Centro de Investigación y de Estudios Avanzados
del Instituto Politécnico Nacional

Unidad Zacatenco

Departamento de Matemáticas

Códigos de Tipo Reed-Muller

Tesis que presenta

Miguel Eduardo Uribe Paczka

para obtener el Grado de

Maestro en Ciencias

en la Especialidad de

Matemáticas

Directores de Tesis:

Dr. Rafael Heraclio Villarreal Rodríguez

Dr. Eliseo Sarmiento Rosales

Ciudad de México. Julio 2016.

Center for Research and Advanced Studies
of the National Polythechnic Institute
Campus Zacatenco
Department of Mathematics

Reed-Muller-Type Codes

A thesis presented by

Miguel Eduardo Uribe Paczka

to obtain the Degree of

Master of Science

in the Speciality of

Mathematics

Thesis Advisors:

Dr. Rafael Heraclio Villarreal Rodríguez

Dr. Eliseo Sarmiento Rosales

Mexico City. July 2016.

Acknowledgements

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

Resumen

Introducimos y estudiamos la familia de los códigos tipo Reed-Muller afines y proyectivos usando álgebra conmutativa, geometría algebraica y técnicas de bases de Gröbner. El primer capítulo está dedicado a introducir el material nesesario para estas tres áreas. En este primer capítulo vamos a estudiar variedades afines y proyectivas, bases de Gröbner y dimensión de una variedad. La definición que vamos a dar para la dimensión de una variedad es la misma que uno puede encontrar en un curso de geometría algebraica, posteriormente probaremos que para cualquier variedad V sobre un campo infinito, su dimensión es igual al grado del polinomio de Hilbert del ideal anulador $\mathbf{I}(V)$. En el segundo capítulo vamos a estudiar funciones de Hilbert, códigos de tipo Reed-Muller afines y proyectivos. En este segundo capítulo veremos que los códigos Reed-Muller afines son un caso particular de los proyectivos, por lo tanto estudiaremos los códigos Reed-Muller proyectivos en vez de los afines. En el tercer capítulo estudiaremos en detalle la familia de los códigos cartesianos afines introducida por López, Rentería y Villarreal, y daremos varios enfoques de cómo calcular los parametros básicos de este tipo de códigos lineales.

Abstract

We introduce and study the family of affine and projective Reed-Muller-type codes using Commutative Algebra, Algebraic Geometry and Gröbner basis techniques. The first chapter is devoted to introduce the necessary material from these three areas. In this first chapter we study affine and projective varieties, Gröbner basis and the dimension of a variety. The definition that we give for the dimension of a variety is the same that one can find in an algebraic geometry course, later we prove that for any variety V over an infinite field, its dimension is equal to the degree of the Hilbert polynomial of the vanishing ideal $\mathbf{I}(V)$. In the second chapter we study Hilbert functions, affine and projective Reed-Muller-type codes. In this second chapter we show that affine Reed-Muller-type codes are projective codes, so, we study the projective Reed-Muller-type codes instead of the affine codes. In the last chapter we study in detail the family of affine cartesian codes introduced by López, Rentería and Villarreal, and give an up to date account of the diverse approaches to compute the basic parameters of this type of linear codes.

Contents

Introduction

In Chapter 1 we introduce the theory of *Gröbner bases*, graded modules, projective closure, vanishing ideals, *Hilbert functions*, dimension of affine and projective varieties. In the first section of this chapter, we review the theory of modules, and in the second section we study affine varieties.

Definition 1.2.3 Let K be a field, and let $f_1, \ldots, f_s$ be polynomials in the polynomial ring $K[x_1, \ldots, x_n]$. Then we set

$$\mathbf{V}(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in K^n \mid f_i(a_1, \ldots, a_n) = 0 \ \forall\ 1 \leq i \leq s\}.$$

We call $\mathbf{V}(f_1, \ldots, f_s)$ the *affine variety* defined by $f_1, \ldots, f_s$.

We are going to prove that finite intersections and unions of affine varieties are again affine varieties. The empty set $\emptyset$ and the affine space K^n are both affine varieties, to see this note that $\emptyset = \mathbf{V}(1)$ and $K^n = \mathbf{V}(0)$. This properties say that we can define a topology on K^n by taking as the closed sets of the topology, the affine varieties. This topology on K^n is called the *Zariski topology.*

Definition 1.2.18 A non empty subset Y of a topological space X is called *irreducible* if it can not be written as the union of two proper closed subsets of Y (closed in Y). If Y is not irreducible we say that Y is *reducible.*

The irreducible varieties are going to be very important when we study the dimension of a variety. Next we introduce the vanishing ideal of any affine variety V, we are going to see that for any affine variety V, we can construct an ideal $\mathbf{I}(V)$, called the vanishing ideal of V.

Definition 1.2.11 Let $V \subseteq K^n$ an affine variety. Then we set

$$\mathbf{I}(V) = \{f \in K[x_1, \ldots, x_n] \mid f(a_1, \ldots, a_n) = 0 \ \forall\ (a_1, \ldots, a_n) \in V\}.$$

Clearly $\mathbf{I}(V)$ is an ideal, we will call $\mathbf{I}(V)$ the *vanishing ideal of* V.

We can ask ourselves whether $\mathbf{I}(V) = \langle f_1, \ldots, f_s \rangle$ for any affine variety $V = \mathbf{V}(f_1, \ldots, f_s)$, but the answer is that this equality is not true in general. By Hilbert-Nullstellensatz, if K is an algebraic closed field then

$$\mathbf{I}(V) = \sqrt{I},$$

where $I = \langle f_1, \ldots, f_s \rangle$. In the third section we study Gröbner bases. Monomials orders play an important role here, they are defined as follows:

Definition 1.3.1 A *monomial ordering* $>$ on $K[x_1, \ldots, x_n]$ is any relation on $\mathbb{Z}^n_{\geq 0}$, or equivalently, any relation on the set of monomials x^α, $\alpha \in \mathbb{Z}^n_{\geq 0}$, satisfying:

(i) $>$ is a total ordering on $\mathbb{Z}^n_{\geq 0}$.

(ii) If $\alpha > \beta$ and $\gamma \in \mathbb{Z}^n_{\geq 0}$, then $\alpha + \gamma > \beta + \gamma$.

(iii) $>$ is a well-ordering on $\mathbb{Z}^n_{\geq 0}$. This means that every nonempty subset of $\mathbb{Z}^n_{\geq 0}$ has a smallest element under $>$.

Definition 1.3.14 Fix a monomial order. A finite subset $G = \{g_1, \ldots, g_t\}$ of and ideal I is said to be a *Gröbner basis* (or standard basis) if

$$\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle,$$

where $LT(I)$ is the set of leading terms of I and $LT(g_i)$ are the leading terms of g_i.

Finally in the last two sections we study projective varieties and the dimension of a variety.

Definition 1.4.7 Let K be a field and let $f_1, \ldots, f_s \in K[x_0, \ldots, x_n]$ be homogeneous polynomials. We set

$$\mathbf{V}(f_1, \ldots, f_s) := \{[(a_0, \ldots, a_n)] \in \mathbb{P}^n_K \mid f_i(a_0, \ldots, a_n) = 0 \text{ for all } 1 \leq i \leq s\}.$$

We call $\mathbf{V}(f_1, \ldots, f_s)$ the *projective variety* defined by $f_1, \ldots, f_s$. $\mathbb{P}^n_K$ denotes the n-dimensional projective space over the field K. We can associate an ideal to any projective variety as in the case of affine varieties.

As before, finite unions of projective varieties are projective varieties and arbitrary intersections of projective varieties are again projective varieties. So, the projective varieties furnish us with the closed sets for a topology on $\mathbb{P}^n_K$, called the *Zariski topology* on $\mathbb{P}^n_K$.

For the dimension of a variety, the definition is the same that one studies in an algebraic geometry course. Then we will see that for any affine variety $\mathbf{V}(I)$, where I is a monomial ideal, the dimension of $\mathbf{V}(I)$ is equal to the maximum of the dimensions of the coordinate subspaces contained in $\mathbf{V}(I)$. This is a particular case of the next fact: Let $Y \subseteq K^n$ be an affine variety, we are going to prove that Y can be expressed as a finite union $Y = Y_1 \cup \cdots \cup Y_r$ of irreducible varieties Y_i. Then we will prove the equality:

$$\dim Y = \max \{ \dim Y_i \mid i = 1, \ldots, r\}.$$

In Chapter 2 we study the projective and the affine Reed-Muller type codes. In the first section we examine Hilbert functions, in this section we are going to prove that for any variety over an infinite field, its dimension is equal to the degree of the Hilbert polynomial. In the last section we prove that the affine Reed-Muller type codes are a special case of the projective Reed-Muller type codes.

Definition 2.1.2 Let I be and ideal in $K[x_1, \ldots, x_n]$. The *affine Hilbert function* of I is the function $HF_I^a : \mathbb{N} \cup \{0\} \to \mathbb{N} \cup \{0\}$ defined by

$$HF_I^a(s) = dim_K \; K[x_1, \ldots, x_n]_{\leq s}/I_{\leq s} = dim_K \; K[x_1, \ldots, x_n]_{\leq s} - \, dim_K \; I_{\leq s}.$$

Theorem 2.1.5 (Hilbert Theorem) Let I be an ideal in $K[x_1, \ldots, x_n]$. The affine Hilbert function of I can be written for s sufficiently large as

$$HF_I^a(s) = \sum_{i=0}^{d} b_i \binom{s}{d-i},$$

where the b_i are integers and b_0 is positive.

Definition 2.1.6 The polynomial which is equal to $HF_I^a(s)$ for s sufficiently large is called the *affine Hilbert polynomial* of I and is denoted $HP_I^a(s)$.

Proposition 2.1.11 Assume that K is an infinite field. If V and W are irreducible affine varieties in K^n, then

$$deg \; HP^a_{\mathbf{I}(V \cup W)} = max \; \{ \dim V, \dim W\}.$$

As a consequence of the last proposition we get that if V is an affine variety and $V = V_1 \cup \cdots \cup V_r$ is the decomposition of V into irreducible varieties, then

$$\deg \; HP^a_{\mathbf{I}(V)} = \max \{ \dim V_i \mid i = 1, \ldots, r\}.$$

The dimension of an affine variety $V \subseteq K^n$, is the degree of the affine Hilbert polynomial of the corresponding ideal $I = \mathbf{I}(V)$.

Theorem 2.1.12 (The Dimension Theorem) Let $V = \mathbf{V}(I)$ be an affine variety, where $I \subseteq K[x_1, \ldots, x_n]$ is an ideal. If K is algebraically closed, then

$$\dim V = deg \; HP_I^a.$$

Furthermore, if $>$ is a graded order on $K[x_1, \ldots, x_n]$, then

$$\begin{aligned}\dim V &= deg\ HP^{a}_{\langle LT(I)\rangle}\\ &= \text{maximum dimension of a coordinate subspace in } \mathbf{V}(\langle LT(I)\rangle).\end{aligned}$$

Finally, the last two equalities hold over any field K when $I = \mathbf{I}(V)$.

Let $I \subseteq K[x_0, \ldots, x_n]$ be a homogeneous ideal. Then the *Hilbert function* of I is defined by

$$HF_I(s) = dim_K\ K[x_0, \ldots, x_n]_s / I_s.$$

The Hilbert function can be written

$$HF_I(s) = \sum_{i=0}^{d} b_i \binom{s}{d-i},$$

for s sufficiently large. The polynomial on the right of this equation is called the Hilbert polynomial of I and is denoted $HP_I(s)$. As in the affine case, we will prove that the dimension of a projective variety $V \subseteq \mathbb{P}^n_K$ is equal to the degree of the Hilbert polynomial $HP_{\mathbf{I}(V)}$.

Theorem 2.1.15 (The Dimension Theorem) Let $V = \mathbf{V}(I) \subseteq \mathbb{P}^n_K$ be a projective variety, where $I \subseteq K[x_0, \ldots, x_n]$ is a homogeneous ideal. If V is nonempty and K is algebraically closed, then

$$\dim V = deg\ HP_I.$$

Furthermore, for any monomial order on $K[x_0, \ldots, x_n]$, we have

$$\dim V = deg\ HP_{\langle LT(I)\rangle} = \text{maximum dimension of a projective coordinate subspace in } \mathbf{V}(\langle LT(I)\rangle).$$

Finally, the last two equalities hold over any field K when $I = \mathbf{I}(V)$.

Projective Reed-Muller-Type Codes We introduce some basic notions from coding theory. Let $K = \mathbb{F}_q$ be the finite field with q elements. We consider the n-dimensional vector space $\mathbb{F}_q^n$ whose elements are n-tuples $a = (a_1, \ldots, a_n)$ with $a_i \in \mathbb{F}_q$.

A *linear code* C over the alphabet $\mathbb{F}_q$ is a linear subspace of $\mathbb{F}_q^n$. The elements of C are called codewords. We call n the *length* of the code C and $dim_{\mathbb{F}_q}\ C$ the *dimension* of the code C as an $\mathbb{F}_q$-vector space.

Let $\mathbb{Y}$ be a subset of $\mathbb{P}^{s-1}_K$. Fix a degree $d \geq 1$. Let $P_1, \ldots, P_m$ be a set of representatives for the points of $\mathbb{Y}$ with $m = |\mathbb{Y}|$. For each i there is $f_i \in S_d$ such that $f_i(P_i) \neq 0$. Indeed suppose $P_i = [(a_1, \ldots, a_s)]$, there is at least one j in $\{1, \ldots, s\}$ such that $a_j \neq 0$. Setting $f_i(t_1, \ldots, t_s) = t_j^d$ one has that $f_i \in S_d$ and $f_i(P_i) \neq 0$. The *evaluation map*, denoted by ev_d, is defined as:

$$\mathrm{ev}_d\colon S_d=K[t_1,\ldots,t_s]_d\to K^{|\mathbb{Y}|},\qquad f\mapsto\left(\frac{f(P_1)}{f_1(P_1)},\ldots,\frac{f(P_m)}{f_m(P_m)}\right).\tag{1}$$

The map ev_d is well-defined, i.e., it is independent of the set of representatives that we choose for the points of $\mathbb{Y}$. The map ev_d defines a linear map of K-vector spaces. The image of S_d under ev_d, denoted by $C_{\mathbb{Y}}(d)$, is called a *projective Reed-Muller-type code* of degree d over $\mathbb{Y}$. It is also called an *evaluation code* associated to $\mathbb{Y}$.

Affine Reed-Muller-Type Codes Let $K=\mathbb{F}_q$ be a finite field, let Y be a subset of K^s, and let $\mathbb{Y}$ be the projective closure of Y. As Y is finite, its projective closure is:

$$\mathbb{Y}=\{[(1,\alpha)]\,|\,\alpha\in Y\}\subset\mathbb{P}^s_K.$$

Let $S=K[x_1,\ldots,x_s]$ 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*

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

defines a linear map of K-vector spaces. The image of ev^a_d, 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. The kernel of ev^a_d is $\mathbf{I}(Y)_{\leq d}$. Thus $S_{\leq d}/\mathbf{I}(Y)_{\leq d}\cong C_Y(d)$. If Y is a subset of K^s it is usual to denote the affine Hilbert function of $\mathbf{I}(Y)$ by H^a_Y. In our situation one has $H^a_Y(d)=\dim_K C_Y(d)$.

In the last chapter we study two particular cases of affine Reed-Muller-type codes, one of them is when:

$$Y:=\{(x_1^{v_{11}}\cdots x_n^{v_{1n}},\ldots,x_1^{v_{s1}}\cdots x_n^{v_{sn}})\in K^s|\,x_i\in K^*\text{ for all }i\},$$

where $K^*=K\setminus\{0\}$ and $v_i=(v_{i1},\ldots,v_{in})\in\mathbb{N}^n$. We call $Y=X^*$ an *affine algebraic toric set* parameterized by $x^{v_1},\ldots,x^{v_s}$. The set X^* is a multiplicative group under componentwise multiplication. We give an algebraic method, using Gröbner bases, to compute the length and the dimension of $C_{X^*}(d)$, the parameterized affine code of degree d on the set X^*. Later we will prove the next theorem:

Theorem 3.1.4 Let $B=K[t_1,\ldots,t_s,y_1,\ldots,y_n]$ be a polynomial ring over a finite field K with q elements. Then

$$\mathbf{I}(X^*)=\left(t_1-y^{v_1},\ldots,t_s-y^{v_s},y_1^{q-1}-1,\ldots,y_n^{q-1}-1\right)\cap S$$

and $\mathbf{I}(X^*)$ is a binomial ideal.

