ is a binomial ideal if and only if $\mathbb{Y} \cup \{[0]\}$ is a submonoid of $\mathbb{P}^{s-1} \cup \{[0]\}$.*

**Proof.** This is a direct consequence of Lemma 1.4.19 and Corollary 4.2.5. □

**Definition 4.2.7.** The set $T = \{[(x_1, \ldots, x_s)] \in \mathbb{P}^{s-1} | \, x_i \in K^* \text{ for all } i\}$ 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 $K^* = K \setminus \{0\}$.

A binomial ideal $I \subset S$ with the property that $t_i$ is not a zero-divisor of $S/I$ for all $i$ is called a *lattice ideal*.

If $Y$ is a submonoid of an affine torus $T^*$, then $I(Y)$ is a non-graded lattice ideal (see [16, Proposition 2.3]). The following corollary is the graded version of this result.

**Corollary 4.2.8.** *If $\mathbb{Y}$ is a submonoid of a projective torus $T$, then $I(\mathbb{Y})$ is a lattice ideal.*

**Proof.** By Theorem 4.2.1, $I(\mathbb{Y})$ is a binomial ideal. Thus it suffices to show that $t_i$ is not a zero-divisor of $S/I(\mathbb{Y})$ for all $i$. If $f \in S$ and $t_i f$ vanishes at all points of $\mathbb{Y}$, then so does $f$, as required. □

**Corollary 4.2.9.** [49, Proposition 6.7(a)] *If $\mathbb{Y} \subset \mathbb{P}^{s-1}$ and $\dim(S/I(\mathbb{Y})) = 1$, then the following are equivalent:*

(a) *$I(\mathbb{Y})$ is a lattice ideal.*

(b) *$\mathbb{Y}$ is a finite subgroup of a projective torus $T$.*

**Proof.** (a) $\Rightarrow$ (b): By Lemma 1.4.19 the set $\mathbb{Y}$ is finite. Using Corollary 4.2.6 and Lemma 4.1.2 it follows that $\mathbb{Y}$ is a submonoid of $T$. As the cancellation laws hold in $T$ and $\mathbb{Y}$ is finite, we get that $\mathbb{Y}$ is a group.

(b) $\Rightarrow$ (a): This is a direct consequence of Corollary 4.2.8. □

**Proposition 4.2.10.** *Let $K$ be an algebraically closed field. If $\mathbb{Y} \subset \mathbb{P}^{s-1}$, then the following are equivalent*:

(a) $\mathbb{Y}$ *is a finite subgroup of a projective torus $T$.*

(b) *There is a finite subgroup $H$ of $K^*$ and $v_1, \ldots, v_s \in \mathbb{Z}^n$ such that*

$$\mathbb{Y} = \{[(x^{v_1}, \ldots, x^{v_s})] \,|\, x = (x_1, \ldots, x_n) \textit{and } x_i \in H \textit{ for all } i\} \subset \mathbb{P}^{s-1}.$$

**Proof.** (b) $\Rightarrow$ (a): It is not hard to verify that $\mathbb{Y}$ is a subgroup of $T$ using the parameterization of $\mathbb{Y}$ relative to $H$.

(a) $\Rightarrow$ (b): By the fundamental theorem of finitely generated abelian groups, $\mathbb{Y}$ is a direct product of cyclic groups. Hence, there are $[\alpha_1], \ldots, [\alpha_n]$ in $\mathbb{Y}$ such that

$$\mathbb{Y} = \left\{ [\alpha_1]^{i_1} \cdots [\alpha_n]^{i_n} \,\middle|\, i_1, \ldots, i_n \in \mathbb{Z} \right\}.$$

We set $\alpha_i = (\alpha_{i1}, \ldots, \alpha_{is})$ for $i = 1, \ldots, n$. As $[\alpha_1], \ldots, [\alpha_n]$ have finite order, for each $1 \leq i \leq n$ there is $m_i = \mathrm{o}([\alpha_i])$ such that $[\alpha_i]^{m_i} = [\mathbf{1}]$. Thus

$$(\alpha_{i1}^{m_i}, \ldots, \alpha_{is}^{m_i}) = (\lambda_i, \ldots, \lambda_i)$$

for some $\lambda_i \in K^*$. Pick $\mu_i \in K^*$ such that $\mu_i^{m_i} = \lambda_i$. Setting, $\beta_{ij} = \alpha_{ij}/\mu_i$, one has $\beta_{ij}^{m_i} = 1$ for all $i, j$, that is all $\beta_{ij}$'s are in $K^*$ and have finite order. Consider the subgroup $H$ of $K^*$ generated by all $\beta_{ij}$'s. This group is cyclic because $K$ is a field. If $\beta$ is a generator of $(H, \cdot)$, we can write $\alpha_{ij}/\mu_i = \beta^{v_{ji}}$ for some $v_{ji}$ in $\mathbb{N}$. Hence

$$[\alpha_1] = [(\beta^{v_{11}}, \ldots, \beta^{v_{s1}})], \ldots, [\alpha_n] = [(\beta^{v_{1n}}, \ldots, \beta^{v_{sn}})].$$

We set $v_i = (v_{i1}, \ldots, v_{in})$ for $i = 1, \ldots, s$. Let $\mathbb{Y}_H$ be the set in $\mathbb{P}^{s-1}$ parameterized by the monomials $y^{v_1}, \ldots, y^{v_s}$ relative to $H$. If $[\gamma] \in \mathbb{Y}$, then we can write

$$[\gamma] = [\alpha_1]^{i_1} \cdots [\alpha_n]^{i_n} = [((\beta^{i_1})^{v_{11}} \cdots (\beta^{i_n})^{v_{1n}}, \ldots, (\beta^{i_1})^{v_{s1}} \cdots (\beta^{i_n})^{v_{sn}})]$$

for some $i_1, \ldots, i_n \in \mathbb{Z}$. Thus $[\gamma] \in \mathbb{Y}_H$. Conversely if $[\gamma] \in \mathbb{Y}_H$, then $[\gamma] = [(x^{v_1}, \ldots, x^{v_s})]$ for some $x_1, \ldots, x_n$ in $H$. Since any $x_k$ is of the form $\beta^{i_k}$ for some integer $i_k$, one can write $[\gamma] = [\alpha_1]^{i_1} \cdots [\alpha_n]^{i_n}$, that is, $[\gamma] \in \mathbb{Y}$. □

**Remark 4.2.11.** The equivalence between (a) and (b) was shown in [49, Proposition 6.7(b)] under the assumption that $K$ is a finite field.

If $I$ is a binomial ideal of $S$, then its saturation $(I\colon (t_1 \cdots t_s)^\infty)$ is binomial ideal. The converse is not true in general as the next example shows.

**Example 4.2.12.** Let $K$ be any field and let $\mathbb{Y} = \{[(1,1,1)], [(1,1,0)], [(1,0,1)]\}$. By Corollary 4.2.5 the vanishing ideal $I(\mathbb{Y})$ is not a binomial ideal because $\mathbb{Y} \cup \{[0]\}$ is not a monoid. The vanishing ideal $I(Y)$ of $Y = \mathbb{Y} \cap T = \{[(1,1,1)]\}$ is a lattice ideal and $(I(\mathbb{Y})\colon (t_1 \cdots t_s)^\infty) = I(Y)$.