The other affine Reed-Muller-type code is when Y is a cartesian product:

$$Y:=A_1\times\cdots\times A_n\subset K^n,$$

where $A_1,\ldots,A_n$ is a collection of non-empty subsets of K with a finite number of elements. The main result of this section is the next theorem:

Theorem 3.2.11 [21] Let K be a field and let $C_{X^*}(d)$ be the cartesian evaluation code of degree d on the finite set $X^* = A_1 \times \cdots \times A_n \subset K^n$. If $2 \leq d_i \leq d_{i+1}$ for all i, with $d_i = |A_i|$, and $d \geq 1$, then the minimum distance of $C_{X^*}(d)$ is given by

$$\delta_{X^*}(d) = \begin{cases} (d_{k+1} - \ell)\, d_{k+2} \cdots d_n & \text{if } d \leq \sum\limits_{i=1}^{n} (d_i - 1) - 1, \\ 1 & \text{if } d \geq \sum\limits_{i=1}^{n} (d_i - 1), \end{cases}$$

where $k \geq 0$, ℓ are the unique integers such that $d = \sum_{i=1}^{k} (d_i - 1) + \ell$ and $1 \leq \ell \leq d_{k+1} - 1$.

In a very recent paper, Bishnoi, Clark, Potukuchi and Schmitt give another proof of the formula ([4], Theorem 5.2) for $\delta_{X^*}(d)$ using a result of Alon and Fürendi [2], Theorem 5. Another proof of this formula using Gröbner bases can be found in [6], Proposition 2.3 and in [22].

As a consequence of Theorem 3.2.11 we get the next corollary:

Corollary 3.2.12 Let $K = \mathbb{F}_q$ be a finite field with $q \neq 2$ elements. If $\mathbb{T}$ is a projective torus in $\mathbb{P}^n$ and $d \geq 1$, then the minimum distance of $C_{\mathbb{T}}(d)$ is given by

$$\delta_{\mathbb{T}}(d) = \begin{cases} (q-1)^{n-k-1}(q-1-\ell) & \text{if} \quad d \leq (q-2)n - 1, \\ 1 & \text{if} \quad d \geq (q-2)n, \end{cases}$$

where k and ℓ are the unique integers such that $k \geq 0$, $1 \leq \ell \leq q-2$ and $d = k(q-2) + \ell$.

Chapter 1

Preliminaries: Varieties, Gröbner Bases and Commutative Algebra

The main topics of this chapter are *Gröbner bases*, graded modules, projective closure, vanishing ideals, *Hilbert functions*, dimension of affine and projective varieties. In this work, unless otherwise stated, by a *ring* we shall always mean a commutative ring with unit. Some classical results, like the Nullstellensatz, Buchbergers's criterion for Gröbner basis, will be introduced here.

1.1 Module and ring theory

We will denote a polynomial ring in several variables by $K[x_1, \dots, x_n]$ and a polynomial ring in one variable by $K[x]$. The letter K will always denote a field.

Definition 1.1.1. A *monomial* in $x_1, \dots, x_n$ is a product of the form

$$x_1^{\alpha_1} \cdots x_n^{\alpha_n},$$

where all the exponents $\alpha_1, \dots, \alpha_n$ are nonnegative integers. The *total degree* of this monomial is the sum $\alpha_1 + \cdots + \alpha_n$.

We can simplify the notation for monomials as follows: let $\alpha = (\alpha_1, \dots, \alpha_n)$ be an n-tuple of nonnegative integers. Then we set

$$x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}.$$

When $\alpha = (0, \dots, 0)$, note that $x^\alpha = 1$. We also let $|\alpha| = \alpha_1 + \cdots + \alpha_n$ denote the total degree of the monomial x^α.

Definition 1.1.2. Let $f = \displaystyle\sum_\alpha a_\alpha x^\alpha \in K[x_1, \dots, x_n]$.

(i) We call a_α the *coefficient* of the monomial x^α.

(ii) If $a_\alpha \neq 0$, then we call $a_\alpha x^\alpha$ a *term* of f.

(iii) The *total degree* of f, denoted $\deg(f)$, is the maximum $|\alpha|$ such that the coefficient a_α is nonzero.

A polynomial $f \in K[x_1, \ldots, x_n]$ is *homogeneous* of total degree k provided that every term appearing in f has total degree k. An important fact is that every polynomial can be written uniquely as a sum of homogeneous polynomials. Namely, given $f \in K[x_1, \ldots, x_n]$, let f_k be the sum of all terms of f of total degree k. Then each f_k is homogeneous and $f = \sum\limits_k f_k$. We call f_k the kth *homogeneous component* of f.

Definition 1.1.3. An ideal I in $K[x_1, \ldots, x_n]$ is said to be *homogeneous* if for each $f \in I$, the homogeneous components f_i of f are in I as well.

It is easy to check that an ideal I is homogeneous if and only if I is generated by homogeneous polynomials. Given an ideal I in $K[x_1, \ldots, x_n]$, we know that exists $f_1, \ldots, f_s$ in $K[x_1, \ldots, x_n]$ such that $I = (f_1, \ldots, f_s)$, where $(f_1, \ldots, f_s)$ is the ideal generated by $f_1, \ldots, f_s$. We say that $f_1, \ldots, f_s$ are a basis of I.

The *prime spectrum* of a ring R, denoted by $\operatorname{Spec}(R)$, is the set of prime ideals of R. The *minimal primes* of R are the minimal elements of $\operatorname{Spec}(R)$ with respect to inclusion and the maximal ideals of R are the maximal elements of the set of proper ideals of R with respect to inclusion.

Let R be a ring and let $X = \operatorname{Spec}(R)$ be its prime spectrum. Given an ideal I of R, the set of all prime ideals of R containing I will be denoted by $V(I)$. The *minimal primes* of I are the minimal elements of $V(I)$ with respect to inclusion. The pair $(X, \mathcal{Z})$ is a topological space, where $\mathcal{Z}$ is the family of open sets of X, and where U is in $\mathcal{Z}$ iff $U = X \setminus V(I)$, for some ideal I. To see this, notice the following:

- $V((0)) = X$ and $V((1)) = \emptyset$, so $X, \emptyset \in \mathcal{Z}$.
- Let $\{U_\alpha\}_{\alpha \in J}$ be any family of elements of $\mathcal{Z}$, then $U_\alpha = V(I_\alpha)^c$, where I_α is an ideal of R. Therefore

$$\bigcup_{\alpha \in J} U_\alpha = \bigcup_{\alpha \in J} V(I_\alpha)^c = \left(\bigcap_{\alpha \in J} V(I_\alpha) \right)^c = (V(H))^c,$$

  where H is the ideal of R generated by $\bigcup\limits_{\alpha \in J} I_\alpha$. Therefore $\bigcup\limits_{\alpha \in J} U_\alpha \in \mathcal{Z}$.

- Now, let U, V elements of $\mathcal{Z}$, then $U = V(I_1)^c$ and $V = V(I_2)^c$, where I_1 and I_2 are ideals of R. Then

$$U \cap V = V(I_1)^c \cap V(I_2)^c = (V(I_1) \cup V(I_2))^c = V(I_1 \cap I_2)^c.$$

This topology is called the *Zariski topology* of the prime spectrum of R.

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

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

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

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

which end at $\mathfrak{p}$. Note $\dim(R_\mathfrak{p}) = \mathrm{ht}\,(\mathfrak{p})$, where $R_\mathfrak{p}$ is the localization of R at $\mathfrak{p}$. If I is an ideal of R, then $\mathrm{ht}\,(I)$, the *height* of I , is defined as

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

In general $\dim(R/I) + \mathrm{ht}\,(I) \leq \dim(R)$. Suppose that $\mathrm{ht}(I) = \mathrm{ht}\,(\tilde{\mathfrak{p}})$ where $I \subseteq \tilde{\mathfrak{p}}$ and $\tilde{\mathfrak{p}} \in \mathrm{Spec}(R)$. Let $\dim(R/I) = n$ and $\mathrm{ht}\,(\tilde{\mathfrak{p}}) = m$, now let

$$\tilde{\mathfrak{p}_0} \subseteq \cdots \subseteq \tilde{\mathfrak{p}_n}$$

be a chain of prime ideals of R/I. We know that for all $i \in \{0, \ldots, n\}$, $\tilde{\mathfrak{p}_i} = \mathfrak{p}_i/I$ where $I \subseteq \mathfrak{p}_i$ and $\mathfrak{p}_i \in \mathrm{Spec}(R)$. The condition $\tilde{\mathfrak{p}_0} \subseteq \cdots \subseteq \tilde{\mathfrak{p}_n}$ implies,

$$I \subseteq \mathfrak{p}_0 \subseteq \cdots \subseteq \mathfrak{p}_n.$$

Let $\mathfrak{q}_0 \subseteq \cdots \subseteq \mathfrak{q}_m = \tilde{\mathfrak{p}}$ a chain of prime ideals that ends at $\tilde{\mathfrak{p}}$. As $I \subseteq \mathfrak{p}_0$, so $\mathrm{ht}\,(\tilde{\mathfrak{p}}) \leq \mathrm{ht}\,(\mathfrak{p}_0)$, therefore

$$n + \mathrm{ht}\,(\mathfrak{p}_0) \leq \dim(R).$$

We conclude that $n + m \leq \dim(R)$. The difference $\dim(R) - \dim(R/I)$ is called the *codimension* of I and $\dim(R/I)$ is called the *dimension* of I.

Let M be an R-module. The *annihilator* of M is given by

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

Note that $\mathrm{ann}_R(M)$ is an ideal of R. If $m \in M$ the *annihilator* of m is $\mathrm{ann}\,(m) = \mathrm{ann}\,(Rm)$. It is convenient to generalize the notion of annihilator to ideals and submodules. Let N_1 and N_2 be submodules of M, their *ideal quotient* or *colon ideal* is defined as

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

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

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

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

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

Let I be an ideal of the ring R, S a nonempty subset of M. Then

$$IS = \left\{ \sum_{i=1}^{n} r_i a_i \mid r_i \in I; a_i \in S; n \in \mathbb{N} \right\},$$

is a submodule of M. Let $\{B_i\}_{i \in I}$ a family of submodules of M, then the submodule generated by $\bigcup_{i \in I} B_i$ is called the sum of the modules B_i. If the index set I is finite, the sum of $B_1, \ldots, B_n$ is denoted $B_1 + \cdots + B_n$.

Proposition 1.1.4. *Let M an R-module and $\{B_i\}_{i \in I}$ a family of submodules of M such that,*

(a) *M is the sum of the family $\{B_i\}_{i \in I}$;*

(b) *for each $k \in I$, $B_k \cap B_k^* = \{0\}$, where B_k^* is the sum of the family $\{B_i \mid i \neq k\}$.*

Then there is an isomorfism $M \cong \sum_{i \in I} B_i$, where $\sum_{i \in I} B_i$ is the (external) direct sum of the family $\{B_i\}_{i \in I}$.

Proof. [19], page 175. □

A module M is said to be the *(internal) direct sum* of a family of submodules $\{B_i\}_{i \in I}$ provided that M and $\{B_i\}_{i \in I}$ satisfy the hypotheses of the last theorem. We write $M = \bigoplus_{i \in I} B_i$ to indicate that the module M is the internal direct sum of the family of submodules $\{B_i\}_{i \in I}$.

Definition 1.1.5. Let M be an R-module. A sequence $\underline{\theta} = \theta_1, \ldots, \theta_n$ in R is called a *regular sequence* of M or an *M-regular sequence* if $(\underline{\theta})M \neq M$ and $\theta_i \notin \mathcal{Z}(M/(\theta_1, \ldots, \theta_{i-1})M)$ for all i. Note that $(\underline{\theta})$ and $(\theta_1, \ldots, \theta_{i-1})$ are the ideals generated by $\underline{\theta}$ and $\{\theta_1, \ldots, \theta_{i-1}\}$.

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

Definition 1.1.6. An R-module M is called *Cohen–Macaulay* (C–M for short) if $\operatorname{depth}(M)$ is equal to $\dim(M)$, or if $M = (0)$.

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

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

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

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

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

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

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

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

Proposition 1.1.7. [23, p. 92] *Let $M = \oplus_{a \in H} M_a$ be an H-graded module and $N \subset M$ a submodule. Then the following conditions are equivalent:*

(g_1) *N is generated over R by homogeneous elements.*

(g_2) *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.*

(g_3) *N is a graded submodule of M.*

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

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

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

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

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

Definition 1.1.8. The *standard grading* or *usual grading* of a polynomial ring $K[x_1, \ldots, x_n]$ is the $\mathbb{N}$-grading induced by setting $\deg(x_i) = 1$ for all i.

1.2 Affine varieties

Definition 1.2.1. Given a field K and a positive integer n, we define the *n-dimensional affine space* over K to be the set

$$K^n = \{(a_1, \ldots, a_n) \mid a_i \in K \; \forall i \in \{1, \ldots, n\}\}.$$

We call $K^1 = K$ the *affine line* and K^2 the *affine plane.* Let us next see how polynomials relate to the affine space. Let $f = \sum_\alpha a_\alpha x^\alpha \in K[x_1, \ldots, x_n]$, the polynomial f gives a function,

$$\begin{aligned} \tilde{f} : K^n &\to K \\ (a_1, \ldots, a_n) &\to f(a_1, \ldots, a_n). \end{aligned}$$

This dual nature of polynomials has some unexpected consequences. For example, the question is $\tilde{f} = 0$? now has two potential meanings: is f the zero polynomial?, which means that all of its coefficients a_α are zero, or is $\tilde{f}$ the zero function?. The surprising fact is that these two statements are not equivalent in general. For example, consider the field $\mathbb{F}_2$. Now consider the polynomial $x^2 - x \in \mathbb{F}_2[x]$. Since this polynomial vanishes at 0 and 1, we found a nonzero polynomial which gives the zero function on the affine line. However, as long as K is infinite, there is no problem.

Proposition 1.2.2. *Let K an infinite field, and let $f \in K[x_1, \ldots, x_n]$. Then $f = 0$ in $K[x_1, \ldots, x_n]$ if and only if $\tilde{f}$ is the zero function.*

Proof. [7], page 3. □

Definition 1.2.3. Let K be a field, and let $f_1, \ldots, f_s$ be polynomials in $K[x_1, \ldots, x_n]$. Then we set

$$\mathbf{V}(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in K^n \mid f_i(a_1, \ldots, a_n) = 0 \; \forall \; 1 \leq i \leq s\}.$$

We call $\mathbf{V}(f_1, \ldots, f_s)$ the *affine variety* defined by $f_1, \ldots, f_s$.

Remark 1.2.4. *An affine variety $\mathbf{V}(f_1, \ldots, f_s) \subseteq K^n$ is the set of all solutions of the system of equations $f_1(x_1, \ldots, x_n) = \cdots = f_s(x_1, \ldots, x_n) = 0$. We will use the letters V, W, etc. to denote affine varieties.*

Example 1.2.5. *Let K a field and consider a system of m linear equations in n unknowns $x_1, x_2, \ldots, x_n$ with coefficients in K:*

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= b_1 \\ &\vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n &= b_m. \end{aligned}$$

The solutions of these equations form an affine variety in K^n, which we will call a linear variety. Thus, lines and planes are linear varieties.

Example 1.2.6. *Consider the set*

$$R = \{(x, y) \in \mathbb{R}^2 \mid y > 0\}.$$

We are going to prove that R is not an affine variety. Suppose that $R = \mathbf{V}(f_1, \ldots, f_s)$ where $f_i \in \mathbb{R}[x, y]$ for all $i \in \{1, \ldots, s\}$. Then each f_i vanishes on R, and if we can show that f_i also vanishes at $(0, 0)$, we will get the desired contradiction. Let $f \in \mathbb{R}[x, y]$ a polynomial that vanishes on R. Let $g(t) = f(t, t) \in \mathbb{R}[t]$. Consider the sequence $x_n = 1/n$. For the continuity of the polynomial g, we have

$$f(0, 0) = g(0) = \lim_{n\to\infty} g(x_n) = \lim_{n\to\infty} f(x_n, x_n) = 0.$$

Lemma 1.2.7. *If $V, W \subseteq K^n$ are affine varieties, then so are $V \cup W$ and $V \cap W$.*

Proof. Suppose that $V = \mathbf{V}(f_1, \ldots, f_s)$ and $W = \mathbf{V}(g_1, \ldots, g_t)$. Then we claim that

$$V \cap W = \mathbf{V}(f_1, \ldots, f_s, g_1, \ldots, g_t)$$
$$V \cup W = \mathbf{V}(f_i g_j \mid 1 \leq i \leq s, 1 \leq j \leq t).$$

The first equality is trivial to prove: being in $V \cup W$ means that both $f_1, \ldots, f_s$ and $g_1, \ldots, g_t$ vanish, which is the same as $f_1, \ldots, f_s, g_1, \ldots, g_t$ vanishing.

If $(a_1, \ldots, a_n) \in V$ we have $f_i(a_1, \ldots, a_n) = 0$ for all i, which implies that $f_i g_j$ vanish at $(a_1, \ldots, a_n)$ for all $(i, j) \in \{1, \ldots, s\} \times \{1, \ldots, t\}$. Thus, $V \subseteq \mathbf{V}(f_i g_j)$, and $W \subseteq \mathbf{V}(f_i g_j)$ follows similarly. This proves that $V \cup W \subseteq \mathbf{V}(f_i g_j)$. Going the other way, let $a = (a_1, \ldots, a_n) \in \mathbf{V}(f_i g_j)$. If $a \in V$ we have finished, suppose that $a \notin V$, then $f_{i_0}(a_1, \ldots, a_n) \neq 0$ for some i_0. Since $f_{i_0} g_j$ vanishes at a for all j, we have $a \in W$. This shows that $\mathbf{V}(f_i g_j) \subseteq V \cup W$. □

Example 1.2.8. *A single point $a = (a_1, \ldots, a_n) \in K^n$ is an affine variety. Let $f_i(x_1, \ldots, x_n)$ be the polynomial $x_i - a_i$ where $1 \leq i \leq n$. Clearly $\{a\} = \mathbf{V}(f_1, \ldots, f_n)$. It follows from the last lemma that every finite subset of K^n is an affine variety.*

We discuss now the problem of describing the points of an affine variety $\mathbf{V}(f_1, \ldots, f_s)$. This reduces to asking whether there is a way to write down the solutions of the system of polynomials equations $f_1 = \cdots = f_s = 0$. To get started, let us look an example. Consider the system of equations

$$2x + 3y - z = 9.$$
$$x - y = 1.$$
$$3x + 7y - 2z = 17.$$

Geometrically, this represents the intersection of 3 planes. To describe the solutions, we use row operations on the last system to obtain the equivalent equations

$$\begin{aligned} x - \tfrac{1}{5}z &= \tfrac{12}{5}. \\ y - \tfrac{1}{5}z &= \tfrac{7}{5}. \end{aligned}$$

Letting $z = t$, where t is arbitrary, this implies that all solutions are given by

$$\begin{aligned} x &= \tfrac{12+t}{5}, \\ y &= \tfrac{7+t}{5}, \\ z &= t, \end{aligned}$$

as t varies over $\mathbb{R}$. We call t a parameter, and the last equations are, thus, a parametrization of the solutions of the system. Let us look at the example of the unit circle $x^2+y^2 = 1$. A common way to parametrize the circle is using trigonometric functions: $x = cos(t)$, $y = sin(t)$.

Now suppose that we are given a variety $V = \mathbf{V}(f_1 \ldots, f_s) \subseteq K^n$. Then a *rational parametric representation* of V consists of rational functions $r_1, \ldots, r_n \in K(t_1, \ldots, t_m)$ such that the points given by

$$\begin{aligned} x_1 &= r_1(t_1, \ldots, t_m), \\ &\vdots \\ x_n &= r_n(t_1, \ldots, t_m), \end{aligned}$$

lie in V. By contrast, the original defining equations $f_1 = \cdots = f_s = 0$ of V are called an *implicit representation* of V.

Example 1.2.9. *Consider the sphere $x^2+y^2+z^2 = 1$ in 3-dimensional space. Let $(u, v, 0)$ a point in the xy-plane. The line connecting the north pole $(0, 0, 1)$ to $(u, v, 0)$ is given by*

$$\{(1 - t)(0, 0, 1) + t(u, v, 0) \mid t \in \mathbb{R}\} = \{(tu, tv, 1 - t) \mid t \in \mathbb{R}\}.$$

Replacing $x = tu$, $y = tv$ and $z = 1 - t$ into the equation for the sphere, we obtain

$$\begin{aligned} x &= \tfrac{2u}{u^2+v^2+1} \\ y &= \tfrac{2v}{u^2+v^2+1} \\ z &= \tfrac{u^2+v^2-1}{u^2+v^2+1} \end{aligned}$$

The desirability of having both types of representations leads to the following two questions:

- (Parametrization) Does every affine variety have a rational parametric representation?

- (Implicitization) Given a parametric representation of an affine variety, can we find the defining equations (i.e., can we find an implicit representation)?

The answer to the first question is no. In fact, most affine varieties cannot be parametrized in the sense described here. For the second question the the answer is always yes.

Proposition 1.2.10. *If $f_1, \ldots, f_s$ and $g_1, \ldots, g_t$ are bases of the same ideal in $K[x_1, \ldots, x_n]$, so that $(f_1, \ldots, f_s) = (g_1, \ldots, g_t)$, then $\mathbf{V}(f_1, \ldots, f_s) = \mathbf{V}(g_1, \ldots, g_t)$.*

Proof. [7], page 32. □

Definition 1.2.11. Let $V \subseteq K^n$ an affine variety. Then we set

$$\mathbf{I}(V) = \{f \in K[x_1, \ldots, x_n] \mid f(a_1, \ldots, a_n) = 0 \ \forall \ (a_1, \ldots, a_n) \in V\}$$

Clearly $\mathbf{I}(V)$ is an ideal, we will call $\mathbf{I}(V)$ the *ideal of V*.

Example 1.2.12. *Let K a field. Consider the variety $\{(0,0)\}$. We claim that $\mathbf{I}(\{(0,0)\}) = (x, y)$. Clearly $(x, y) \subseteq \mathbf{I}(\{(0,0)\})$. Let $f \in \mathbf{I}(\{(0,0)\})$. Then*

$$f = \sum_{(i,j) \neq (0,0)} a_{ij} x^i y^j = \left(\sum_{\substack{(i,j) \\ i>0}} a_{ij} x^{i-1} y^j \right) x + \left(\sum_{j>0} a_{0j} y^{j-1} \right) y \in (x, y).$$

Example 1.2.13. *Let K a field. Consider the variety $V = \mathbf{V}(x - y) = \{(t,t) \mid t \in K\}$. We are going to show that $\mathbf{I}(V) = (x - y)$. Clearly we have $(x - y) \subseteq \mathbf{I}(V)$. Let $f \in \mathbf{I}(V)$. Consider $K[x, y] = k[y][x]$. The polynomial $x - y \in K[y][x]$ is monic, so, for the division algorithm we can write*

$$f(x, y) = (x - y)q(x, y) + r(x, y).$$

Where $r(x, y) = 0$ or the degree of $r(x, y)$ in x is less than 1. Suppose that the degree of $r(x, y)$ in x is less than 1, then $r(x, y) = r(y)$. We have that f vanishes at V, therefore $r(t) = 0$ for all $t \in K$. This argument shows that $f \in (x - y)$.

Lemma 1.2.14. *If $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$, then $(f_1, \ldots, f_s) \subseteq \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$, although equality need not occur.*

Proof. [7], page 34. □

For the second part of the lemma, consider $(x^m, y^n) \subseteq \mathbf{I}(\mathbf{V}(x^m, y^n))$, where n and m are positive integers, consider $m \geq 2$. Note that $\mathbf{V}(x^m, y^n) = \{(0,0)\}$, therefore $\mathbf{I}(\mathbf{V}(x^m, y^n)) = (x, y)$. Note that $x \notin (x^m, y^n)$.

Proposition 1.2.15. *Let V and W be affine varieties in K^n. Then:*

(i) *$V \subseteq W$ if and only if $\mathbf{I}(W) \subseteq \mathbf{I}(V)$.*

(ii) *$V = W$ if and only if $\mathbf{I}(W) = \mathbf{I}(V)$.*

Proof. [7], page 35. □

Let $I \subseteq K[x_1, \ldots, x_n]$ be an ideal. We will denote by $\mathbf{V}(I)$ the set

$$\mathbf{V}(I) = \{(a_1, \ldots, a_n) \mid f(a_1, \ldots, a_n) = 0 \; \forall f \in I\}.$$

We will see that every ideal $I \subseteq K[x_1, \ldots, x_n]$ has a finite generating set, then $\mathbf{V}(I)$ is an affine variety. In particular, if $I = \langle f_1, \ldots, f_s \rangle$, then $\mathbf{V}(I) = \mathbf{V}(f_1, \ldots, f_s)$.

We extend this notation to any family $T \subseteq K[x_1, \ldots, x_n]$ as follows:

$$\mathbf{V}(T) = \{(a_1, \ldots, a_n) \mid f(a_1, \ldots, a_n) = 0 \; \forall f \in T\}.$$

Remark 1.2.16. *It is easy to show that if $T \subseteq K[x_1, \ldots, x_n]$ and $\langle T \rangle$ is the ideal generated by T then*

$$\mathbf{V}(T) = \mathbf{V}(\langle T \rangle).$$

The zeros of any set of polynomials is always the same as the zeros of a finite set of polynomials.

We know that finite intersections and unions of affine varieties are again affine varieties. The $\emptyset$ and K^n are both affine varieties, to see this note that $\emptyset = \mathbf{V}(1)$ and $K^n = \mathbf{V}(0)$. These properties say that we can define a topology on K^n by taking as the closet sets of the topology, the affine varieties. This topology on K^n is called the *Zariski topology.*

Example 1.2.17. *Consider K^1, the affine line over K. To study the Zariski topology on this space we need to know the form of the ideals in $A = k[x]$. This ring is a PID, so every ideal is principal. Let $I = \langle f \rangle$. Since A is a UFD we can write*

$$f(x) = p_1(x)^{\alpha_1} \cdots p_r(x)^{\alpha_r}.$$

Where the $p_i(x)$ are irreducible polynomials in A. Suppose that K is algebraically closed, we must have $p_i(x) = a_i x + b_i$ with $a_i \neq 0$ and $b_i \in K$. Hence

$$\mathbf{V}(f) = \left\{ -\left(\frac{b_1}{a_1}\right), \ldots, -\left(\frac{b_r}{a_r}\right) \right\}.$$

The affine varieties of K^1 are finite subsets of K^1. Conversely, if $\mathcal{F} = \{r_1, \ldots, r_s\}$ is a finite subset of K^1 then $\mathcal{F} = \mathbf{V}(f)$ for some polynomial $f \in A$ (namely $f = (x - r_1) \cdots (x - r_s)$).

Definition 1.2.18. A non empty subset Y of the topological space X is called *irreducible* if it can not be written as the union of two proper closed subsets of Y (closed in Y). If Y is not irreducible we say that Y is *reducible.*

Example 1.2.19. *K^1 is irreducible, if K is algebraically closed. This is so since if K is algebraically closed it must be infinite. But, the closed sets are all finite. So, in fact, any infinite subset of K^1 is irreducible.*

Proposition 1.2.20. (i) *$I_1 \subseteq I_2 \subseteq K[x_1, \dots, x_n]$ implies that $\mathbf{V}(I_2) \subseteq \mathbf{V}(I_1)$.*

(ii) *$Y_1 \subseteq Y_2 \subseteq K^n$ implies that $\mathbf{I}(Y_2) \subseteq \mathbf{I}(Y_1)$.*

(iii) *$\mathbf{I}(Y_1 \cup Y_2) = \mathbf{I}(Y_1) \cap \mathbf{I}(Y_2)$.*

Proof. The proofs of parts (*i*) and (*ii*) are easy to see. To prove part (*iii*), let $f \in \mathbf{I}(Y_1 \cup Y_2)$, then $f(a) = 0$ for all $a \in Y_1$ and for all $a \in Y_2$. It follows that $f \in \mathbf{I}(Y_1) \cap \mathbf{I}(Y_2)$.

Let $f \in \mathbf{I}(Y_1) \cap \mathbf{I}(Y_2)$ and $a \in Y_1 \cup Y_2$, then $a \in Y_1$ or $a \in Y_2$. If $a \in Y_1$ we have that $f(a) = 0$, similar if $a \in Y_2$. Therefore $\mathbf{I}(Y_1 \cup Y_2) = \mathbf{I}(Y_1) \cap \mathbf{I}(Y_2)$. □

Theorem 1.2.21. (Hilbert Nullstellensatz) *Let K be an algebraically closed field and $I \subseteq K[x_1, \dots, x_n]$. Then $f \in \mathbf{I}(\mathbf{V}(I))$ if and only if there is a positive integer r such that $f^r \in I$, i.e.,*

$$\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}.$$

So, if I is a radical ideal (i.e. equal to its radical) then we have

$$\mathbf{I}(\mathbf{V}(I)) = I.$$

Proof. [7], page 176. □

Proposition 1.2.22. *Let $Y \subseteq K^n$, then*

$$\mathbf{V}(\mathbf{I}(Y)) = \overline{Y} \text{ (closure of } Y\text{)}.$$

Proof. $\mathbf{V}(\mathbf{I}(Y))$ is a closed set, by definition, and it contains Y, hence it contains $\overline{Y}$. So, it suffices to prove that

$$\mathbf{V}(\mathbf{I}(Y)) \subseteq \overline{Y}.$$

So, let W be any closed set which contains Y, we will show that $\mathbf{V}(\mathbf{I}(Y)) \subseteq W$ and that will be enough to prove the theorem. Now, since W is closed we can write $W = \mathbf{V}(J)$ for some ideal J. Then we have $Y \subseteq \mathbf{V}(J)$, which in turn implies that $\mathbf{I}(\mathbf{V}(J)) \subseteq \mathbf{I}(Y)$. But $J \subseteq \mathbf{I}(\mathbf{V}(J))$, i.e. $J \subseteq \mathbf{I}(Y)$. Therefore

$$\mathbf{V}(\mathbf{I}(Y)) \subseteq \mathbf{V}(J) = W,$$

which is what we wanted to show. □

Theorem 1.2.23. *An affine variety $Y \subseteq K^n$ is irreducible if and only if $\mathbf{I}(Y)$ is a prime ideal.*

Proof. [18], page 4. □

1.3 Gröbner bases

In this part we review some basic facts and definitions on Gröbner bases.

Note that we can reconstruct the monomial $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ from the n-tuple of exponents $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$. This observation establishes a one-to-one correspondence between the monomials in $K[x_1, \ldots, x_n]$ and $\mathbb{Z}^n_{\geq 0}$. Furhermore, any ordering $>$ we establish on the space $\mathbb{Z}^n_{\geq 0}$ will give us an ordering on monomials: if $\alpha > \beta$ according to this ordering, we will also say that $x^\alpha > x^\beta$.

There are many different ways to define orderings on $\mathbb{Z}^n_{\geq 0}$. For our purposes, most of these orderings will not be useful, however, since we will want our orderings to be compatible with the algebraic structure of the polynomial rings.

Definition 1.3.1. A *monomial ordering* $>$ on $K[x_1, \ldots, x_n]$ is any relation on $\mathbb{Z}^n_{\geq 0}$, or equivalently, any relation on the set of monomials x^α, $\alpha \in \mathbb{Z}^n_{\geq 0}$, satisfying:

(i) $>$ is a total ordering on $\mathbb{Z}^n_{\geq 0}$.

(ii) If $\alpha > \beta$ and $\gamma \in \mathbb{Z}^n_{\geq 0}$, then $\alpha + \gamma > \beta + \gamma$.

(iii) $>$ is a well-ordering on $\mathbb{Z}^n_{\geq 0}$. This means that every nonempty subset of $\mathbb{Z}^n_{\geq 0}$ has a smallest element under $>$.

Lemma 1.3.2. *An order relation $>$ on $\mathbb{Z}^n_{\geq 0}$ is a well ordering if and only if every strictly decreasing sequence in $\mathbb{Z}^n_{\geq 0}$*

$$\alpha_1 > \alpha_2 > \cdots$$

eventually terminates.