**Proposition 4.2.13.** *Let $K$ be an algebraically closed field of characteristic zero and let $I$ be a graded ideal of $S$ of dimension* 1*. Then $I$ is a lattice ideal if and only if $I$ is the vanishing ideal of a finite subgroup $\mathbb{Y}$ of a projective torus $T$.*

**Proof.** $\Rightarrow$) Assume that $I = I(\mathcal{L})$ is the lattice ideal of a lattice $\mathcal{L}$ in $\mathbb{Z}^s$. Since $I$ is graded and $\dim(S/I) = 1$, for each $i \geq 2$, there is $a_i \in \mathbb{N}_+$ such that $f_i := t_i^{a_i} - t_1^{a_i} \in I$. This polynomial has a factorization into linear factors of the form $t_i - \mu t_1$ with $\mu \in K^*$. In characteristic zero a lattice ideal is radical [70, Theorem 8.2.27]. Therefore $I$ is the intersection of its minimal primes and each minimal prime is generated by $s-1$ linear polynomials of the form $t_i - \mu t_1$. It follows that $I$ is the vanishing ideal of some finite subset $\mathbb{Y}$ of a projective torus $T$. By Corollary 4.2.5, $\mathbb{Y}$ is a submonoid of $T$. As the cancellation laws hold in $T$ and $\mathbb{Y}$ is finite, we get that $\mathbb{Y}$ is a group.

$\Leftarrow$) This implication follows at once from Corollary 4.2.8. $\square$

# Chapter 5

# Complete intersection vanishing ideals on sets of clutter type

In this chapter we give a classification of complete intersection vanishing ideals on parameterized sets of clutter type over finite fields.

## 5.1 Vanishing ideals of clutter type

Let $R = K[\mathbf{y}] = K[y_1, \ldots, y_n]$ be a polynomial ring over a finite field $K = \mathbb{F}_q$ and let $y^{v_1}, \ldots, y^{v_s}$ be a finite set of monomials in $K[\mathbf{y}]$. As usual we denote the affine and projective spaces over the field $K$ of dimensions $s$ and $s-1$ by $\mathbb{A}^s$ and $\mathbb{P}^{s-1}$, respectively. Points of the projective space $\mathbb{P}^{s-1}$ are denoted by $[\alpha]$, where $0 \neq \alpha \in \mathbb{A}^s$.

We consider a set $\mathbb{X}$, in the projective space $\mathbb{P}^{s-1}$, parameterized by $y^{v_1}, \ldots, y^{v_s}$. The set $\mathbb{X}$ consists of all points $[(x^{v_1}, \ldots, x^{v_s})]$ in $\mathbb{P}^{s-1}$ that are well defined, i.e., $x \in K^n$ and $x^{v_i} \neq 0$ for some $i$. The set $\mathbb{X}$ is called of *clutter type* if $\operatorname{supp}(y^{v_i}) \not\subset \operatorname{supp}(y^{v_j})$ for $i \neq j$, where $\operatorname{supp}(y^{v_i})$ is the *support* of the monomial $y^{v_i}$ consisting of the variables that occur in $y^{v_i}$. In this case we say that the set of monomials $y^{v_1}, \ldots, y^{v_s}$ is of *clutter type*. This terminology comes from the fact that the condition $\operatorname{supp}(y^{v_i}) \not\subset \operatorname{supp}(y^{v_j})$ for $i \neq j$ means that there is a *clutter* $\mathcal{C}$, in the sense of [55], with vertex set $V(\mathcal{C}) = \{y_1, \ldots, y_n\}$ and edge set

$$E(\mathcal{C}) = \{\operatorname{supp}(y^{v_1}), \ldots, \operatorname{supp}(y^{v_s})\}.$$

A clutter is also called a *simple hypergraph*, see Definition 5.2.7.

Let $S = K[t_1, \ldots, t_s] = \oplus_{d=0}^{\infty} S_d$ be a polynomial ring over the field $K$ with the standard grading. The graded ideal $I(\mathbb{X})$ generated by the homogeneous polynomials of $S$ that vanish at all points of $\mathbb{X}$ is called the *vanishing ideal* of $\mathbb{X}$.

There are good reasons to study vanishing ideals over finite fields. They are used in algebraic coding theory [29] and in polynomial interpolation problems [19, 63]. The Reed-Muller-type codes arising from vanishing ideals on monomial parameterizations have received a lot of attention [7, 10, 21, 29, 43, 52, 55, 59].

The vanishing ideal $I(\mathbb{X})$ is a *complete intersection* if $I(\mathbb{X})$ is generated by $s-1$ homogeneous polynomials. Notice that $s-1$ is the height of $I(\mathbb{X})$ in the sense of [47]. The interest in complete intersection vanishing ideals over finite fields comes from information and communication theory, and algebraic coding theory [12, 23, 33].

Let $T$ be a projective torus in $\mathbb{P}^{s-1}$ (see Definition 4.2.7) and let $\mathbb{X}$ be the set in $\mathbb{P}^{s-1}$ parameterized by a clutter $\mathcal{C}$ (see Definition 5.2.8). Consider the set $X = \mathbb{X} \cap T$. In [55] it is shown that $I(X)$ is a complete intersection if and only if $X$ is a projective torus in $\mathbb{P}^{s-1}$ . If the clutter $\mathcal{C}$ has all its edges of the same cardinality, in [56] a classification of the complete intersection property of $I(X)$ is given using linear algebra.

The main result of this chapter is a classification of the complete intersection property of $I(\mathbb{X})$ when $\mathbb{X}$ is of clutter type (Theorem 5.2.17). Using the techniques of [52], this classification can be used to study the *basic parameters* [46, 66] of the Reed-Muller-type codes associated to $\mathbb{X}$.

For all unexplained terminology and additional information, we refer to [47] (for commutative algebra), [9] (for Gröbner bases), and [52, 63, 66] (for vanishing ideals and coding theory).

## 5.2 Complete intersections

In this section we give a full classification of the complete intersection property of vanishing ideals of sets of clutter type over finite fields. We continue to employ the notations and definitions used in Section 5.1.

Throughout this section $K = \mathbb{F}_q$ is a finite field, $y^{v_1}, \ldots, y^{v_s}$ are distinct monomials in the polynomial ring $R = K[\mathbf{y}] = K[y_1, \ldots, y_n]$, with $v_i = (v_{i1}, \ldots, v_{in})$ and $y^{v_i} = y_1^{v_{i1}} \cdots y_n^{v_{in}}$ for $i = 1, \ldots, s$, $\mathbb{X}$ is the set in $\mathbb{P}^{s-1}$ parameterized by these monomials, and $I(\mathbb{X})$ is the vanishing ideal of $\mathbb{X}$. Recall that $I(\mathbb{X})$ is the graded ideal of the polynomial ring $S = K[t_1, \ldots, t_s]$ generated by the homogeneous polynomials of $S$ that vanish on $\mathbb{X}$.

**Definition 5.2.1.** Given $a = (a_1, \ldots, a_n) \in \mathbb{N}^n$, we set $y^a := y_1^{a_1} \cdots y_n^{a_n}$. The *support* of $y^a$, denoted $\mathrm{supp}(y^a)$, is the set of all $y_i$ such that $a_i > 0$.

**Definition 5.2.2.** The set $\mathbb{X}$ is of *clutter type* if $\mathrm{supp}(y^{v_i}) \not\subset \mathrm{supp}(y^{v_j})$ for $i \neq j$.

**Definition 5.2.3.** A *binomial* of $S$ is an element of the form $f = t^a - t^b$, for some $a, b$ in $\mathbb{N}^s$. An ideal generated by binomials is called a *binomial ideal*.

The set $\mathcal{S} = \mathbb{P}^{s-1} \cup \{[0]\}$ is a monoid under componentwise multiplication, that is, given $[\alpha] = [(\alpha_1, \ldots, \alpha_s)]$ and $[\beta] = [(\beta_1, \ldots, \beta_s)]$ in $\mathcal{S}$, the operation of this monoid is given by

$$[\alpha] \cdot [\beta] = [\alpha_1\beta_1, \cdots, \alpha_s\beta_s],$$

where $[\mathbf{1}] = [(1, \ldots, 1)]$ is the identity element.