Proof. [7], page 55. □

We will see that given parts (i) and (ii) in Definition 1.3.1, the well-ordering condition of part (iii) is equivalent to $\alpha \geq 0$ for all $\alpha \in \mathbb{Z}^n_{\geq 0}$.

- (*Lexicographic Order*). Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{lex} \beta$ if, in the vector difference $\alpha - \beta \in \mathbb{Z}^n$, the leftmost nonzero entry is positive. We will write $x^\alpha >_{lex} x^\beta$ if $\alpha >_{lex} \beta$.

  The variables $x_1, \ldots, x_n$ are ordered in the usual way by the lex ordering:

  $$(1, 0, \ldots, 0) >_{lex} (0, 1, 0, \ldots, 0) >_{lex} \cdots >_{lex} (0, \ldots, 0, 1).$$

  So $x_1 >_{lex} \cdots >_{lex} x_n$.

- (*Graded Lex Order*). Let $\alpha = (\alpha_1, \ldots, \alpha_n)$, $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{grlex} \beta$ if

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i, \text{ or } |\alpha| = |\beta| \text{ and } \alpha >_{lex} \beta.$$

- (*Graded Reverse Lex Order*). Let $\alpha = (\alpha_1, \dots, \alpha_n)$, $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{grevlex} \beta$ if

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i, \text{ or } |\alpha| = |\beta| \text{ and the rightmost nonzero entry of } \alpha - \beta \in \mathbb{Z}^n \text{ is negative.}$$

It is easy to check that the lex, grlex and grevlex orderings on $\mathbb{Z}^n_{\geq 0}$ are monomial orderings.

Definition 1.3.3. Let $f = \sum_{\alpha} a_\alpha x^\alpha \in K[x_1, \dots, x_n]$ a nonzero polynomial and let $>$ be a monomial order.

(i) The *multidegree* of f is

$$multideg(f) := max\{\alpha \in \mathbb{Z}^n_{\geq 0} \mid a_\alpha \neq 0\}.$$

The maximum is taken with respect to $>$.

(ii) The *leading coefficient* of f is

$$LC(f) := a_{multideg(f)} \in K.$$

(iii) The *leading monomial* of f is

$$LM(f) := x^{multideg(f)}.$$

(iv) The *leading term* of f is

$$LT(f) := LC(f) \cdot LM(f).$$

Consider the following, let $I \subseteq K[x]$ an ideal. We know that $K[x]$ is a PID, therefore $I = \langle f \rangle$ for some $f \in K[x]$. Let $g \in K[x]$, for the division algorithm we can write $g(x) = f(x)q(x) + r(x)$ where $r(x) = 0$ or $deg(r) < deg(f)$. If $r = 0$ then $g \in I$. Now suppose that $g \in I$, if $r \neq 0$ then $deg(r) < deg(f)$. We have that $g(x) = f(x)q(x) + r(x)$, then $r \in I$, so $f \mid r$ and this could not be because $deg(r) < deg(f)$. Therefore $r = 0$.

The division algorithm could be used to solved the ideal membership problem for polynomials of one variable. To study this problem when there are more variables, we will formulate a division algorithm for polynomials in $K[x_1, \dots, x_n]$ that extends the algorithm for $K[x]$.

Theorem 1.3.4. (Division Algorithm) *Fix a monomial order $>$ on $\mathbb{Z}^n_{\geq 0}$, and let $F = (f_1, \dots, f_s)$ be an ordered s-tuple of polynomials in $K[x_1, \dots, x_n]$. Then every f in the ring $K[x_1, \dots, x_n]$ can be written as*

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

Where a_i,$r \in K[x_1, \dots, x_n]$, and either $r = 0$ or r is a linear combination, with coefficients in K, of monomials, none of which is divisible by any $LT(f_i)$ for all $i \in \{1, \dots, s\}$. We will call r a remainder of f on division by F. Furthermore, if $a_i f_i \neq 0$, then we have

$$multideg(f) \geq multideg(a_i f_i).$$

Proof. [7], page 64. □

Definition 1.3.5. An ideal $I \subseteq K[x_1, \dots, x_n]$ is a *monomial ideal* if there is a subset $A \subseteq \mathbb{Z}^n_{\geq 0}$ (possibly infinite) such that:

$$I = \langle \{x^\alpha \mid \alpha \in A\} \rangle.$$

Lemma 1.3.6. *Let $I = \langle \{x^\alpha \mid \alpha \in A\} \rangle$ be a monomial ideal. Then a monomial $x^\beta \in I$ if and only if x^β is divisible by x^α for some $\alpha \in A$.*

Proof. If x^β is divisible by x^α for some $\alpha \in A$, clearly $x^\beta \in I$. Conversely, if $x^\beta \in I$, then

$$x^\beta = \sum_{i=1}^{s} h_i x^{\alpha_i},$$

where $h_i \in K[x_1, \dots, x_n]$ and $\alpha_i \in A$. For all $i \in \{1, \dots, s\}$, let

$$h_i = \sum_{j=1}^{m_i} c^i_j x^{\beta_{ji}}.$$

With $c^i_j \in K$ and $\beta_{ji} \in \mathbb{Z}^n_{\geq 0}$ for all $i \in \{1, \dots, s\}$, $j \in \{1, \dots, m_i\}$. Therefore

$$x^\beta = \sum_{i=1}^{s} \sum_{j=1}^{m_i} c^i_j x^{\beta_{ji} + \alpha_i}.$$

Then, we get that $x^\beta = x^{\beta_{ji} + \alpha_i}$ for some $i \in \{1, \dots, s\}$ and $j \in \{1, \dots, m_i\}$. □

Lemma 1.3.7. (Dickson) *Let $I = \langle \{x^\alpha \mid \alpha \in A\} \rangle$ be a monomial ideal. Then I can be written in the form $I = \langle x^{\alpha_1}, \dots, x^{\alpha_s} \rangle$, where $\alpha_i \in A$. In particular; I has a finite basis.*

Proof. [7], page 71. □

Corollary 1.3.8. *Let $>$ be a relation on $\mathbb{Z}^n_{\geq 0}$ satisfying:*

(i) $>$ *is a total ordering on* $\mathbb{Z}^n_{\geq 0}$.

(ii) *If* $\alpha > \beta$ *and* $\gamma \in \mathbb{Z}^n_{\geq 0}$, *then* $\alpha + \gamma > \beta + \gamma$.

Then $>$ *is a well ordering if and only if* $\alpha \geq 0$ *for all* $\alpha \in \mathbb{Z}^n_{\geq 0}$.

Proof. Suppose that $>$ is a well ordering. Let α_0 be the smallest element of $\mathbb{Z}^n_{\geq 0}$. It suffices to show $\alpha_0 \geq 0$. This is easy: if $0 > \alpha_0$, then by the hypothesis (ii), we can add α_0 to both sides to obtain $\alpha_0 > 2\alpha_0$, which is impossible since α_0 is the smallest element.

Now suppose that $\alpha \geq 0$ for all $\alpha \in \mathbb{Z}^n_{\geq 0}$. Let $A \subseteq \mathbb{Z}^n_{\geq 0}$ be nonempty. We need to show that A has a smallest element. Since $I = \langle \{x^\alpha \mid \alpha \in A\} \rangle$ is a monomial ideal, we know that we can write $I = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$. Relabeling if necessary, we can assume that $\alpha_1 < \alpha_2 < \cdots < \alpha_s$. We claim that α_1 is the smallest element of A. To prove this, take $\alpha \in A$, then $x^\alpha \in I$, therefore x^α is divisible by some x^{α_i}. This tell us that $\alpha = \alpha_i + \gamma$ for some $\gamma \in \mathbb{Z}^n_{\geq 0}$. Then $\gamma \geq 0$ and

$$\alpha = \alpha_i + \gamma \geq \alpha_i \geq \alpha_1.$$

□

Fix a monomial order on $K[x_1, \ldots, x_n]$, each $f \in K[x_1, \ldots, x_n]$ has a unique leading term $LT(f)$. Then for any ideal I, we can define its *ideal of leading terms* as follows.

Definition 1.3.9. Let $I \subseteq K[x_1, \ldots, x_n]$ be and ideal other than $\{0\}$. We denote by $LT(I)$ the *set of leading terms* of elements of I. Thus,

$$LT(I) := \{LT(f) \mid f \in I\}.$$

We denote by $\langle LT(I) \rangle$ the ideal generated by $LT(I)$.

Remark 1.3.10. *Let* $I \subseteq K[x_1, \ldots, x_n]$ *be and ideal other than* $\{0\}$. *Given a finite generating set for* I, *say* $I = \langle f_1, \ldots, f_s \rangle$, *then* $\langle LT(f_1), \ldots, LT(f_s) \rangle$ *and* $\langle LT(I) \rangle$ *may be different ideals. It is true that* $\langle LT(f_1), \ldots, LT(f_s) \rangle \subseteq \langle LT(I) \rangle$. *However* $\langle LT(I) \rangle$ *can be strictly larger. To see this, consider the following example.*

Let $I = \langle f_1, f_2, f_3 \rangle$, *where* $f_1 = x^4y^2 - z^5$, $f_2 = x^3y^3 - 1$ *and* $f_3 = x^2y^4 - 2z$, *and use grlex ordering on monomials in* $K[x, y, z]$. *Then*

$$g = xf_2 - yf_1 = yz^5 - x,$$

so that $g \in I$. *Thus* $yz^5 = LT(g) \in \langle LT(I) \rangle$. *Note that* $yz^5 \notin \langle LT(f_1), LT(f_2), LT(f_3) \rangle$.

Proposition 1.3.11. *Let* $I \subseteq K[x_1, \ldots, x_n]$ *be and ideal.*

(i) $\langle LT(I) \rangle$ *is a monomial ideal.*

(ii) *There are* $g_1, \ldots, g_t \in I$ *such that* $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$.

Proof. [7], page 76. □

Theorem 1.3.12. (Hilbert Basis Theorem) *Every ideal $I \subseteq K[x_1, \dots, x_n]$ has a finite generating set.*

Proof. If $I = \{0\}$, we take our generating set to be $\{0\}$, suppose that $I \neq \{0\}$. By the last proposition, there are $g_1, \dots, g_t \in I$ such that $\langle LT(I)\rangle = \langle LT(g_1), \dots, LT(g_t)\rangle$. We claim that $I = \langle g_1, \dots, g_t\rangle$.

It is clear that $\langle g_1, \dots, g_t\rangle \subseteq I$ since each $g_i \in I$. Conversely, let $f \in I$. If we apply the division algorithm to divide f by $F = (g_1, \dots, g_t)$, then we get an expression of the form

$$f = a_1g_1 + \cdots + a_sg_s + r$$

where no term of r is divisible by any of $LT(g_1), \dots, LT(g_t)$. We claim that $r = 0$. To see this, note that

$$r = f - (a_1g_1 + \cdots + a_sg_s) \in I.$$

If $r \neq 0$, then $LT(r) \in \langle LT(I)\rangle = \langle LT(g_1), \dots, LT(g_t)\rangle$, it follows that $LT(r)$ must be divisible by some $LT(g_i)$. Consequently, r must be zero. Thus,

$$f = a_1g_1 + \cdots + a_sg_s \in \langle g_1, \dots, g_t\rangle,$$

this completes the proof. □

Remark 1.3.13. *The basis $\{g_1, \dots, g_t\}$ used in the proof of the last theorem has the special property that $\langle LT(I)\rangle = \langle LT(g_1), \dots, LT(g_t)\rangle$.*

Definition 1.3.14. Fix a monomial order. A finite subset $G = \{g_1, \dots, g_t\}$ of and ideal I is said to be a *Gröbner basis (or standard basis)* if

$$\langle LT(I)\rangle = \langle LT(g_1), \dots, LT(g_t)\rangle.$$

Corollary 1.3.15. *Fix a monomial order: Then every ideal $I \subseteq K[x_1, \dots, x_n]$ other than $\{0\}$ has a Gröbner basis. Furthermore, any Gröbner basis for an ideal I is a basis of I.*

Proof. [7], page 77. □

Example 1.3.16. *Let $I = \langle x - z^2, y - z^3\rangle$. Consider lex order. Note that $LT(x-z^2) = x$ and $LT(y-z^3) = y$. Let $f = h_1(x-z^2)+h_2(y-z^3) \in I \setminus \{0\}$. Suppose that $LT(f) \notin \langle x, y\rangle$. Then $LT(f)$ is not divisible by either x or y, by the definition of lex order, f must be a polynomial in z alone. Let $g(z) = f(x, y, z)$, we have that $f(t^2, t^3, t) = 0$ $\forall t \in K$, it follows that $f = 0$. Therefore $LT(f) \in \langle x, y\rangle$.*

Definition 1.3.17. Let $I \subseteq K[x_1, \dots, x_n]$ be an ideal. We will denote by $\mathbf{V}(I)$ the set

$$\mathbf{V}(I) = \{(a_1, \dots, a_n) \mid f(a_1, \dots, a_n) = 0 \ \forall f \in I\}.$$

Proposition 1.3.18. $\mathbf{V}(I)$ *is an affine variety. In particular, if* $I = \langle f_1, \ldots, f_s \rangle$, *then* $\mathbf{V}(I) = \mathbf{V}(f_1, \ldots, f_s)$.

Proof. [7], page 79. □

Proposition 1.3.19. *Let* $G = \{g_1, \ldots, g_t\}$ *be a Gröbner basis for an ideal* $I \subseteq K[x_1, \ldots, x_n]$ *and let* $f \in K[x_1, \ldots, x_n]$. *Then there is a unique* $r \in K[x_1, \ldots, x_n]$ *with the following two properties:*

(i) *No term of* r *is divisible by any of* $LT(g_1), \ldots, LT(g_t)$.

(ii) *There is* $g \in I$ *such that* $f = g + r$.

In particular, r *is the remainder on division of* f *by* G *no matter how the elements of* G *are listed when using the division algorithm.*

Proof. [7], page 82. □

Corollary 1.3.20. *Let* $G = \{g_1, \ldots, g_t\}$ *be a Gröbner basis for an ideal* $I \subseteq K[x_1, \ldots, x_n]$ *and let* $f \in K[x_1, \ldots, x_n]$. *Then* $f \in I$ *if and only if the remainder on division of* f *by* G *is zero.*

Proof. [7], page 82. □

Definition 1.3.21. We will write $\bar{f}^F$ for the remainder on division of f by the ordered s-tuple $F = (f_1, \ldots, f_s)$. If F is a Gröbner basis for $\langle f_1, \ldots, f_s \rangle$, then we can regard F as a set (without any particular order) by proposition 1.3.19.

We next will discuss how to tell whether a given generating set of an ideal is a Gröbner basis.

Definition 1.3.22. Let $f, g \in K[x_1, \ldots, x_n]$ be nonzero polynomials.

(i) If $multideg(f) = \alpha$ and $multideg(g) = \beta$, then let $\gamma = (\gamma_1, \ldots, \gamma_n)$, where $\gamma_i = max\{\alpha_i, \beta_i\}$ for each i. We call x^γ the *least common multiple* of $LM(f)$ and $LM(g)$, written $x^\gamma = LCM(LM(f), LM(g))$.

(ii) The *S-polynomial* of f and g is the combination

$$S(f,g) := \tfrac{x^\gamma}{LT(f)} f - \tfrac{x^\gamma}{LT(g)} g.$$

An S-polynomial $S(f,g)$ is designed to produce cancellation of leading terms.

Theorem 1.3.23. (Buchberger's Criterion) *Let* I *be a polynomial ideal. Then a basis* $G = \{g_1, \ldots, g_t\}$ *for* I *is a Gröbner basis for* I *if and only if for all pairs* $i \neq j$ $\overline{S(g_i, g_j)}^G = 0$.