**Remark 5.2.4.** Since $\mathbb{X}$ is parameterized by monomials, the set $\mathbb{X}\cup\{[0]\}$ is a monoid under componentwise multiplication. Hence, by Theorem 4.2.5, $I(\mathbb{X})$ is a binomial ideal.

**Lemma 5.2.5.** *Let $y^{v_1},\ldots,y^{v_s}$ be a set of monomials such that* $\mathrm{supp}(y^{v_i})\not\subset\mathrm{supp}(y^{v_j})$ *for any $i\neq j$ and let $\mathcal{G}$ be a minimal generating set of $I(\mathbb{X})$ consisting of binomials. The following hold.*

(a) *If $0\neq f=t_j^{a_j}-t^c$ for some $1\leq j\leq s$ and some positive integer $a_j$, then $f\notin I(\mathbb{X})$.*

(b) *For each pair $1\leq i<j\leq s$, there is $g_{ij}$ in $\mathcal{G}$ such that $g_{ij}=\pm(t_i^{c_{ij}}t_j-t^{b_{ij}})$, where $c_{ij}$ is a positive integer less than or equal to $q$ and $b_{ij}\in\mathbb{N}^s\setminus\{0\}$.*

(c) *If $I(\mathbb{X})$ is a complete intersection, then $s\leq 4$.*

**Proof.** (a): We proceed by contradiction. Assume that $f$ is in $I(\mathbb{X})$. Since $I(\mathbb{X})$ is a graded binomial ideal, the binomial $f$ is homogeneous of degree $a_j$, otherwise $t_j^{a_j}$ and $t^c$ would be in $I(\mathbb{X})$ which is impossible. Thus $c\in\mathbb{N}^s\setminus\{0\}$. Hence, as $f\neq 0$, we can pick $t_i\in\mathrm{supp}(t^c)$ with $i\neq j$. By hypothesis there is $y_k\in\mathrm{supp}(y^{v_i})\setminus\mathrm{supp}(y^{v_j})$, i.e., $v_{ik}>0$ and $v_{jk}=0$. Making $y_k=0$ and $y_\ell=1$ for $\ell\neq k$, we get that $f(y^{v_1},\ldots,y^{v_s})=1$, a contradiction.

(b): The binomial $h=t_i^qt_j-t_it_j^q$ vanishes at all points of $\mathbb{P}^{s-1}$, i.e., $h$ is in $I(\mathbb{X})$. Thus there is $g_{ij}$ in $\mathcal{G}$ such that $t_i^qt_j$ is a multiple of one of the two terms of the binomial $g_{ij}$. Hence, by part (a), the assertion follows.

(c): Since $I(\mathbb{X})$ is a complete intersection, there is a set of binomials $\mathcal{G}=\{g_1,\ldots,g_{s-1}\}$ that generate $I(\mathbb{X})$. The number of monomials that occur in $g_1,\ldots,g_{s-1}$ is at most $2(s-1)$. Thanks to part (b) for each pair $1\leq i<j\leq s$, there is a monomial $t_i^{c_{ij}}t_j$, with $c_{ij}\in\mathbb{N}_+$, and a binomial $g_{ij}$ in $\mathcal{G}$ such that the monomial $t_i^{c_{ij}}t_j$ occurs in $g_{ij}$. As there are $s(s-1)/2$ of these monomials, we get $s(s-1)/2\leq 2(s-1)$. Thus $s\leq 4$. □

**Lemma 5.2.6.** *Let $K$ be a field and let $I$ be the ideal of $S=K[t_1,t_2,t_3,t_4]$ generated by the binomials $g_1=t_1t_2-t_3t_4, g_2=t_1t_3-t_2t_4, g_3=t_2t_3-t_1t_4$. The following hold.*

(i) *$\mathcal{G}=\{t_2t_3-t_1t_4,t_1t_3-t_2t_4,t_1t_2-t_3t_4,t_2^2t_4-t_3^2t_4,t_1^2t_4-t_3^2t_4,t_3^3t_4-t_3t_4^3\}$ is a Gröbner basis of $I$ with respect to the GRevLex order $\prec$ on $S$.*

(ii) *If* $\mathrm{char}(K)=2$, *then* $\mathrm{rad}(I)\neq I$.

(iii) *If* $\mathrm{char}(K)\neq 2$ *and $e_i$ is the $i$-th unit vector, then $I=I(\mathbb{X})$, where*

$$\mathbb{X}=\{[e_1],\ [e_2],\ [e_3],\ [e_4],\ [(1,-1,-1,1)],\ [(1,1,1,1)],\ [(-1,-1,1,1)],\ [(-1,1,-1,1)]\}.$$

**Proof.** (i): Using Buchberger's criterion [9, p. 84], it is seen that $\mathcal{G}$ is a Gröbner basis of $I$.

(ii): Setting $h=t_1t_2-t_1t_3$, we get $h^2=(t_1t_2)^2-(t_1t_3)^2=t_1t_2g_1+t_1t_3g_2$, where $g_1=t_1t_2-t_3t_4$ and $g_2=t_1t_3-t_2t_4$. Thus $h\in\mathrm{rad}(I)$. Using part (i) it is seen that $h\notin I$.

(iii): As $g_i$ vanishes at all points of $\mathbb{X}$ for $i = 1, 2, 3$, we get the inclusion $I \subset I(\mathbb{X})$. Since $\mathbb{X} \cup \{0\}$ is a monoid under componentwise multiplication, by Theorem 4.2.5, $I(\mathbb{X})$ is a binomial ideal. Take a homogeneous binomial $f$ in $S$ that vanishes at all points of $\mathbb{X}$. Let $h = t^a - t^b$, $a = (a_i)$, $b = (b_i)$, be the residue obtained by dividing $f$ by $\mathcal{G}$. Hence we can write $f = g + h$, where $g \in I$ and the terms $t^a$ and $t^b$ are not divisible by any of the leading terms of $\mathcal{G}$. It suffices to show that $h = 0$. Assume that $h \neq 0$. As $h \in I(\mathbb{X})$ and $[e_i]$ is in $\mathbb{X}$ for all $i$, we get that $|\text{supp}(t^a)| \geq 2$ and $|\text{supp}(t^b)| \geq 2$. It follows that $h$ has one of the following forms:

$$\begin{array}{lll} h = t_1t_4^i - t_2t_4^i, & h = t_1t_4^i - t_3t_4^i, & h = t_2t_4^i - t_3t_4^i, \\ h = t_3^2t_4^{i-1} - t_3t_4^i, & h = t_3^2t_4^{i-1} - t_2t_4^i, & h = t_3^2t_4^{i-1} - t_1t_4^i, \end{array}$$

where $i \geq 1$, a contradiction because none of these binomials vanishes at all points of $\mathbb{X}$. □

**Definition 5.2.7.** A *hypergraph* $\mathcal{H}$ is a pair $(V(\mathcal{H}), E(\mathcal{H}))$ such that $V(\mathcal{H})$ is a finite set and $E(\mathcal{H})$ is a subset of the set of all subsets of $V(\mathcal{H})$. The elements of $E(\mathcal{H})$ and $V(\mathcal{H})$ are called *edges* and *vertices*, respectively. A hypergraph is *simple* if $f_1 \not\subset f_2$ for any two edges $f_1, f_2$. A simple hypergraph is called a *clutter* and will be denoted by $\mathcal{C}$ instead of $\mathcal{H}$.

One example of a clutter is a graph with the vertices and edges defined in the usual way.

**Definition 5.2.8.** Let $\mathcal{C}$ be a *clutter* with vertex set $V(\mathcal{C}) = \{y_1, \ldots, y_n\}$, let $f_1, \ldots, f_s$ be the edges of $\mathcal{C}$ and let $v_k = \sum_{x_i \in f_k} e_i$ be the *characteristic vector* of $f_k$ for $1 \leq k \leq s$, where $e_i$ is the $i$-th unit vector. The set in the projective space $\mathbb{P}^{s-1}$ parameterized by $y^{v_1}, \ldots, y^{v_s}$, denoted by $\mathbb{X}_{\mathcal{C}}$, is called the *projective set parameterized* by $\mathcal{C}$.

**Lemma 5.2.9.** *Let $K = \mathbb{F}_q$ be a finite field with $q \neq 2$ elements, let $\mathcal{C}$ be a clutter with vertices $y_1, \ldots, y_n$, let $v_1, \ldots, v_s$ be the characteristic vectors of the edges of $\mathcal{C}$ and let $\mathbb{X}_{\mathcal{C}}$ be the projective set parameterized by $\mathcal{C}$. If $f = t_it_j - t_kt_\ell \in I(\mathbb{X}_{\mathcal{C}})$, with $i, j, k, l$ distinct, then $y^{v_i}y^{v_j} = y^{v_k}y^{v_\ell}$.*

**Proof.** For simplicity assume that the polynomial $f = t_1t_2 - t_3t_4$. Setting $A_1 = \text{supp}(y^{v_1}y^{v_2})$, $A_2 = \text{supp}(y^{v_3}y^{v_4})$, $S_1 = \text{supp}(y^{v_1}) \cap \text{supp}(y^{v_2})$ and $S_2 = \text{supp}(y^{v_3}) \cap \text{supp}(y^{v_4})$, it suffices to show the equalities $A_1 = A_2$ and $S_1 = S_2$. If $A_1 \not\subset A_2$, pick $y_k \in A_1 \setminus A_2$. Making $y_k = 0$ and $y_\ell = 1$ for $\ell \neq k$, and using that $f$ vanishes on $\mathbb{X}_{\mathcal{C}}$, we get that $f(y^{v_1}, \ldots, y^{v_4}) = -1 = 0$, a contradiction. Thus $A_1 \subset A_2$. The other inclusion follows by a similar reasoning. Next we show the equality $S_1 = S_2$. If $S_1 \not\subset S_2$, pick a variable $y_k \in S_1 \setminus S_2$. Let $\beta$ be a generator of the cyclic group $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. Making $y_k = \beta$, $y_\ell = 1$ for $\ell \neq k$, and using that $f$ vanishes on $\mathbb{X}_{\mathcal{C}}$ and the equality $A_1 = A_2$, we get that $f(y^{v_1}, \ldots, y^{v_4}) = \beta^2 - \beta = 0$. Hence $\beta^2 = \beta$ and $\beta = 1$, a contradiction because $q \neq 2$. Thus $S_1 \subset S_2$. The other inclusion follows by a similar argument. □

**Remark 5.2.10.** Let $K = \mathbb{F}_q$ be a finite field with $q$ odd and let $\mathbb{X}$ be the set of clutter type in $\mathbb{P}^3$ parameterized by the following monomials:

$$\begin{aligned} y^{v_1} &= y_1^{q-1}y_2^r y_3^r y_4^{q-1}y_5^{q-1}y_6^{q-1}y_7^{q-1},\\ y^{v_2} &= y_1^r y_2^r y_3^{q-1}y_4^{q-1}y_5^{q-1}y_6^{q-1}y_8^{q-1},\\ y^{v_3} &= y_2^{q-1}y_4^{q-1}y_1^r y_3^r y_5^{q-1}y_7^{q-1}y_8^{q-1},\\ y^{v_4} &= y_1^{q-1}y_2^{q-1}y_3^{q-1}y_4^{q-1}y_6^{q-1}y_7^{q-1}y_8^{q-1}, \end{aligned}$$

where $r = (q-1)/2$. Then

$$\mathbb{X} = \{[e_1],\ [e_2],\ [e_3],\ [e_4],\ [(1,-1,-1,1)],\ [(1,1,1,1)],\ [(-1,-1,1,1)],\ [(-1,1,-1,1)]\},$$

$|\mathbb{X}| = 8$ and $I(\mathbb{X}) = (t_1t_2 - t_3t_4, t_1t_3 - t_2t_4, t_2t_3 - t_1t_4)$.

Below we show that the set $\mathbb{X}$ of Remark 5.2.10 cannot be parameterized by a clutter.

**Remark 5.2.11.** Let $K = \mathbb{F}_q$ be a field with $q \neq 2$ elements. Then the ideal

$$I = (t_1t_2 - t_3t_4, t_1t_3 - t_2t_4, t_2t_3 - t_1t_4)$$

cannot be the vanishing ideal of a set in $\mathbb{P}^3$ parameterized by a clutter. Indeed assume that there is a clutter $\mathcal{C}$ such that $I = I(\mathbb{X}_\mathcal{C})$ and $\mathbb{X}_\mathcal{C} \subset \mathbb{P}^3$. If $v_1, \ldots, v_4$ are the characteristic vectors of the edges of $\mathcal{C}$. Then, by Lemma 5.2.9, we get $v_1+v_2 = v_3+v_4$, $v_1+v_3 = v_2+v_4$ and $v_2+v_3 = v_1+v_4$. It follows that $v_1 = v_2 = v_3 = v_4$, a contradiction.

**Lemma 5.2.12.** *Let $K$ be a field and let $I$ be the ideal of $S = K[t_1, t_2, t_3]$ generated by the binomials $g_1 = t_1t_2 - t_2t_3, g_2 = t_1t_3 - t_2t_3$. The following hold.*

(i) *$\mathcal{G} = \{t_1t_3 - t_2t_3,\ t_1t_2 - t_2t_3,\ t_2^2t_3 - t_2t_3^2\}$ is a Gröbner basis of $I$ with respect to the GRevLex order $\prec$ on $S$.*

(ii) *$I = I(\mathbb{X})$, where $\mathbb{X} = \{[e_1],\ [e_2],\ [e_3],\ [(1,1,1)]\}$.*

**Proof.** It follows using the arguments given in Lemma 5.2.6. □

**Remark 5.2.13.** Let $K = \mathbb{F}_q$ be a finite field with $q$ elements and let $\mathbb{X}$ be the projective set in $\mathbb{P}^2$ parameterized by the following monomials:

$$y^{v_1} = y_1^{q-1}y_2^{q-1},\ y^{v_2} = y_2^{q-1}y_3^{q-1},\ y^{v_3} = y_1^{q-1}y_3^{q-1}.$$

Then $\mathbb{X} = \{[e_1],\ [e_2],\ [e_3],\ [(1,1,1)]\}$ and $I(\mathbb{X}) = (t_1t_2 - t_2t_3,\ t_1t_3 - t_2t_3)$.