Proof. [7], page 85. □

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

Theorem 1.3.24. (Buchberger [5]) 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: $\mathcal{G} := \mathcal{F}, \quad B := \{\{f_i, f_j\} \,|\, f_i \neq f_j \in \mathcal{G}\}$
while $B \neq \emptyset$ do
  pick any $\{f, g\} \in B$
  $B := B \setminus \{\{f, g\}\}$
  $r :=$ remainder of $\mathrm{S}(f, g)$ with respect to $\mathcal{G}$
  if $r \neq 0$ then
    $B := B \cup \{\{r, h\} \,|\, h \in \mathcal{G}\}$
    $\mathcal{G} := \mathcal{G} \cup \{r\}$
```

Lemma 1.3.25. *Let G be a Gröbner basis for the polynomial ideal I. Let $p \in G$ be a polynomial such that $LT(p) \in \langle LT(G \setminus \{p\}) \rangle$. Then $G \setminus \{p\}$ is also a Gröbner basis for I.*

Proof. We know that $\langle LT(I) \rangle = \langle LT(G) \rangle$. If $LT(p) \in \langle LT(G \setminus \{p\}) \rangle$, then we have $\langle LT(G \setminus \{p\}) \rangle = \langle LT(G) \rangle$. By definition, it follows that $G \setminus \{p\}$ is also a Gröbner basis for I. □

By adjusting constants to make all leading coefficients 1 and removing any p with $LT(p) \in \langle LT(G \setminus \{p\}) \rangle$ from G, we arrive at what we will call a *minimal Gröbner basis.*

Definition 1.3.26. A *minimal Gröbner basis* for a polynomial ideal I is a Gröbner basis G for I such that:

(i) $LC(p) = 1$ for all $p \in G$.

(ii) For all $p \in G$, $LT(p) \notin \langle LT(G \setminus \{p\}) \rangle$.

Unfortunately, a given ideal may have many minimal Gröbner bases. Fortunately, we can single out one minimal basis that is better than then others. The definition is as follows.

Definition 1.3.27. A *reduced Gröbner basis* for a polynomial ideal I is a Gröbner basis G for I such that:

(i) $LC(p) = 1$ for all $p \in G$.

(ii) For all $p \in G$, no monomial of p lies in $\langle LT(G \setminus \{p\}) \rangle$.

Example 1.3.28. *Consider lex order. Let $I = \langle x^2y-1, xy^2-x\rangle$. By Theorem 1.3.23, we have that $G = \{f_1 = x^2y-1, f_2 = xy^2-x, f_3 = x^2-y, f_4 = y^2-1\}$ is a Gröbner basis for I.*

Note that $LT(f_1) = yLT(f_3)$ and $LT(f_2) = yLT(f_4)$, therefore $\acute{G} = \{f_3, f_4\}$ is a reduced Gröbner basis for I.

Proposition 1.3.29. *Let $I \neq \{0\}$ be a polynomial ideal. Then, for a given monomial ordering, I has a unique reduced Gröbner basis.*

Proof. [7], page 92. □

Proposition 1.3.30. *Let I be an ideal of $S = K[x_1, \ldots, x_n]$ and let $\mathcal{F} = \{f_1, \ldots, f_s\}$ be a Gröbner basis of I. If*

$$\mathcal{B} = \{\overline{u} \mid u \textit{ is a monomial in } K[x_1, \ldots, x_n] \textit{ and } u \notin \langle LT(f_1), \ldots, LT(f_s)\rangle\},$$

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 $\overline{f} \in S/I$. By the division algorithm, 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 $LT(f_j)$. 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 $u_i \in \mathcal{B}$ and $\lambda_i \in K$. We must show $h = 0$. If $h \neq 0$, then we can label the u_i's so that $u_1 > \cdots > u_s$ and $\lambda_1 \neq 0$. Hence $LT(h) = \lambda_1 u_1 \in LT(I)$, but this is a clear contradiction because $\langle LT(I)\rangle = \langle LT(f_1), \ldots, LT(f_s)\rangle$. Therefore $h = 0$, as required. □

Definition 1.3.31. A monomial in $\mathcal{B}$ is called a *standard monomial* with respect to $f_1, \ldots, f_s$. The set $\mathcal{B}$ of standard monomials is called the *footprint* of I and is denoted by $\Delta_{\succ}(I)$.

Elimination Theory

Definition 1.3.32. Given $I = \langle f_1, \ldots, f_s\rangle \subseteq K[x_1, \ldots, x_n]$ the *l-th elimination ideal I_l* is the ideal of $K[x_{l+1}, \ldots, x_n]$ defined by

$$I_l := I \cap K[x_{l+1}, \ldots, x_n].$$

Theorem 1.3.33. (The Elimination Theorem) *Let $I \subseteq K[x_1, \ldots, x_n]$ be and ideal and let G be a Gröbner basis for I with respect to the lex order where $x_1 > \cdots > x_n$. Then for every $0 \leq l \leq n$, the set*

$$G_l := G \cap K[x_{l+1}, \ldots, x_n],$$

is a Gröbner basis of the l-th elimination ideal I_l.

Proof. Fix $0 \leq l \leq n$. Since $G_l \subseteq I_l$ by construction, it suffices to show that

$$\langle LT(I_l) \rangle = \langle LT(G_l) \rangle,$$

by the definition of the Gröbner basis. Clearly $\langle LT(I_l) \rangle \supseteq \langle LT(G_l) \rangle$. Now, we are going to prove the other inclusion. Let $f \in I_l$, then $LT(f)$ is divisible by $LT(g)$ for some $g \in G$. Therefore $LT(g) \in K[x_{l+1}, \ldots, x_n]$. Now comes the crucial observation: since we are using lex order with $x_1 > \cdots > x_n$, any monomial involving $x_1, \ldots, x_l$ is greater than all monomials in $K[x_{l+1}, \ldots, x_n]$, so that $LT(g) \in K[x_{l+1}, \ldots, x_n]$ implies $g \in K[x_{l+1}, \ldots, x_n]$, this shows that $g \in G_l$, and the theorem is proved. □

1.4 Projective varieties

We define an equivalence relation $\sim$ on $K^{n+1} \setminus \{(0, \ldots, 0)\}$ by setting

$$(y_0, \ldots, y_n) \sim (x_0, \ldots, x_n),$$

if there is a nonzero element $\lambda \in K$ such that $(y_0, \ldots, y_n) = \lambda(x_0, \ldots, x_n)$. If we let $\hat{0}$ denote the origin $(0, \ldots, 0)$ in K^{n+1}, then we define the *projective space* as follows.

Definition 1.4.1. The *n-dimensional projective space* over the field K, denoted $\mathbb{P}^n_K$, is the set of equivalence classes of $\sim$ on $K^{n+1} \setminus \{\hat{0}\}$. Thus,

$$\mathbb{P}^n_K = (K^{n+1} \setminus \{\hat{0}\}) / \sim.$$

Each nonzero $(n+1)$-tuple $(x_0, \ldots, x_n) \in K^{n+1}$ defines a point $p = [(x_0, \ldots, x_n)]$ in $\mathbb{P}^n_K$, and we say that $(x_0, \ldots, x_n)$ are *homogeneous coordinates* of p.

Remark 1.4.2. *We can think of $\mathbb{P}^n_K$ more geometrically as the set of lines through the origin in K^{n+1}. More precisely, there is a one-to-one correspondence*

$$\mathbb{P}^n_K \cong \{ \textit{ lines through the origin in } K^{n+1}\}.$$

Proposition 1.4.3. *Let*

$$\mathcal{U}_0 := \{[(x_0, \ldots, x_n)] \in \mathbb{P}^n_K \mid x_0 \neq 0\}.$$

The map ϕ taking $(a_1, \ldots, a_n)$ in K^n to the point $[(1, a_1, \ldots, a_n)] \in \mathbb{P}^n_K$ is a one-to-one correspondence between K^n and $\mathcal{U}_0 \subseteq \mathbb{P}^n_K$.

Proof. Note that $\phi : K^n \to \mathcal{U}_0$. We can also define an inverse map $\psi : \mathcal{U}_0 \to K^n$ as follows. Given $p = [(x_0, \ldots, x_n)] \in \mathcal{U}_0$ since $x_0 \neq 0$ we can multiply the homogeneous coordinates by the nonzero scalar $\lambda = x_0^{-1}$ to obtain $p = [(1, \frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0})]$. Then set $\psi(p) := (\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}) \in K^n$.

Now, we will prove that ψ is well-defined. Suppose that $p = [(y_0, \ldots, y_n)] \in \mathcal{U}_0$, then $(x_0, \ldots, x_n) = \gamma(y_0, \ldots, y_n)$ for some $\gamma \in K \setminus \{0\}$. Therefore

$$x_i = \gamma y_i \text{ for all } i \in \{0, \dots, n\}.$$

Then, we have that $(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}) = (\frac{\gamma y_1}{\gamma y_0}, \dots, \frac{\gamma y_n}{\gamma y_0}) = (\frac{y_1}{y_0}, \dots, \frac{y_n}{y_0})$. It follows that ψ is well-defined. It is clear that ϕ and ψ are inverse mappings. This establishes the desired one-to-one correspondence. □

Remark 1.4.4. *By the definition of* $\mathcal{U}_0$, *we see that* $\mathbb{P}^n_K = \mathcal{U}_0 \cup \mathcal{H}$, *where*

$$\mathcal{H} = \{[(x_0, \dots, x_n)] \in \mathbb{P}^n_K \mid x_0 = 0\}.$$

If we identify $\mathcal{U}_0$ *with the affine space* K^n, *then we can think of* $\mathcal{H}$ *as the hyperplane at infinity. It follows from the last equality that the points in* $\mathcal{H}$ *are in one-to-one correspondence with n-tuples* $(x_1, \dots, x_n)$, *where two n-tuples represent the same point in* $\mathcal{H}$ *if one is a nonzero scalar multiple of the other (just ignore the first component of points in* $\mathcal{H}$*). In other words,* $\mathcal{H}$ *is a copy of* $\mathbb{P}^{n-1}_K$, *the projective space of one smaller dimension. We can write* $\mathbb{P}^n_K = K^n \cup \mathbb{P}^{n-1}_K$.

Corollary 1.4.5. *For each* $i \in \{0, \dots, n\}$, *let*

$$\mathcal{U}_i := \{[(x_0, \dots, x_n)] \in \mathbb{P}^n_K \mid x_i \neq 0\}.$$

(i) *The points of each* $\mathcal{U}_i$ *are in one-to-one correspondence with the points of* K^n.

(ii) *The complement* $\mathbb{P}^n_K \setminus \mathcal{U}_i$ *may be identify with* $\mathbb{P}^{n-1}_K$.

(iii) *We have* $\mathbb{P}^n_K = \displaystyle\bigcup_{i=0}^{n} \mathcal{U}_i$.

Proof. [7], page 369. □

Our next goal is to extend the definition of varieties in affine space to projective space. For instance, we can ask whether it makes sense to consider $\mathbf{V}(f)$ for a polynomial $f \in K[x_0, \dots, x_n]$. A simple example shows that some care must be taken here. In $\mathbb{P}^2_{\mathbb{R}}$, we can try to construct $\mathbf{V}(x_1 - x_2^2)$, the point $p = [(1, 4, 2)]$ appears to be in this set, a problem arises when we note that the same point p can be represented by the homogeneous coordinates $(2, 8, 4)$. To avoid problems of this type, we use homogeneous polynomials when working in $\mathbb{P}^n_K$.

Proposition 1.4.6. *Let* $f \in K[x_0, \dots, x_n]$ *be a homogeneous polynomial. If* f *vanishes on any set of homogeneous coordinates for a point* $p \in \mathbb{P}^n_K$, *then* f *vanishes for all homogeneous coordinates of* p. *In particular* $\mathbf{V}(f) = \{[(x_0, \dots, x_n)] \in \mathbb{P}^n_K \mid f(x_0, \dots, x_n) = 0\}$ *is a well-defined subset of* $\mathbb{P}^n_K$.

Proof. Let $(a_0, \dots, a_n)$ and $(\lambda a_0, \dots, \lambda a_n)$ be homogeneous coordinates for $p \in \mathbb{P}^n_K$ and assume that $f(a_0, \dots, a_n) = 0$. If f is homogeneous of total degree k, then every term in f has the form

$$cx_0^{\alpha_0}\cdots x_n^{\alpha_n},$$

where $\alpha_0+\cdots+\alpha_n=k$. When we substitute $x_i=\lambda a_i$, this term becomes

$$c(\lambda a_0)^{\alpha_0}\cdots(\lambda a_a)^{\alpha_n}=\lambda^k c a_0^{\alpha_0}\cdots a_n^{\alpha_n}.$$

Summing over the terms in f, we find a common factor of λ^k and, hence,

$$f(\lambda a_0,\ldots,\lambda a_n)=\lambda^k f(a_0,\ldots,a_n)=0.$$

□

Notice that even if f is homogeneous, the equation $f=a$ does not make sense in $\mathbb{P}_K^n$ when $a\neq 0$. The equation $f=0$ is special because it gives a well-defined subset of $\mathbb{P}_K^n$. We can also consider subsets of $\mathbb{P}_K^n$ defined by the vanishing of a system of homogeneous polynomials.

Definition 1.4.7. Let K be a field and let $f_1,\ldots,f_s\in K[x_0,\ldots,x_n]$ be homogeneous polynomials. We set

$$\mathbf{V}(f_1,\ldots,f_s):=\{[(a_0,\ldots,a_n)]\in\mathbb{P}_K^n\mid f_i(a_0,\ldots,a_n)=0\text{ for all }1\leq i\leq s\}.$$

We call $\mathbf{V}(f_1,\ldots,f_s)$ the *projective variety* defined by $f_1,\ldots,f_s$.

For example, in $\mathbb{P}_K^n$, any nonzero homogeneous polynomial of degree 1,

$$l(x_0,\ldots,x_n)=c_0x_0+\cdots+c_nx_n,$$

defines a projective variety $\mathbf{V}(l)$ called a *hyperplane*. When $n=2$, we call $\mathbf{V}(l)$ a *projective line*. Similarly, when $n=3$, we call a hyperplane a *plane* in $\mathbb{P}_K^3$.

Now we will see the relation between affine and projective varieties. We saw that $\mathbb{P}_K^n=\displaystyle\bigcup_{i=0}^{n}\mathcal{U}_i$, the subsets $\mathcal{U}_i\subseteq\mathbb{P}_K^n$ are copies of K^n. If we take a projective a projective variety V and intersect it with one of the $\mathcal{U}_i$, it makes sense to ask whether we obtain an affine variety. The answer to this question is always yes, and the defining equations of the variety $V\cap\mathcal{U}_i$ may be obtained by a process called *dehomogenization.*

Consider $V\cap\mathcal{U}_0$, if $p\in\mathcal{U}_0$, then p has homogeneous coordinates of the form $(1,x_1,\ldots,x_n)$. If $f\in K[x_0,\ldots,x_n]$ is one of the defining equations of V, then the polynomial $g(x_1,\ldots,x_n)$ is equal to $f(1,x_1,\ldots,x_n)\in K[x_1,\ldots,x_n]$ vanishes at every point of $V\cap\mathcal{U}_0$. Setting $x_0=1$ in f produces a *dehomogenized polynomial* g which is usually nonhomogeneous.

Proposition 1.4.8. *Let $V=\mathbf{V}(f_1,\ldots,f_s)$ be a projective variety. Then $W=V\cap\mathcal{U}_0$ can be identified with the affine variety $\mathbf{V}(g_1,\ldots,g_s)\subseteq K^n$, where $g_i(y_1,\ldots,y_n)=f_i(1,y_1,\ldots,y_n)$ for each $1\leq i\leq s$.*

Proof. The comments before the statement of the proposition show that using the mapping $\psi : \mathcal{U}_0 \to K^n$ from proposition 1.4.3, $\psi(W) \subseteq \mathbf{V}(g_1, \ldots, g_s)$. On the other hand, if $(a_1, \ldots, a_n) \in \mathbf{V}(g_1, \ldots, g_s)$, then the point with homogeneous coordinates $(1, a_1, \ldots, a_n)$ is in $\mathcal{U}_0$ and it satisfies the equations

$$f_i(1, a_1, \ldots, a_n) = g_i(1, a_1, \ldots, a_n) = 0.$$