**Lemma 5.2.14.** *Let $\beta$ be a generator of $\mathbb{F}_q^*$ and $0 \neq r \in \mathbb{N}$. Suppose $s = 2$. If $I = (t_1^{r+1}t_2 - t_1t_2^{r+1})$ and $r$ divides $q-1$, then $I = I(\mathbb{X})$, where $\mathbb{X}$ is the set of clutter type in $\mathbb{P}^1$ parameterized by $y_1^{q-1}$, $y_2^{q-1}y_3^k$ and $r = \mathrm{o}(\beta^k)$.*

**Proof.** We set $f = t_1^{r+1}t_2 - t_1t_2^{r+1}$. Take a point $P = [(x_1^{q-1}, x_2^{q-1}x_3^k)]$ in $\mathbb{X}$. Then

$$f(P) = (x_1^{q-1})^{r+1}(x_2^{q-1}x_3^k) - (x_1^{q-1})(x_2^{q-1}x_3^k)^{r+1}.$$

We may assume $x_1 \neq 0$ and $x_2 \neq 0$. Then $f(P) = x_3^k - (x_3^k)^{r+1}$. If $x_3 \neq 0$, then $x_3 = \beta^i$ for some $i$ and $(x_3^k)^{r+1} = x_3^k$, that is, $f(P) = 0$. Therefore one has the inclusion $(f) \subset I(\mathbb{X})$.

Next we show the inclusion $I(\mathbb{X}) \subset (f)$. By Theorem 4.2.5, $I(\mathbb{X})$ is a binomial ideal. Take a non-zero binomial $g = t_1^{a_1}t_2^{a_2} - t_1^{b_1}t_2^{b_2}$ that vanishes on $\mathbb{X}$. Then $a_1 + a_2 = b_1 + b_2$ because $I(\mathbb{X})$ is graded. We may assume that $b_1 > a_1$ and $a_2 > b_2$. We may also assume that $a_1 > 0$ and $b_2 > 0$ because $\{[e_1], [e_2]\} \subset \mathbb{X}$. Then $g = t_1^{a_1}t_2^{b_2}(t_2^{a_2-b_2} - t_1^{b_1-a_1})$. As $g$ vanishes on $\mathbb{X}$, making $y_3 = \beta$ and $y_1 = y_2 = 1$, we get $(\beta^k)^{a_2-b_2} = 1$. Hence $a_2 - b_2 = \lambda r$ for some $\lambda \in \mathbb{N}_+$, where $r = o(\beta^k)$. Thus $t_2^{a_2-b_2} - t_1^{b_1-a_1}$ is equal to $t_2^{\lambda r} - t_1^{\lambda r} \in (t_1^r - t_2^r)$. Therefore $g$ is a multiple of $f = t_1t_2(t_1^r - t_2^r)$ because $a_1 > 0$ and $b_2 > 0$. Thus $g \in (f)$. □

**Lemma 5.2.15.** *Let $K = \mathbb{F}_q$ be a finite field. If $\{[e_1], [e_2]\} \subset \mathbb{Y} \subset \mathbb{P}^1$ and $\mathbb{Y} \cup \{0\}$ is a monoid under componentwise multiplication, then there is $0 \neq r \in \mathbb{N}$ such that $I(\mathbb{Y}) = (t_1^{r+1}t_2 - t_1t_2^{r+1})$ and $r$ divides $q-1$.*

**Proof.** We set $f = t_1^{r+1}t_2 - t_1t_2^{r+1}$ and $X = \mathbb{Y} \cap T$, where $T$ is a projective torus in $\mathbb{P}^1$. The set $X$ is a group, under componentwise multiplication, because $X$ is a finite monoid and the cancellation laws hold. By Theorem 4.2.5, $I(\mathbb{Y})$ is a binomial ideal. Clearly $(f) \subset I(\mathbb{Y})$. To show the other inclusion take a non-zero binomial $g = t_1^{a_1}t_2^{a_2} - t_1^{b_1}t_2^{b_2}$ that vanish on $\mathbb{Y}$. Then $a_1 + a_2 = b_1 + b_2$ because $I(\mathbb{Y})$ is graded. We may assume that $b_1 > a_1$ and $a_2 > b_2$. We may also assume that $a_1 > 0$ and $b_2 > 0$ because $\{[e_1], [e_2]\} \subset \mathbb{X}$. Then $g = t_1^{a_1}t_2^{b_2}(t_2^{a_2-b_2} - t_1^{b_1-a_1})$. The subgroup of $\mathbb{F}_q^*$ given by $H = \{\xi \in \mathbb{F}_q^* \,|\, [(1, \xi)] \in X\}$ has order $r = |X|$. Pick a generator $\beta$ of the cyclic group $\mathbb{F}_q^*$. Then $H$ is a cyclic group generated by $\beta^k$ for some $k \geq 0$. As $g$ vanishes on $\mathbb{Y}$, one has that $t_2^{a_2-b_2} - t_1^{b_1-a_1}$ vanishes on $X$. In particular $(\beta^k)^{a_2-b_2} = 1$. Hence $a_2 - b_2 = \lambda r$ for some $\lambda \in \mathbb{N}_+$, where $r = o(\beta^k) = |X|$. Proceeding as in the proof of Lemma 5.2.14 one derives that $g \in (f)$. Noticing that $T$ has order $q-1$, we obtain that $r$ divides $q-1$. □

**Definition 5.2.16.** An ideal $I \subset S$ is called a *complete intersection* if there exists $g_1, \ldots, g_r$ in $S$ such that $I = (g_1, \ldots, g_r)$, where $r$ is the height of $I$.

Recall that a graded ideal $I$ is a complete intersection if and only if $I$ is generated by a homogeneous regular sequence with $\mathrm{ht}(I)$ elements (see [70, Proposition 2.3.19, Lemma 2.3.20]).

**Theorem 5.2.17.** *Let $K = \mathbb{F}_q$ be a finite field and let $\mathbb{X}$ be a set in $\mathbb{P}^{s-1}$ parameterized by a set of monomials $y^{v_1}, \ldots, y^{v_s}$ such that $\mathrm{supp}(y^{v_i}) \not\subset \mathrm{supp}(y^{v_j})$ for any $i \neq j$. Then $I(\mathbb{X})$ is a complete intersection if and only if $s \leq 4$ and, up to permutation of variables, $I(\mathbb{X})$ has one of the following forms:*

(i) *$s = 4$, $q$ is odd and $I = (t_1t_2 - t_3t_4, t_1t_3 - t_2t_4, t_2t_3 - t_1t_4)$.*

(ii) $s = 3$ *and* $I = (t_1t_2 - t_2t_3, t_1t_3 - t_2t_3)$.

(iii) $s = 2$ *and* $I = (t_1^{r+1}t_2 - t_1t_2^{r+1})$, *where* $0 \neq r \in \mathbb{N}$ *is a divisor of* $q - 1$.

(iv) $s = 1$ *and* $I = (0)$.

**Proof.** $\Rightarrow$): Assume that $I(\mathbb{X})$ is a complete intersection. By Lemma 5.2.5(c) one has $s \leq 4$.

Case (i): Assume that $s = 4$. Setting $I = I(\mathbb{X})$, by hypothesis $I$ is generated by 3 binomials $g_1, g_2, g_3$. By Lemma 5.2.5(b) for each pair $1 \leq i < j \leq 4$ there are positive integers $c_{ij}$ and $a_{ij}$ such that $t_i^{c_{ij}}t_j$ and $t_it_j^{a_{ij}}$ occur as terms in $g_1, g_2, g_3$. Since there are at most 6 monomials that occur in the $g_i$'s, we get that $c_{ij} = a_{ij} = 1$ for $1 \leq i < j \leq 4$. Thus, up to permutation of variables, there are 4 subcases to consider:

$$\begin{aligned}
(a):&\quad g_1 = t_1(t_2 - t_3), \quad g_2 = t_1t_4 - t_2t_3, \quad g_3 = t_4(t_2 - t_3).\\
(b):&\quad g_1 = t_1(t_2 - t_3), \quad g_2 = t_4(t_1 - t_3), \quad g_3 = t_2(t_3 - t_4).\\
(c):&\quad g_1 = t_1t_2 - t_3t_4, \quad g_2 = t_1t_3 - t_2t_4, \quad g_3 = t_2t_3 - t_1t_4.\\
(d):&\quad g_1 = t_3(t_1 - t_2), \quad g_2 = t_1(t_3 - t_4), \quad g_3 = t_2(t_1 - t_4).
\end{aligned}$$

Subcase (a): This case cannot occur because the ideal $(g_1, g_2, g_3)$ has height 2.