Thus, $\phi(\mathbf{V}(g_1, \ldots, g_s)) \subseteq W$. Since the mappings ϕ and ψ are inverses, the points of W are in one-to-one correspondence with the points of $\mathbf{V}(g_1, \ldots, g_s)$. □

Remark 1.4.9. *We can also dehomogenize with respect to the other variables.*

Proposition 1.4.10. *Let $g \in K[x_1, \ldots, x_n]$ be a polynomial of total degree d.*

(i) *Let $g = \sum_{i=0}^{d} g_i$ be the expansion of g as the sum of its homogeneous components where g_i has total degree i. Then*

$$g^h(x_0, \ldots, x_n) = \sum_{i=0}^{d} g_i(x_1, \ldots, x_n) x_0^{d-i}$$

is a homogeneous polynomial of total degree d in $K[x_0, \ldots, x_n]$. We will call g^h the homogenization of g.

(ii) *The homogenization of g can be computed using the formula*

$$g^h = x_0^d \cdot g\left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right).$$

(iii) *Dehomogenizing g^h yields g. That is, $g^h(1, x_1, \ldots, x_n) = g(x_1, \ldots, x_n)$.*

(iv) *Let $F(x_0, \ldots, x_n)$ be a homogeneous polynomial and let x_0^e be the highest power of x_0 dividing F. if $f = F(1, x_1, \ldots, x_n)$ is a dehomogenization of F, then $F = x_0^e \cdot f^h$.*

Proof. [7], page 373. □

Let $I \subseteq K[x_0, \ldots, x_n]$ be a homogeneous ideal. We will denote by $\mathbf{V}(I)$ the set

$$\mathbf{V}(I) = \{[(a_0, \ldots, a_n)] \mid f(a_0, \ldots, a_n) = 0 \ \forall f \in I\}.$$

It is clear that $\mathbf{V}(I)$ is a well-defined subset of $\mathbb{P}_K^n$. If $I = \langle f_1, \ldots, f_s \rangle$, where $f_i \in K[x_0, \ldots, x_n]$ are homogeneous polynomials, it is easy to see that $\mathbf{V}(I) = \mathbf{V}(f_1, \ldots, f_s)$.

As earlier, finite unions of projective varieties are projective varieties and arbitrary intersections of projective varieties. So, the projective varieties furnish us with the closed sets for a topology on $\mathbb{P}_K^n$, called the *Zariski topology* on $\mathbb{P}_K^n$. We can pretty well repeat all our earlier observations about this topology on K^n and apply them to $\mathbb{P}_K^n$.

Let $Y \subseteq \mathbb{P}_K^n$. Then we set

$$\mathbf{I}(Y) = \langle \{f \in K[x_0, \dots, x_n] \mid \text{f is homogeneous and } f(p) = 0 \ \forall p \in Y\} \rangle.$$

We will call $\mathbf{I}(Y)$ the ideal of Y.

Let $I \subseteq K[x_0, \dots, x_n]$ be a homogeneous ideal in $K[x_0, \dots, x_n]$. The ideal I gives us the projective variety $V = \mathbf{V}(I) \subseteq \mathbb{P}^n_K$. We will also work with the affine variety $C_V = \mathbf{V}_a(I) \subseteq K^{n+1}$. We call C_V the *affine cone* of V. If we interpret points in $\mathbb{P}^n_K$ as lines through the origin in K^{n+1}, then C_V is the union of the lines determined by the points of V, C_V contains all homogeneous coordinates of the points in V.

Theorem 1.4.11. (The Projective Strong Nullstellensatz) *Let K be an algebraically closed field and let I be a homogeneous ideal in $K[x_0, \dots, x_n]$. If $V = \mathbf{V}(I)$ is a nonempty projective variety in $\mathbb{P}^n_K$, then we have*

$$\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}.$$

Proof. [7], page 84. □

Projective Closure

Definition 1.4.12. Let I be an ideal in $K[x_1, \dots, x_n]$. We define the *homogenization of* I to be the ideal

$$I^h = \left\langle \{f^h \mid f \in I\} \right\rangle \subseteq K[x_0, \dots, x_n],$$

where f^h is the homogenization of f.

Naturally enough, for any ideal $I \subseteq K[x_1, \dots, x_n]$, the homogenization I^h is a homogeneous ideal in $K[x_0, \dots, x_n]$. There is a subtle point here. Given a particular finite generating set $f_1, \dots, f_s$ for $I \subseteq K[x_1, \dots, x_n]$, it is always true that $\left\langle f_1^h, \dots, f_s^h \right\rangle$ is a homogeneous ideal contained in I^h. However, I^h can be strictly larger than $\left\langle f_1^h, \dots, f_s^h \right\rangle$.

A *graded monomial order* in $K[x_1, \dots, x_n]$ is one that orders first by total degree. $x^\alpha > x^\beta$ whenever $|\alpha| > |\beta|$. Note that grlex and grevlex are graded orders.

Theorem 1.4.13. *Let I be an ideal in $K[x_1, \dots, x_n]$ and let $G = \{g_1, \dots, g_t\}$ be a Gröbner basis for I with respect to a graded monomial order in $K[x_1, \dots, x_n]$. Then $G^h = \{g_1^h, \dots, g_t^h\}$ is a basis for $I^h \subseteq K[x_0, \dots, x_n]$.*

Proof. [7], page 388. □

Let $Y \subseteq K^n$. The *projective closure* of Y is defined as: $\mathbb{Y} = \overline{\phi(Y)}$, where ϕ is the map $\phi : K^n \to \mathbb{P}^n_K$, $\alpha = (\alpha_1, \dots, \alpha_n) \to [(1, \alpha_1, \dots, \alpha_n)]$, and $\overline{\phi(Y)}$ is the closure of $\phi(Y)$ in the Zariski topology of $\mathbb{P}^n_K$. Note that $\mathbb{Y} = \mathbf{V}(\mathbf{I}(\phi(Y)))$. We claim that $\mathbf{I}(\mathbb{Y}) = \mathbf{I}(Y)^h$.

Let $f \in \mathbf{I}(Y)$ and $\alpha = (\alpha_1, \dots, \alpha_n) \in Y$. Now $f^h(1, \alpha_1, \dots, \alpha_n) = f(\alpha_1, \dots, \alpha_n) = 0$, then $\phi(Y) \subseteq \mathbf{V}(f^h)$, therefore $\overline{\phi(Y)} \subseteq \mathbf{V}(f^h)$. It implies that $f^h \in \mathbf{I}(\mathbb{Y})$, so $\mathbf{I}(\mathbb{Y}) \supseteq \mathbf{I}(Y)^h$.

Let $G \in \mathbf{I}(\mathbb{Y})$. Then $G = x_0^e \cdot g^h$, where $g(x_1, \dots, x_n) = G(1, x_1, \dots, x_n)$ and x_0^e is the highest power of x_0 dividing G. It is clear that $g \in \mathbf{I}(Y)$.

1.5 Dimension of a variety

In this section we study the dimension of a variety. The definition is the same that one can study in a geometric algebraic course. Then we will see that for any affine variety $\mathbf{V}(I)$, where I is a monomial ideal, the dimension of $\mathbf{V}(I)$ is equal to the maximum of the dimensions of the coordinate subspaces contained in $\mathbf{V}(I)$.

Definition 1.5.1. A topological space X is called *noetherian* if it satisfies the descending chain condition for closed subsets: for any sequence $Y_1 \supseteq Y_2 \supseteq \cdots$ of closed subsets, there is an integer r such that $Y_r = Y_{r+1} = \cdots$.

Example 1.5.2. *K^n is a noetherian topological space. Indeed, if $Y_1 \supseteq Y_2 \supseteq \cdots$ is a descending chain of closed subsets, then $\mathbf{I}(Y_1) \subseteq \mathbf{I}(Y_2) \subseteq \cdots$ is an ascending chain of ideals in $K[x_1, \ldots, x_n]$. Since $K[x_1, \ldots, x_n]$ is a noetherian ring, this chain of ideals is eventually stationary. But for each i, $Y_i = \mathbf{V}(\mathbf{I}(Y_i))$, so the chain Y_i is also stationary.*

Proposition 1.5.3. *In a noetherian topological space X, every nonempty closed subset Y can be expressed as a finite union $Y = Y_1 \cup Y_2 \cup \cdots \cup Y_r$ of irreducible closed subsets Y_i. If we requiere that $Y_j \nsubseteq Y_i$ for $i \neq j$, then the Y_i are uniquely determined. They are called the irreducible components of Y.*

Proof. [18], page 5. □

Definition 1.5.4. If X is a topological space, we define the *dimension of X* (denoted *$dimX$*) to be the supremum of all integers n such that there exists a chain $Y_0 \subseteq Y_1 \subseteq \ldots Y_n$ of distinct irreducible closed subsets of X.

If $Y \subseteq K^n$ is an affine variety, we define the *affine coordinate ring* $\mathbf{A}(Y)$ of Y, to be $K[x_1, \ldots, x_n]/\mathbf{I}(Y)$.

Proposition 1.5.5. *If Y is an affine variety, then the dimension of Y (as topological subspace) is equal to the dimension of its affine coordinate ring $\mathbf{A}(Y)$.*

Proof. Let $Y \supsetneq Y_0 \supsetneq \cdots \supsetneq Y_t$ be a chain of irreducible closed subsets of Y of length t. Then

$$\mathbf{I}(Y) \subsetneq \mathbf{I}(Y_0) \subsetneq \cdots \subsetneq \mathbf{I}(Y_t)$$

is a chain of prime ideals that contains $\mathbf{I}(Y)$ of length t. Therefore $t \leq dim\mathbf{A}(Y)$, so we have that $dimY \leq dim\mathbf{A}(Y)$. Similarly we can prove that $dimY \geq dim\mathbf{A}(Y)$. □

Remark 1.5.6. *Let $Y \subseteq K^n$ be an affine variety. Since K^n is a noetherian topological space with Zariski topology, we know that Y can be expressed as a finite union $Y = Y_1 \cup Y_2 \cup \cdots \cup Y_r$ of irreducible varieties Y_i, therefore $\mathbf{I}(Y_i)$ is a prime ideal for all i. Let $S = K[x_1, \ldots, x_n]$, now*

$$\mathbf{I}(Y) = \mathbf{I}(Y_1) \cap \mathbf{I}(Y_2) \cap \cdots \mathbf{I}(Y_r).$$

Then, dim $\mathbf{A}(Y) =$ *dim* $S/\bigcap_{i=1}^{r}\mathbf{I}(Y_i)$*, let* $I_j = \mathbf{I}(Y_j)$*. It is easy to prove that*

$$\textit{dim}\ \mathbf{A}(Y) = \textit{max}\ \{\ \textit{dim}\ S/I_j \mid j = 1,\dots,r\}.$$

In K^n, a vector subspace defined by setting some subset of the variables $x_1,\dots,x_n$ equal to zero is called a *coordinate subspace.*

Proposition 1.5.7. *The affine variety of a monomial ideal in* $K[x_1,\dots,x_n]$ *is a finite union of coordinate subspaces of* K^n*.*

Proof. [7], page 440. □

When we write the variety of a monomial ideal I as union of finitely many coordinate subspaces, we can omit a subspace if it is contained in another in the union. Thus, we can write $\mathbf{V}(I)$ as a union of coordinate subspaces.

$$\mathbf{V}(I) = V_1 \cup \cdots \cup V_p,$$

where $V_i \not\subseteq V_j$ for $i \neq j$. Then the coordinate subspaces V_i are the irreducible components of $\mathbf{V}(I)$. Let $S = K[x_1,\dots,x_n]$, therefore

$$\dim \mathbf{V}(I) = \max\ \{\ \dim S/\mathbf{I}(V_i) \mid i = 1,\dots,p\}.$$

Remark 1.5.8. *Let* $i \in \{1,\dots,p\}$*, note that dim* $S/\mathbf{I}(V_i) = \textit{dim}_K\ V_i$*. In fact, suppose without loss of generality that* $V_i = \mathbf{V}(x_1,\dots,x_r)$*, we know that* $\mathbf{I}(V_i) = \langle x_1,\dots,x_r\rangle$*. Then*

$$S/\mathbf{I}(V_i) = S/\left\langle x_1,\dots,x_r\right\rangle \cong K[x_{r+1},\dots,x_n],$$

thus, dim $V_i =$ *dim* $K[x_{r+1},\dots,x_n] = n - r = \textit{dim}_K\ V_i$*. The dimension of* $\mathbf{V}(I)$*, is the largest of the dimensions of the subspaces.*

Let $I = \langle m_1,\dots,m_t\rangle$ be a proper ideal generated by the monomials m_j. In trying to compute dim $\mathbf{V}(I)$, we need to pick out the component of

$$\mathbf{V}(I) = \bigcap_{j=1}^{t}\mathbf{V}(m_j),$$

of largest dimension. If we can find a collection of variables $x_{i_1},\dots,x_{i_r}$ such that at least one of these variables appears in each m_j, then the coordinate subspace defined by the equations $x_{i_1} =,\cdots,= x_{i_r} = 0$ is contained in $\mathbf{V}(I)$. This means we should look for variables which occur in as many of the different m_j as possible. More precisely, for $1 \leq j \leq t$, let

$$M_j = \{k \in \{1,\dots,n\} \mid x_k \text{ divides the monomial } m_j\},$$

be the subset of subscripts of variables occurring with positive exponent in m_j. Note that $M_j \neq \emptyset$ by our assumption that $I \neq K[x_1, \dots, x_n]$. Then let

$$\mathcal{M} = \{J \subseteq \{1, \dots, n\} \mid J \cap M_j \neq \emptyset \ \forall 1 \leq j \leq t\}.$$

Note that $\mathcal{M} \neq \emptyset$ because $\{1, \dots, n\} \in \mathcal{M}$.

Proposition 1.5.9. *With the notation above,*

$$dim\ \mathbf{V}(I) = n -\ min\ \{|J| \mid J \in \mathcal{M}\}.$$

Proof. [7], page 441. □

Example 1.5.10. *Let $I = \langle x_1x_2, x_2x_3, x_1x_3\rangle = \langle m_1, m_2, m_3\rangle$. Where*

$$m_1 = x_1x_2,\ m_2 = x_2x_3, m_3 = x_1x_3.$$

We have that,

$$M_1 = \{1, 2\},\ M_2 = \{2, 3\},\ M_3 = \{1, 3\},$$

so that

$$\mathcal{M} = \{\{1, 2, 3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}\}.$$

Then min $\{|J| \mid J \in \mathcal{M}\} = 2$, therefore dim $\mathbf{V}(I) = 3 - 2 = 1$.

The dimension of a projective variety is its dimension as a topological space.

Theorem 1.5.11. *Let $V \subseteq \mathbb{P}^n_K$ be a nonempty projective variety and $C_V \subseteq K^{n+1}$ be its affine cone, then*

$$dim\ C_V = dim\ V + 1.$$

Proof. [11], Lect4b page 4. □

Chapter 2

Reed-Muller-Type Codes

In this chapter we study the projective and the affine Reed-Muller-type codes. First we examine Hilbert functions, in the first section we prove that for any variety over an infinite field, its dimension is equal to the degree of the Hilbert polynomial. In the last section we will prove that the affine Reed-Muller-type codes are an special case of the projective Reed-Muller-type codes.

2.1 Hilbert functions

Given a vector space V and a subspace $W \subseteq V$, it is no difficult to show that the relation on V defined by $v \sim w$ if $v - w \in W$ is an equivalence relation. The set of equivalence classes of $\sim$ is denoted V/W, so that

$$V/W = \{[v] \mid v \in V\}.$$

It is easy to check that the operations $[v]+[w] = [v+w]$ and $a[v] = [av]$, where $a \in K$ and $v, w \in V$ are well defined and make V/W into a K- vector space, called the *quotient space* of V modulo W. When V is finite dimensional, we can compute the dimension of V/W as follows.

Proposition 2.1.1. *Let W a subspace of a finite dimensional vector space V. Then W and V/W are also finite dimensional vector spaces, and*

$$dim_K\ V = dim_K\ W + \ dim_K\ V/W.$$

Proof. [7], page 457. □