Subcase (b): The reduced Gröbner basis of $I = (g_1, g_2, g_3)$ with respect to the GRevLex order $\prec$ is given by

$$\begin{aligned}
&g_1 = t_1t_2 - t_1t_3, \quad g_2 = t_1t_4 - t_3t_4, \quad g_3 = t_2t_3 - t_2t_4,\\
&g_4 = t_3^2t_4 - t_2t_4^2, \quad g_5 = t_1t_3^2 - t_2t_4^2, \quad g_6 = t_2^2t_4^2 - t_2t_4^3.
\end{aligned}$$

Hence the binomial $h = t_2t_4 - t_3t_4 \notin I$ because $t_2t_4$ does not belong to $\mathrm{in}_\prec(I)$, the initial ideal of $I$. Since $h^2 = -2t_4^2g_3 + t_4g_4 + g_6$, we get that $h \in \mathrm{rad}(I)$. Thus $I$ is not a radical ideal which is impossible because $I = I(\mathbb{X})$ is a vanishing ideal. Therefore this case cannot occur.

Subcase (c): In this case one has $I = (t_1t_2 - t_3t_4, t_1t_3 - t_2t_4, t_2t_3 - t_1t_4)$, as required. From Lemma 5.2.6, we obtain that $q$ is odd.

Subcase (d): The reduced Gröbner basis of $I = (g_1, g_2, g_3)$ with respect to the GRevLex order $\prec$ is given by

$$\begin{aligned}
&h_1 = t_2t_3 - t_1t_4, \quad g_2 = t_1t_3 - t_1t_4, \quad g_3 = t_1t_2 - t_2t_4,\\
&g_4 = t_1t_4^2 - t_2t_4^2, \quad g_5 = t_1^2t_4 - t_2t_4^2, \quad g_6 = t_2^2t_4^2 - t_2t_4^3.
\end{aligned}$$

Setting $h = t_1t_4 - t_2t_4$, as in Subcase (b), one can readily verify that $h \notin I$ and $h^2 \in I$. Hence $I$ is not a radical ideal. Therefore this case cannot occur.

Case (ii): Assume that $s = 3$. By hypothesis $I = I(\mathbb{X})$ is generated by 2 binomials $g_1, g_2$. By Lemma 5.2.5(b) for each pair $1 \leq i < j \leq 3$ there are positive integers $c_{ij}$ and $a_{ij}$ such that $t_i^{c_{ij}}t_j$ and $t_it_j^{a_{ij}}$ occur as terms in $g_1, g_2$. Since there are at most 4 monomials that occur in the $g_i$'s it is seen that, up to permutation of variables, there are 2 subcases to consider:

$$
\begin{aligned}
(a): &\quad g_1 = t_1t_3 - t_2t_3,\ g_2 = t_1^{c_{12}}t_2 - t_1t_2^{a_{12}} \text{ with } c_{12} = a_{12} \geq 2.\\
(b): &\quad g_1 = t_1t_2 - t_2t_3,\ g_2 = t_1t_3 - t_2t_3.
\end{aligned}
$$

Subcase (a) cannot occur because the ideal $I = (g_1, g_2)$, being contained in $(t_1 - t_2)$, has height 1. Thus we are left with subcase (b), that is, $I = (t_1t_2 - t_2t_3, t_1t_3 - t_2t_3)$, as required.

Case (iii): If $s = 2$, then $\mathbb{X}$ is parameterized by $y^{v_1}$, $y^{v_2}$. Pick $y_k \in \mathrm{supp}(y^{v_1})\backslash\mathrm{supp}(y^{v_2})$. Making $y_k = 0$ and $y_\ell = 1$ for $\ell \neq k$, we get that $[e_2] \in \mathbb{X}$, and by a similar argument $[e_1] \in \mathbb{X}$. As $\mathbb{X} \cup \{[0]\}$ is a monoid under componentwise multiplication, by Lemma 5.2.15, $I(\mathbb{X})$ has the required form.

Case (iv): If $s = 1$, this case is clear.

$\Leftarrow$) The converse is clear because the vanishing ideal $I(\mathbb{X})$ has height $s - 1$. □

**Proposition 5.2.18.** *If $I$ is an ideal of $S$ of one of the following forms:*

(i) $s = 4$, *$q$ is odd and* $I = (t_1t_2 - t_3t_4, t_1t_3 - t_2t_4, t_2t_3 - t_1t_4)$,

(ii) $s = 3$ *and* $I = (t_1t_2 - t_2t_3, t_1t_3 - t_2t_3)$,

(iii) $s = 2$ *and* $I = (t_1^{r+1}t_2 - t_1t_2^{r+1})$, *where* $0 \neq r \in \mathbb{N}$ *and $r$ divides* $q - 1$,

*then there is a set $\mathbb{X}$ in $\mathbb{P}^{s-1}$ of clutter type such that $I$ is the vanishing ideal $I(\mathbb{X})$.*

**Proof.** The result follows from Lemma 5.2.6 and Remark 5.2.10, Lemma 5.2.12 and Remark 5.2.13, and Lemma 5.2.14, respectively. □

# Chapter 6

# Problems and Related Results

## 6.1 Degree and regularity of vanishing ideals

The results of this thesis allows us to compute the degree and regularity index of vanishing ideals parameterized by rational functions over any field.

The following general problem was one of our initial motivations to find computational tools to compute generating sets of vanishing ideals.

**Problem 6.1.1.** Find explicit formulas for the degree and regulariy index for families of vanishing ideals arising from combinatorial structures when the base field is finite.

**Problem 6.1.2.** Let $K = \mathbb{F}_q$ be a finite field and let $\mathbb{X}$ and $X$ be the projective and algebraic sets in $\mathbb{P}^{s-1}$ parameterized by a set $y^{v_1}, \ldots, y^{v_s}$ of Laurent monomials. Find formulas for the algebraic invariants of the vanishing ideals $I(\mathbb{X})$ an $I(X)$, and for the basic parameters of $C_{\mathbb{X}}(d)$ and $C_X(d)$, the Reed-Muller-type codes of degree $d$ over $\mathbb{X}$ and $X$, respectively, in terms of $s$, $q$, $d$, and the combinatorics of $v_1, \ldots, v_s$.

This is an open problem where our results can be used to find formulas for the degree and the regularity of $I(\mathbb{X})$ and $I(X)$, and for the dimension and length of the Reed-Muller-type codes $C_{\mathbb{X}}(d)$ and $C_X(d)$. The degree is the easiest invariant to compute. The regularity is harder to compute.

If $X_G$ is the algebraic projective set parameterized by the edges of $G$, then a formula for the degree of $S/X_G$ is given in [50, Theorem 3.2].

**Problem 6.1.3.** Let $G$ be a graph and let $\mathbb{X}_G$ be the set in $\mathbb{P}^{s-1}$ parameterized by the edges of $G$. Find a formula for the degree of $S/I(\mathbb{X}_G)$ in terms of the graph invariants of $G$ and the combinatorics of the graph.

The following is still a wide open problem.

**Problem 6.1.4.** Let $G$ be a graph and let $\mathbb{X}_G$ and $X_G$ be the projective and algebraic sets in $\mathbb{P}^{s-1}$, respectively, parameterized by the edges of $G$. Find formulas for the regularity index of $I(\mathbb{X}_G)$ and $I(X_G)$ in terms of $q$ and the combinatorics of $G$.

The regularity index of $S/I(X_G)$ has been studied in [28, 50, 68] for certain families of graphs.

**Problem 6.1.5.** For a connected graph $G$ characterize when $I(\mathbb{X})$ is a complete intersection.

For an arbitrary graph $G$ in [55] it is shown that $I(X)$ is a complete intersection if and only if $X$ is a projective torus.

## 6.2 Binomial vanishing ideals

**Problem 6.2.1.** If $\mathbb{X}$ is a projective set parameterized by rational functions over a finite field and $I(\mathbb{X})$ is a binomial ideal, then by Proposition 2.3.9 $I(X)$ is a binomial ideal. Is the converse true?

Let $K = \mathbb{F}_q$ be a finite field. If $\mathbb{X}$ is a set in $\mathbb{P}^{s-1}$ parameterized by Laurent monomials, then $I(\mathbb{X})$ is a binomial ideal (see Corollary 2.3.21). We give a family of ideals where the converse is true; see Proposition 2.3.25.

This leads us to pose the following conjecture.

**Conjecture 6.2.2.** Let $K = \mathbb{F}_q$ be a finite field and let $\mathbb{Y}$ be a subset of $\mathbb{P}^{s-1}$. If $I(\mathbb{Y})$ is a binomial ideal, then $\mathbb{Y}$ is a set parameterized by Laurent monomials (see Conjecture 2.3.26).

This conjecture fails for infinite fields (see Example 2.2.9). Notice that this conjecture can be restated as:

**Problem 6.2.3.** Let $K = \mathbb{F}_q$ be a finite field and $\mathbb{Y} \subset \mathbb{P}^{s-1}$. If $V(I(\mathbb{Y})) \cup \{[0]\}$ is a monoid under componentwise multiplication, then $\mathbb{Y}$ is parameterized by Laurent monomials.

The next problem seems likely to hold.

**Problem 6.2.4.** Let $K = \mathbb{F}_q$ be a finite field and $\mathbb{X} \subset \mathbb{P}^{s-1}$. If $\mathbb{X} \cup \{0\}$ is a multiplicative monoid and $\mathbb{X} = \{[e_1], \ldots, [e_s]\} \cup (\mathbb{X} \cap T)$, where $T$ is a projective torus in $\mathbb{P}^{s-1}$, then $\mathbb{X}$ is parameterized by Laurent monomials. For this family when is $I(\mathbb{X})$ a complete intersection?

Another problem on vanishing ideals is:

**Problem 6.2.5.** Let $K$ be a field and let $\mathbb{X}$ be a subset of $\mathbb{P}^{s-1}$ parameterized by Laurent monomials. Give necessary and/or sufficient conditions for the equality $V(I(\mathbb{X})) = \mathbb{X}$.

If $K$ is an infinite field, the affine case of this equality was studied [39, 40, 54]. We plan to study these three papers to see if all results there hold for the projective case.

**Problem 6.2.6.** Let $\mathbb{X}$ be a set of clutter type such that $I(\mathbb{X})$ is a complete intersection. Using the techniques of [12, 43, 52, 55] and Theorem 5.2.17 find formulas for the *basic parameters* of the Reed-Muller-type codes associated to $\mathbb{X}$.

# Bibliography

[1] N. Alon, Combinatorial Nullstellensatz, Recent trends in combinatorics (Mat́raháza, 1995), Combin. Probab. Comput. **8** (1999), no. 1-2, 7–29.

[2] M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, Reading, MA, 1969.

[3] E. Ballico and C Fontanari, The Horace method for error-correcting codes, Appl. Algebra Engrg. Comm. Comput. **17** (2006), no. 2, 135–139.

[4] W. Bruns and J. Gubeladze, *Polytopes, Rings, and K-Theory*, Springer Monographs in Mathematics, Springer, Dordrecht, 2009.

[5] W. Bruns and J. Herzog, *Cohen-Macaulay Rings*, Revised Edition, Cambridge University Press, 1997.

[6] B. Buchberger, An algorithmic method in polynomial ideal theory, in *Recent Trends in Mathematical Systems Theory* (N.K. Bose, Ed.), Reidel, Dordrecht, 1985, 184–232.

[7] C. Carvalho, On the second Hamming weight of some Reed-Muller type codes, Finite Fields Appl. **24** (2013), 88–94.

[8] C. Carvalho, V. G. Lopez Neumann and H. H. López, Projective nested cartesian codes. Preprint, 2014, `arXiv:1411.6819v1`.

[9] D. Cox, J. Little and D. O'Shea, *Ideals, Varieties, and Algorithms*, Springer-Verlag, 1992.

[10] P. Delsarte, J. M. Goethals and F. J. MacWilliams, On generalized Reed–Muller codes and their relatives, Information and Control **16** (1970), 403–442.

[11] E. Dias and J. Neves, Codes over a weighted torus, Finite Fields Appl. **33** (2015), 66–79.

[12] I. M. Duursma, C. Rentería and H. Tapia-Recillas, Reed–Muller codes on complete intersections, Appl. Algebra Engrg. Comm. Comput. **11** (2001), no. 6, 455–462.

[13] D. Eisenbud, *Commutative Algebra with a view toward Algebraic Geometry*, Graduate Texts in Mathematics **150**, Springer-Verlag, 1995.

[14] D. Eisenbud, *The geometry of syzygies: A second course in commutative algebra and algebraic geometry*, Graduate Texts in Mathematics **229**, Springer-Verlag, New York, 2005.

[15] D. Eisenbud, D. R. Grayson, and M. Stillman, eds., *Computations in algebraic geometry with Macaulay 2*, Algorithms and Computation in Mathematics **8**, Springer-Verlag, Berlin, 2002.

[16] D. Eisenbud and B. Sturmfels, Binomial ideals, Duke Math. J. **84** (1996), 1–45.

[17] V. Ene and J. Herzog, *Gröbner Bases in Commutative Algebra*, Graduate Studies in Mathematics **130**, American Mathematical Society, Providence, RI, 2012.

[18] C. Escobar, J. Martínez-Bernal and R. H. Villarreal, Relative volumes and minors in monomial subrings, Linear Algebra Appl. **374** (2003), 275–290.

[19] M. Gasca, Mariano and T. Sauer, Polynomial interpolation in several variables, Adv. Comput. Math. **12** (2000), no. 4, 377–410.

[20] O. Geil, On the second weight of generalized Reed-Muller codes, Des. Codes Cryptogr. **48** (2008), 323–330.

[21] O. Geil and C. Thomsen, Weighted Reed–Muller codes revisited, Des. Codes Cryptogr. **66** (2013), 195–220.

[22] A. V. Geramita, M. Kreuzer and L. Robbiano, Cayley-Bacharach schemes and their canonical modules, Trans. Amer. Math. Soc. **339** (1993), no. 1, 163–189.

[23] L. Gold, J. Little and H. Schenck, Cayley-Bacharach and evaluation codes on complete intersections, J. Pure Appl. Algebra **196** (2005), no. 1, 91–99.

[24] M. González-Sarabia and C. Rentería, Evaluation codes associated to complete bipartite graphs, Int. J. Algebra **2** (2008), no. 1-4, 163–170.

[25] M. González-Sarabia and C. Rentería, The second generalized Hamming weight of some evaluation codes arising from complete bipartite graphs, Int. J. Contemp. Math. Sci. **4** (2009), no. 25–28, 1345–1352.

[26] M. González-Sarabia, C. Rentería and M. A. Hernández de la Torre, Minimum distance and second generalized Hamming weight of two particular linear codes, Congr. Numer. **161** (2003), 105–116.