Affine Hilbert Polynomial We let $K[x_1, \ldots, x_n]_{\leq s}$ denote the set of polynomials of total degree $\leq s$ in $K[x_1, \ldots, x_n]$. We know that $K[x_1, \ldots, x_n]_{\leq s}$ is a K- vector space of dimension $\binom{n+s}{s}$. Then given an ideal $I \subseteq K[x_1, \ldots, x_n]$, we let

$$I_{\leq s} = I \cap K[x_1, \ldots, x_n]_{\leq s},$$

denote the set of polynomials in I of total degree $\leq s$. Note that $I_{\leq s}$ is a vector subspace of $K[x_1, \ldots, x_n]_{\leq s}$.

Definition 2.1.2. Let I be and ideal in $K[x_1, \ldots, x_n]$. The *affine Hilbert function* of I is the function $HF_I^a : \mathbb{N} \cup \{0\} \to \mathbb{N} \cup \{0\}$ defined by

$$HF_I^a(s) = dim_K\ K[x_1, \ldots, x_n]_{\leq s}/I_{\leq s} = dim_K\ K[x_1, \ldots, x_n]_{\leq s} - dim_K\ I_{\leq s}.$$

Proposition 2.1.3. *Let I be a proper monomial ideal in $K[x_1, \ldots, x_n]$.*

(i) *For all $s \geq 0$, $HF_I^a(s)$ is the number of monomials not in I of total degree $\leq s$.*

(ii) *For all s sufficiently large, the affine Hilbert function of I is given by a polynomial function*

$$HF_I^a(s) = \sum_{i=0}^{d} b_i \binom{s}{d-i},$$

where $b_i \in \mathbb{Z}$ and b_0 is positive.

(iii) *The degree of the polynomial in part (ii) is the maximum of the dimensions of the coordinate subspaces contained in $\mathbf{V}(I)$.*

Proof. [7], page 458. □

Proposition 2.1.4. *Let $I \subseteq K[x_1, \ldots, x_n]$ be an ideal and let $>$ be a graded order on $K[x_1, \ldots, x_n]$. Then the monomial ideal $\langle LT(I) \rangle$ has the same affine Hilbert function as I.*

Proof. Fix s and consider the leading monomials $LM(f)$ of all elements $f \in I_{\leq s}$. There are only finitely many such monomials, so that

$$\{LM(f) \mid f \in I_{\leq s}\} = \{LM(f_1), \ldots, LM(f_m)\}.$$

For some polynomials $f_1, \ldots, f_m \in I_{\leq s}$. By rearranging and deleting duplicates, we can assume that $LM(f_1) > \cdots > LM(f_m)$. We claim that $f_1, \ldots, f_m$ are a basis of $I_{\leq s}$ as a vector space over K.

(i) Consider a nontrivial linear combination equal to zero, $a_1 f_1 + \cdots + a_m f_m = 0$. Choose the smallest i such that $a_i \neq 0$. Given how we ordered the leading monomials, there is nothing to cancel $a_i LT(f_i)$, so the linear combination is nonzero. Hence, $f_1, \ldots, f_m$ are linearly independent.

Next, let $W = \mathcal{L}(f_1, \ldots, f_m) \subseteq I_{\leq s}$ be the subspace spanned by $f_1, \ldots, f_m$. If $W \neq I_{\leq s}$, pick $f \in I_{\leq s} - W$ with $LM(f)$ minimal. We have that $LM(f) = LM(f_i)$ for some i, and hence, $LT(f) = \lambda LT(f_i)$ for some $\lambda \in K$. Then $f - \lambda f_i \in I_{\leq s}$ has a smaller leading monomial, so that $f - \lambda f_i \in W$ by the minimality of $LM(f)$. This implies $f \in W$. which is a contradiction, it follows that $W = I_{\leq s}$, and we conclude that $f_1, \ldots, f_m$ are a basis.

(ii) The monomial ideal $\langle LT(I) \rangle$ is generated by the leading terms (or leading monomials) of elements of I. Thus, $LM(f_i) \in \langle LT(I) \rangle_{\leq s}$ since $f_i \in I_{\leq s}$. We claim that $LM(f_1), \ldots, LM(f_m)$ are a vector space basis of $\langle LT(I) \rangle_{\leq s}$. Arguing as above, it is easy to see that they are linearly independent. It remains to show that they span, i.e., that $\mathcal{L}(LM(f_1), \ldots, LM(f_m)) = \langle LT(I) \rangle_{\leq s}$. It suffices to show that

$$\{LM(f_1), \ldots, LM(f_m)\} = \{LM(f) \mid f \in I, LM(f) \text{ has total degree } \leq s\}.$$

Note that $>$ is a graded order, which implies that for any nonzero polynomial $f \in K[x_1, \ldots, x_n]$, $LM(f)$ has the same total degree as f. In particular, if $LM(f)$ has total degree $\leq s$, then so does f, which means that

$$\{LM(f) \mid f \in I, LM(f) \text{ has total degree } \leq s\} = \{LM(f) \mid f \in I_{\leq s}\}.$$

Thus, $I_{\leq s}$ and $\langle LT(I) \rangle_{\leq s}$ have the same dimension (since they both have bases consisting of m elements). □

Theorem 2.1.5. (Hilbert Theorem) *Let I be an ideal in $K[x_1, \ldots, x_n]$. The affine Hilbert function of I can be written for s sufficiently large as*

$$HF_I^a(s) = \sum_{i=0}^{d} b_i \binom{s}{d-i},$$

where the b_i are integers and b_0 is positive.

Proof. If we combine the last two propositions, the result follows immediately. □

Definition 2.1.6. The polynomial which equals $HF_I^a(s)$ for sufficiently large s is called the *affine Hilbert polynomial* of I and is denoted $HP_I^a(s)$.

By definition the Hilbert function of an ideal I coincides with the affine Hilbert polynomial of I when s is sufficiently large.

Definition 2.1.7. The smallest integer s_0 such that $HP_I^a(s) = HF_I^a(s)$ for all $s \geq s_0$ is called the *index of regularity* of I. It will be denoted by $\operatorname{reg} K[x_1, \ldots, x_n]/I$.

Remark 2.1.8. *For a monomial ideal I, we know that the degree of the affine Hilbert polynomial is the dimension of the largest coordinate subspace of K^n contained in $\mathbf{V}(I)$. It is easy to show that $\sqrt{I}$ is a monomial ideal and $\mathbf{V}(I) = \mathbf{V}(\sqrt{I})$, it follows immediately that HP_I^a and $HP_{\sqrt{I}}^a$ have the same degree.*

Proposition 2.1.9. *If $I \subseteq K[x_1, \ldots, x_n]$ is an ideal, then the affine hilbert polynomials of I and $\sqrt{I}$ have the same degree.*

Proof. Let I be an arbitrary ideal in $K[x_1, \ldots, x_n]$ and pick any graded order $>$ in $K[x_1, \ldots, x_n]$. We claim that

$$\langle LT(I)\rangle \subseteq \left\langle LT(\sqrt{I})\right\rangle \subseteq \sqrt{\langle LT(I)\rangle}.$$

The first containment is immediate from $I \subseteq \sqrt{I}$. To establish the second, let x^α be a monomial in $LT(\sqrt{I})$. This means that there is a polynomial $f \in \sqrt{I}$ such that $LT(f) = x^\alpha$. We know $f^r \in I$ for some $r \geq 0$, and it follows that $x^{r\alpha} = LT(f^r) \in \langle LT(I)\rangle$. Thus, $x^\alpha \in \sqrt{\langle LT(I)\rangle}$.

It is easy to see that if $I_1 \subseteq I_2$ are any ideals of $K[x_1, \ldots, x_n]$, then *deg* $HP_{I_2}^a \leq$ *deg* $HP_{I_1}^a$. Therefore we obtain the inequalities

$$deg\ HP^a_{\sqrt{\langle LT(I)\rangle}} \leq deg\ HP^a_{\left\langle LT(\sqrt{I})\right\rangle} \leq deg\ HP^a_{\langle LT(I)\rangle}.$$

We conclude that $HP^a_{\left\langle LT(\sqrt{I})\right\rangle}$ and $HP^a_{\langle LT(I)\rangle}$ have the same degree. Then the same is true for HP_I^a and $HP_{\sqrt{I}}^a$. □

Theorem 2.1.10. *For any irreducible affine variety V, dim V is equal to the degree of the affine Hilbert polynomial $HP^a_{\mathbf{I}(V)}$.*

Proof. [7], page 481. □

Proposition 2.1.11. *Assume that K is an infinite field. If V and W are irreducible affine varieties in K^n, then*

$$deg\ HP^a_{\mathbf{I}(V\cup W)} = max\ \{dim\ V,\ dim\ W\}.$$

Proof. Let $I = \mathbf{I}(V)$ and $J = \mathbf{I}(W)$, so that dim $V =$ *deg* HP_I^a and dim $W =$ *deg* HP_J^a . We know that $\mathbf{I}(V \cup W) = I \cap J$. It is more convenient to work with the product ideal IJ and we note that

$$IJ \subseteq I \cap J \subseteq \sqrt{IJ}.$$

We conclude that

$$deg\ HP^a_{\sqrt{IJ}} \leq deg\ HP^a_{I\cap J} \leq deg\ HP^a_{IJ}.$$

We conclude that $deg\ HP^a_{I\cap J} = deg\ HP^a_{IJ}$. Now fix a graded order $>$ on $K[x_1,\ldots,x_n]$. By the last results, it follows that dim V and dim W are given by the maximal dimension of a coordinate subspace contained in $\mathbf{V}(\langle LT(I)\rangle)$ and $\mathbf{V}(\langle LT(J)\rangle)$, also we have that $deg\ HP^a_{IJ}$ is the maximal dimension of a coordinate subspace contained in $\mathbf{V}(\langle LT(IJ)\rangle)$. It is easy to show that

$$\langle LT(I)\rangle \cdot \langle LT(J)\rangle \subseteq \langle LT(IJ)\rangle.$$

This implies

$$\mathbf{V}(\langle LT(IJ)\rangle) \subseteq \mathbf{V}(\langle LT(I)\rangle) \cup \mathbf{V}(\langle LT(J)\rangle).$$

Since K is infinite, every coordinate subspace is irreducible, and as a result, a coordinate subspace contained in $\mathbf{V}(\langle LT(IJ)\rangle)$ lies in either $\mathbf{V}(\langle LT(I)\rangle)$ or $\mathbf{V}(\langle LT(J)\rangle)$. This implies $deg\ HP^a_{\mathbf{I}(V\cup W)} \leq max\ \{$ dim V, dim $W\}$. The opposite inequality is easy to prove. □

Let K be an infinite field and let V be an affine variety in K^n. If $V = V_1\cup\cdots\cup V_r$ is the decomposition of V into irreducible components, then by the last proposition and an induction on r shows that

$$deg\ HP^a_{\mathbf{I}(V)} = max\ \{\ \text{dim}\ V_i \mid i = 1,\ldots,r\}.$$

Then the dimension of an affine variety $V \subseteq K^n$, is the degree of the affine Hilbert polynomial of the corresponding ideal $I = \mathbf{I}(V)$.

Theorem 2.1.12. (The Dimension Theorem) *Let $V = \mathbf{V}(I)$ be an affine variety, where $I \subseteq K[x_1,\ldots,x_n]$ is an ideal. If K is algebraically closed, then*

$$dim\ V = deg\ HP^a_I.$$

Furthermore, if $>$ is a graded order on $K[x_1,\ldots,x_n]$, then

$$\begin{aligned} dim\ V &= deg\ HP^a_{\langle LT(I)\rangle} \\ &= \textit{maximum dimension of a coordinate subspace in } \mathbf{V}(\langle LT(I)\rangle). \end{aligned}$$

Finally, the last two equalities hold over any filed K when $I = \mathbf{I}(V)$.

Proof. Since K is algebraically closed, the Nullstellensatz implies that $\mathbf{I}(V) = \mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$. Then

$$\text{dim}\ V = deg\ HP^a_{\mathbf{I}(V)} = deg\ HP^a_{\sqrt{I}} = deg\ HP^a_I.$$

The second part of the theorem now follows immediately using Propositions 2.1.3 and 2.1.4. □

In other words, over an algebraically closed field, to compute the dimension of a variety $V = \mathbf{V}(I)$, one can proceed as follows:

- Compute a Göbner basis for I using a graded order such as grlex or grevlex.
- Compute the maximum dimension d of a coordinate subspace contained in $\mathbf{V}(\langle LT(I)\rangle)$.

Hilbert Polynomial Let K be an infinite field. Let $K[x_0,\ldots,x_n]_s$ denote the set of homogeneous polynomials of total degree s in $K[x_0,\ldots,x_n]$, together with the zero polynomial. It is easy to show that $K[x_0,\ldots,x_n]_s$ is a vector space of dimension $\binom{n+s}{s}$. If $I \subseteq K[x_0,\ldots,x_n]$ is a homogeneous ideal, we let

$$I_s = I \cap K[x_0,\ldots,x_n]_s$$

denote the set of homogeneous polynomials in I of total degree s (and the zero polynomial). Note that I_s is a vector subspace of $K[x_0,\ldots,x_n]_s$. Then the *Hilbert function* of I is defined by

$$HF_I(s) = dim_K\ K[x_0,\ldots,x_n]_s/I_s.$$

When I is a monomial ideal, $HF_I(s)$ is the number of monomials not in I of total degree s. Also For s sufficiently large, we can express the Hilbert function of a monomial ideal in the form

$$HF_I(s) = \sum_{i=0}^{d} b_i \binom{s}{d-i},$$

where $b_i \in \mathbb{Z}$ and b_0 is positive. We also know that d is the largest dimension of a projective coordinate subspace contained in $\mathbf{V}(I) \subseteq \mathbb{P}^n_K$.

As in the affine case, we can use a monomial order to link the Hilbert function of a homogeneous ideal to the Hilbert function of a monomial ideal.

Proposition 2.1.13. *Let $I \subseteq K[x_0,\ldots,x_n]$ be a homogeneous ideal and let $>$ be a monomial order on $K[x_0,\ldots,x_n]$. Then the monomial ideal $\langle LT(I)\rangle$ has the same Hilbert function as I.*

Proof. The argument is similar to the proof of proposition 2.1.4. However, since we do not require that $>$ be a graded order, some changes are needed.

For a fixed s, we can find $f_1,\ldots,f_m \in I_s$ such that

$$\{LM(f) \mid f \in I_s\} = \{LM(f_1),\ldots,LM(f_m)\},$$

and we can assume that $LM(f_1) > \cdots > LM(f_m)$. As in the proof of Proposition 2.1.4, $f_1,\ldots,f_m$ form a basis of I_s as a vector space over K.

Now consider $\langle LT(I)\rangle_s$. We know $LM(f_i) \in \langle LT(I)\rangle_s$ since $f_i \in I_s$ and we need to show that $LM(f_1),\ldots,LM(f_m)$ form a vector space basis of $\langle LT(I)\rangle_s$. The leading terms are distinct, so as above, they are linearly independent. It remains to prove that they span $\langle LT(I)\rangle_s$. It suffices to show that

$$\{LM(f_1),\ldots,LM(f_m)\} = \{LM(f) \mid f \in I, LM(f) \text{ has total degree } s\}.$$

Suppose that $LM(f)$ has total degree s for some $f \in I$. If we write f as a sum of homogeneous polynomials $f = \sum_i h_i$, where h_i has total degree i, it follows that $LM(f) = LM(h_s)$. Since I is a homogeneous ideal, we have $h_s \in I$. From here, the argument is identical to what we did in Proposition 2.1.4, and we are done. □

If we combine the last proposition with the description of the Hilbert function for a monomial ideal, we see that for any homogeneous ideal $I \subseteq K[x_0, \dots, x_n]$, the Hilbert function can be written as

$$HF_I(s) = \sum_{i=0}^{d} b_i \binom{s}{d-i},$$

for s sufficiently large. The polynomial on the right of this equation is called the *Hilbert polynomial* of I and is denoted by $HP_I(s)$.