[27] M. González-Sarabia, C. Rentería and A. J. Sánchez, Minimum distance of some evaluation codes, Appl. Algebra Engrg. Comm. Comput. **24** (2013), no. 2, 95–106.

[28] M. Gonzalez–Sarabia, C. Rentería and E. Sarmiento, Parameterized codes over some embedded sets and their applications to complete graphs, Math. Commun. **18** (2013), no. 2, 377–391.

[29] M. González-Sarabia, C. Rentería and H. Tapia-Recillas, Reed–Muller-type codes over the Segre variety, Finite Fields Appl. **8** (2002), no. 4, 511–518.

[30] D. Grayson and M. Stillman, *Macaulay*2, 1996. Available via anonymous ftp from `math.uiuc.edu`.

[31] G. M. Greuel and G. Pfister, *A Singular Introduction to Commutative Algebra*, 2nd extended edition, Springer, Berlin, 2008.

[32] A. Guerrieri and I. Swanson, On the ideal of minors of matrices of linear forms, Contemp. Math. **331** (2003), 139-152.

[33] J. Hansen, Linkage and codes on complete intersections, Appl. Algebra Engrg. Comm. Comput. **14** (2003), no. 3, 175–185.

[34] J. Harris, *Algebraic Geometry. A first course*, Graduate Texts in Mathematics **133**, Springer-Verlag, New York, 1992.

[35] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, 1977.

[36] M. Hellus and R. Waldi, Interpolation in affine and projective space over a finite field, J. Commut. Algebra, to appear.

[37] N. Jacobson, *Basic Algebra I*, Second Edition, W. H. Freeman and Company, New York, 1996.

[38] T. Kahle and J. Rauh, Toric fiber products versus Segre products, Abh. Math. Semin. Univ. Hambg. **84** (2014), no. 2, 187–201.

[39] A. Katsabekis and A. Thoma, Toric sets and orbits on toric varieties, J. Pure Appl. Algebra **181** (2003), 75–83.

[40] A. Katsabekis and A. Thoma, Parametrizations of toric varieties over any field, J. Algebra **308** (2007), no. 2, 751–763.

[41] M. Kreuzer and L. Robbiano, *Computational Commutative Algebra* 2, Springer-Verlag, Berlin, 2005.

[42] G. Lachaud, The parameters of projective Reed-Muller codes, Discrete Math. **81** (1990), no. 2, 217–221.

[43] H. H. López, C. Rentería and R. H. Villarreal, Affine cartesian codes, Des. Codes Cryptogr. **71** (2014), no. 1, 5–19.

[44] H. H. López, E. Sarmiento, M. Vaz Pinto and R. H. Villarreal, Parameterized affine codes, Studia Sci. Math. Hungar. **49** (2012), no. 3, 406–418.

[45] H. H. López and R. H. Villarreal, Computing the degree of a lattice ideal of dimension one, *J. Symbolic Comput.* **65** (2014), 15–28.

[46] F. J. MacWilliams and N.J.A. Sloane, *The Theory of Error-correcting Codes*, North-Holland, 1977.

[47] H. Matsumura, *Commutative Ring Theory*, Cambridge Studies in Advanced Mathematics **8**, Cambridge University Press, 1986.

[48] E. Miller and B. Sturmfels, *Combinatorial Commutative Algebra*, Graduate Texts in Mathematics **227**, Springer, 2004.

[49] J. Neves, M. Vaz Pinto and R. H. Villarreal, Regularity and algebraic properties of certain lattice ideals, Bull. Braz. Math. Soc. (N.S.), to appear.

[50] J. Neves, M. Vaz Pinto and R. H. Villarreal, Vanishing ideals over graphs and even cycles, Comm. Algebra, to appear. Preprint, 2011, arXiv:1111.6278v3.

[51] L. O'Carroll, F. Planas-Vilanova and R. H. Villarreal, Degree and algebraic properties of lattice and matrix ideals, SIAM J. Discrete Math. **28** (2014), no. 1, 394–427.

[52] C. Rentería, A. Simis and R. H. Villarreal, Algebraic methods for parameterized codes and invariants of vanishing ideals over finite fields, Finite Fields Appl. **17** (2011), no. 1, 81-104.

[53] C. Rentería and H. Tapia-Recillas, Linear codes associated to the ideal of points in $\mathbf{P}^d$ and its canonical module, Comm. Algebra **24** (1996), no. 3, 1083–1090.

[54] E. Reyes, R. H. Villarreal and L. Zárate, A note on affine toric varieties, Linear Algebra Appl. **318** (2000), 173–179.

[55] E. Sarmiento, M. Vaz Pinto and R. H. Villarreal, The minimum distance of parameterized codes on projective tori, Appl. Algebra Engrg. Comm. Comput. **22** (2011), no. 4, 249–264.

[56] E. Sarmiento, M. Vaz Pinto and R. H. Villarreal, On the vanishing ideal of an algebraic toric set and its parameterized linear codes, J. Algebra Appl. **11** (2012), no. 4, 1250072 (16 pages).

[57] T. Sauer, Polynomial interpolation in several variables: lattices, differences, and ideals, Stud. Comput. Math. **12** (2006), 191–230.

[58] H. G. Schaathun and W. Willems, A lower bound on the weight hierarchies of product codes, Discrete Appl. Math. **128** (2003), no. 1, 251–261.

[59] A. Sørensen, Projective Reed–Muller codes, IEEE Trans. Inform. Theory **37** (1991), no. 6, 1567–1576.

[60] R. Stanley, Hilbert functions of graded algebras, Adv. Math. **28** (1978), 57–83.

[61] B. Sturmfels, *Gröbner Bases and Convex Polytopes*, University Lecture Series **8**, American Mathematical Society, Rhode Island, 1996.

[62] W. V. Vasconcelos, *Computational Methods in Commutative Algebra and Algebraic Geometry*, Springer-Verlag, 1998.

[63] A. Tochimani and R. H. Villarreal, Vanishing ideals over rational parameterizations. Preprint, 2015, arXiv:1502.05451v1.

[64] A. Tochimani and R. H. Villarreal, Vanishing ideals generated by binomials, preprint, 2015.

[65] S. Tohăneanu, Lower bounds on minimal distance of evaluation codes, Appl. Algebra Engrg. Comm. Comput. **20** (2009), no. 5-6, 351–360.

[66] M. Tsfasman, S. Vladut and D. Nogin, *Algebraic geometric codes*: *basic notions*, Mathematical Surveys and Monographs **139**, American Mathematical Society, Providence, RI, 2007.

[67] J. H. van Lint, *Coding Theory*, Second printing, Lecture Notes in Mathematics, Vol. 201, Springer-Verlag, Berlin–New York, 1973.

[68] M. Vaz Pinto and R. H. Villarreal, The degree and regularity of vanishing ideals of algebraic toric sets over finite fields, Comm. Algebra **41** (2013), no. 9, 3376–3396.

[69] R. H. Villarreal, *Monomial Algebras*, Monographs and Textbooks in Pure and Applied Mathematics **238**, Marcel Dekker, New York, 2001.

[70] R. H. Villarreal, *Monomial Algebras, Second Edition*, Monographs and Research Notes in Mathematics, Chapman and Hall/CRC, 2015.

[71] V. K. Wei, Generalized Hamming weights for linear codes, IEEE Trans. Inform. Theory **37** (1991), no. 5, 1412–1418.

[72] V. K. Wei and K. Yang, On the generalized Hamming weights of product codes, IEEE Trans. Inform. Theory **39** (1993), no. 5, 1709–1713.

# Notation

# Index