Theorem 2.1.14. *Let $I \subseteq K[x_0, \dots, x_n]$ be a homogeneous ideal. Then, for $s \geq 1$, we have*

$$HF_I(s) = HF_I^a(s) - HF_I^a(s-1).$$

There is a similar relation between Hilbert polynomials. Consequently, if $V \subseteq \mathbb{P}_K^n$ is a nonempty projective variety and $C_V \subseteq K^{n+1}$ is its affine cone, then

$$dim\ C_V = deg\ HP_{\mathbf{I_p}(V)} + 1.$$

Proof. Suppose that I is a monomial ideal. We have that $HF_I^a(s)$ is the number of monomials not in I of total degree $\leq s$ and $HF_I^a(s-1)$ is the number of monomials not in I of total degree $\leq s-1$, so $HF_I^a(s) - HF_I^a(s-1)$ is the number of monomials not in I of total degree s, then $HF_I(s) = HF_I^a(s) - HF_I^a(s-1)$. It follows the last equality for an arbitrary homogeneous ideal using Proposition 2.1.11.

For s sufficiently large, we have $HP_I(s) = HP_I^a(s) - HP_I^a(s-1)$. For the second part of the theorem, note that the affine cone C_V is simply the affine variety in K^{n+1} defined by $I_p(V)$. Further, it is easy to see that $I_a(C_V) = I_p(V)$. Then

$$deg\ HP_{\mathbf{I_p}(V)}(s) = deg\ (HP_{I_a(C_V)}^a(s) - HP_{I_a(C_V)}^a(s-1)).$$

Note that $deg\ HP_{I_a(C_V)}^a = dim\ C_V$, therefore $deg\ HP_{\mathbf{I_p}(V)} = dim\ C_V - 1$. □

It follows by the last proposition that if $V \subseteq \mathbb{P}_K^n$ is a nonempty projective variety, then $dim\ V = deg\ HP_{\mathbf{I}(V)}$.

Theorem 2.1.15. (The Dimension Theorem) *Let $V = \mathbf{V}(I) \subseteq \mathbb{P}_K^n$ be a projective variety, where $I \subseteq K[x_0, \dots, x_n]$ is a homogeneous ideal. If V is nonempty and K is algebraically closed, then*

$$dim\ V = deg\ HP_I.$$

Furthermore, for any monomial order on $K[x_0, \dots, x_n]$, we have

$$\textit{dim } V = \textit{deg } HP_{\langle LT(I)\rangle} = \textit{maximum dimension of a projective coordinate subspace in } \mathbf{V}(\langle LT(I)\rangle).$$

Finally, the last two equalities hold over any field K when $I = \mathbf{I}(V)$.

Proof. [7], page 464. □

Proposition 2.1.16. *Let K be an algebraically closed field and let V be a nonempty affine or projective variety. Then V consists of finitely many points if and only if dim $V = 0$.*

Proof. We will give a proof only in the affine case. Let $>$ be a graded order on $K[x_1, \dots, x_n]$. If V is finite, then let a_j, for $j = 1, \dots, m_i$, be the distinct elements of K appearing as i-th coordinates of points of V. Then

$$f = \prod_{j=1}^{m_i}(x_i - a_j) \in \mathbf{I}(V),$$

and we conclude that $LT(f) = x_i^{m_i} \in \langle LT(\mathbf{I}(V))\rangle$. This implies that $\mathbf{V}(\langle LT(\mathbf{I}(V))\rangle) = \{0\}$ and then dimension theorem implies that dim $V = 0$.

Now suppose that dim $V = 0$. Then the affine Hilbert polynomial of $\mathbf{I}(V)$ is a constant C, so that

$$\dim K[x_1, \dots, x_n]_{\leq s}/\mathbf{I}(V)_{\leq s} = C,$$

for s sufficiently large. If we also have $s \geq C$, then the classes $\overline{1}, \overline{x_i}, \dots, \overline{x_i}^s \in K[x_1, \dots, x_n]_{\leq s}/\mathbf{I}(V)_{\leq s}$ are $s+1$ vectors in a vector space of dimension $C \leq s$ and, hence, they must be linearly dependent. But a nontrivial linear relation

$$\overline{0} = \sum_{j=0}^{s} a_j \overline{x_i}^j,$$

means that $\sum_{j=0}^{s} a_j x_i^j$ is a nonzero polynomial in $\mathbf{I}(V)_{\leq s}$. This polynomial vanishes on V, which implies that there are only finitely many distinct i-th coordinates among the points of V. Since this is true for all $1 \leq i \leq n$, it follows that V must be finite. □

2.2 Projective Reed-Muller-Type codes

Linear Codes We introduce some basic notions from coding theory. Let $K = \mathbb{F}_q$ be the finite field with q elements. We consider the n-dimensional vector space $\mathbb{F}_q^n$ whose elements are n-tuples $a = (a_1, \ldots, a_n)$ with $a_i \in \mathbb{F}_q$.

Definition 2.2.1. The *Hamming distance* is the function δ defined by

$$\delta : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{N} \cup \{0\}$$
$$\delta((a_1, \ldots, a_n), (b_1, \ldots, b_n)) = |\{i \mid a_i \neq b_i\}|.$$

The *weight of* an element $a = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ is defined as

$$w(a) = |\{i \mid a_i \neq 0\}|.$$

The Hamming distance is a metric on $\mathbb{F}_q^n$ as one can verify immediately. In particular, the triangle inequality $\delta(a, c) \leq \delta(a, b) + \delta(b, c)$ holds for all $a, b, c \in \mathbb{F}_q^n$.

Definition 2.2.2. A *linear code* C over the alphabet $\mathbb{F}_q$ is a linear subspace of $\mathbb{F}_q^n$. The elements of C are called codewords. We call n the *length* of the code C and $dim_{\mathbb{F}_q} C$ the *dimension* of the code C as an $\mathbb{F}_q$-vector space.

Definition 2.2.3. The *minimum distance* $\delta(C)$ of a code $C \neq 0$ is defined as

$$\delta(C) = min\{\delta(a, b) \mid a, b \in C \text{ and } a \neq b\}.$$

Remark 2.2.4. *As $\delta(a, b) = \delta(a - b, 0) = w(a - b)$ and C is a linear space, the minimum distance is given by*

$$\delta(C) = min\{w(a) \mid 0 \neq a \in C\}.$$

The length, dimension and minimum distance of a code are called its *basic parameters.*

Let $K = \mathbb{F}_q$ be a finite field and let $\mathbb{Y}$ be a subset of $\mathbb{P}_K^{s-1}$. Fix a degree $d \geq 1$. Let $P_1, \ldots, P_m$ be a set of representatives for the points of $\mathbb{Y}$ with $m = |\mathbb{Y}|$. For each i there is $f_i \in S_d$ such that $f_i(P_i) \neq 0$. Indeed suppose $P_i = [(a_1, \ldots, a_s)]$, there is at least one j in $\{1, \ldots, s\}$ such that $a_j \neq 0$. Setting $f_i(t_1, \ldots, t_s) = t_j^d$ one has that $f_i \in S_d$ and $f_i(P_i) \neq 0$. The evaluation map, denoted by ev_d, is defined as:

$$\mathrm{ev}_d \colon S_d = K[t_1, \ldots, t_s]_d \to K^{|\mathbb{Y}|}, \qquad f \mapsto \left(\frac{f(P_1)}{f_1(P_1)}, \ldots, \frac{f(P_m)}{f_m(P_m)}\right). \tag{2.1}$$

Lemma 2.2.5. *The map ev_d is well-defined, i.e., it is independent of the set of representatives that we choose for the points of $\mathbb{Y}$.*

Proof. If $P_1', \ldots, P_m'$ is another set of representatives, there are $\lambda_1, \ldots, \lambda_m$ in K^* such that $P_i' = \lambda_i P_i$ for all i. Thus, $f(P_i')/f_i(P_i') = f(P_i)/f_i(P_i)$ for $f \in S_d$ and $1 \leq i \leq m$. □

The map ev_d defines a linear map of K-vector spaces. The image of S_d under ev_d, denoted by $C_{\mathbb{Y}}(d)$, is called a *projective Reed-Muller-type code* of degree d over $\mathbb{Y}$ [9, 16]. It is also called an *evaluation code* associated to $\mathbb{Y}$ [13].

Remark 2.2.6. *The kernel of the evaluation map* ev_d *is* $\mathbf{I}(\mathbb{Y})_d$. *Hence there is an isomorphism of* K*-vector spaces* $S_d/\mathbf{I}(\mathbb{Y})_d \cong C_{\mathbb{Y}}(d)$.

We will denote the Hilbert function of $\mathbf{I}(\mathbb{Y})$ *by* $H_{\mathbb{Y}}$. *Thus* $H_{\mathbb{Y}}(d)$ *is equal to* $\dim_K C_{\mathbb{Y}}(d)$. *The basic parameters are given by,*

- *The length of* $C_{\mathbb{Y}}(d) \subseteq K^{|\mathbb{Y}|}$ *is* $|\mathbb{Y}|$.
- *The dimension of* $C_{\mathbb{Y}}(d)$ *is* $H_{\mathbb{Y}}(d)$.
- *The minimum distance is* $\delta(C_{\mathbb{Y}}(d)) = \delta_{\mathbb{Y}}(d) = min\{w(v) \mid 0 \neq v \in C_{\mathbb{Y}}(d)\}$.

If $\mathbb{Y} = \mathbb{P}_K^{s-1}$, $C_{\mathbb{Y}}(d)$ is the *classical projective Reed–Muller code*, and formulas for its basic parameters are given in [27, Theorem 1].

Definition 2.2.7. The set $\mathbb{T} = \{[(x_1, \ldots, x_s)] \in \mathbb{P}_K^{s-1} | \, x_i \in K^* \text{ for all } i\}$ is called a *projective torus* in $\mathbb{P}_K^{s-1}$, where $K^* = K \setminus \{0\}$.

Proposition 2.2.8. *The basic parameters of the Reed-Muller-type code* $C_{\mathbb{Y}}(d)$ *are independent of* $f_1, \ldots, f_m$.

Proof. Let $f_1', \ldots, f_m'$ be homogeneous polynomials of S of degree d such that $f_i'(P_i) \neq 0$ for $i = 1, \ldots, m$. Let

$$\mathrm{ev}_d' \colon S_d \to K^{|\mathbb{Y}|}, \qquad f \mapsto \left(\frac{f(P_1)}{f_1'(P_1)}, \ldots, \frac{f(P_m)}{f_m'(P_m)} \right)$$

be the evaluation map relative to $f_1', \ldots, f_m'$. Clearly $\ker(\mathrm{ev}_d) = \ker(\mathrm{ev}_d')$ and $\omega(\mathrm{ev}_d(f)) = \omega(\mathrm{ev}_d'(f))$ for $f \in S_d$. It follows readily that the basic parameters of $\mathrm{ev}_d(S_d)$ and $\mathrm{ev}_d'(S_d)$ are the same. □

Let $\mathbb{T}$ be a projective torus in $\mathbb{P}_K^{s-1}$. If $P = [(a_1, \ldots, a_s)] \in \mathbb{T}$ then $[(1, a_1^{-1}a_2, \ldots, a_1^{-1}a_s)] \in \mathbb{T}$, so we can put

$$\mathbb{T} = \{[(1, a_2, \ldots, a_s)] \mid a_i \in K^*\}.$$

It follows that $|\mathbb{T}| = (q-1)^{s-1}$. Let $\mathbf{I}(P)$ be the ideal generated by the homogeneous polynomial of $K[x_1, \ldots, x_s]$ that vanish at P. We claim that

$$\mathbf{I}(P) = \langle \{a_1 x_i - a_i x_1 \mid i \in \{2, \ldots, s\}\} \rangle.$$

It is clear that $J = \langle \{a_1x_i - a_ix_1 \mid i \in \{2, \ldots, s\}\}\rangle \subseteq \mathbf{I}(P)$. Let $f \in \mathbf{I}(P)$ and $>$ be a monomial order on $K[x_1, \ldots, x_s]$ with the property $x_i > x_1$ for all $i \geq 2$. By the division algorithm, we have that

$$f(x_1, \ldots, x_s) = \sum_{i=2}^{s} h_i(x_1, \ldots, x_s)(a_1x_i - a_ix_1) + r(x_1).$$

Then $r \in \mathbf{I}(P)$, since $\mathbf{I}(P)$ is a homogeneous ideal and $a_1 \neq 0$ we have $r = 0$. It follows that $\mathbf{I}(P) = J$. If $\mathbb{T} = \{P_1, \ldots, P_m\}$ with $m = |\mathbb{T}|$, then

$$\mathbf{I}(\mathbb{T}) = \bigcap_{i=1}^{m} \mathbf{I}(P_m).$$

Theorem 2.2.9. *If $\mathbb{Y} = \mathbb{T}$ is a projective torus in $\mathbb{P}_K^{s-1}$, then*

(i) $\mathbf{I}(\mathbb{T}) = \left\langle \{x_i^{q-1} - x_1^{q-1}\}_{i=2}^{s} \right\rangle$.

(ii) *Let $d \geq 1$, the minimum distance of $C_{\mathbb{Y}}(d)$ is given by*

$$\delta_{\mathbb{Y}}(d) = \begin{cases} (q-1)^{s-(k+2)}(q-1-l) & \text{if } d \leq (q-2)(s-1)-1 \\ 1 & \text{if } d \geq (q-2)(s-1) \end{cases}$$

where k and l are the unique integers such that $k \geq 0$, $1 \leq l \leq q-2$ and $d = k(q-2)+l$.

Proof. [25], pages 17 and 23. □

2.3 Affine Reed-Muller-Type codes

Let $K = \mathbb{F}_q$ be a finite field, let Y be a subset of K^s, and let $\mathbb{Y}$ be the projective closure of Y. As Y is finite, its projective closure is:

$$\mathbb{Y} = \{[(1, \alpha)] \mid \alpha \in Y\} \subset \mathbb{P}_K^s.$$

Let $S = K[x_1, \ldots, x_s]$ 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 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 [30, p. 37]. The kernel of ev_d^a is $\mathbf{I}(Y)_{\leq d}$. Thus $S_{\leq d}/\mathbf{I}(Y)_{\leq d} \cong C_Y(d)$. If Y is a subset of K^s it is usual to denote the affine Hilbert function of $\mathbf{I}(Y)$ by H_Y^a. In our situation one has $H_Y^a(d) = \dim_K C_Y(d)$.

Proposition 2.3.1. *The affine Reed-Muller-type code $C_Y(d)$ has the same basic parameters that the projective Reed-Muller-type code $C_{\mathbb{Y}}(d)$.*

Proof. We set $Q_i = (1, P_i)$ for $i = 1, \dots, m$. Thanks to Lemma 2.2.5 and Proposition 2.2.8 we may take that $Q_1, \dots, Q_m$ as the set of representatives of $\mathbb{Y}$ and assume that $C_{\mathbb{Y}}(d)$ is the image of the linear map

$$\mathrm{ev}_d \colon K[x_0, \dots, x_n]_d \to K^{|\mathbb{Y}|}, \qquad f \mapsto (f(Q_i)/f_0(Q_i))_{i=1}^m\,,$$

where $f_0(x_0, \dots, x_n) = x_0^d$. Let $S = K[x_1, \dots, x_n]$ and $S[x_0] = K[x_0, \dots, x_n]$, we know that

$$S_{\leq d}/\mathbf{I}(Y)_{\leq d} \cong C_Y(d) = \{(f(P_1), \dots, f(P_m)) \mid f \in S_{\leq d}\}.$$

The homogenization map $\varphi : S_{\leq d} \to S[x_0]_d$, $f \to f^h$, is an isomorfism of K-vector spaces such that $\varphi(\mathbf{I}(Y)_{\leq d}) = \mathbf{I}(\mathbb{Y})_d$. Hence, the induced map

$$\varphi : S_{\leq d} \to S[x_0]_d/\mathbf{I}(\mathbb{Y})_d,\ f \to f^h + \mathbf{I}(\mathbb{Y})_d,$$

is a surjection. Note that $Ker(\varphi) = \mathbf{I}(Y)_{\leq d}$. It follows that $C_Y(d) \cong C_{\mathbb{Y}}(d)$ as a vector spaces, then $C_Y(d)$ and $C_{\mathbb{Y}}(d)$ have the same dimension, it is clear that both codes have the same length. □

Proposition 2.3.2. $C_Y(d) = C_{\mathbb{Y}}(d)$ *for* $d \geq 1$.

Proof. Since $S[u]_d/\mathbf{I}(\mathbb{Y})_d \cong C_{\mathbb{Y}}(d)$ and $S_{\leq d}/\mathbf{I}(Y)_{\leq d} \cong C_Y(d)$, by Proposition 2.3.1, we get that the linear codes $C_Y(d)$ and $C_{\mathbb{Y}}(d)$ have the same dimension, and the same length. Thus, it suffices to show the inclusion "$\supset$". Any point of $C_{\mathbb{Y}}(d)$ has the form $W = (f(1, P_i))_{i=1}^m$, where $P_1, \dots, P_m$ are the points of Y and $f \in S[x_0]_d$. If $\widetilde{f}$ is the polynomial $f(1, x_1, \dots, x_n)$, then $\widetilde{f}$ is in $S_{\leq d}$ and $f(1, P_i) = \widetilde{f}(P_i)$ for all i. Thus, W is in $C_Y(d)$, as required. □

This means that affine Reed-Muller-type codes are a particular case of projective Reed-Muller-type-codes and are somewhat easier to understand.

Chapter 3

Parameterized Affine Codes and Affine Cartesian Codes

In this chapter we give an algebraic method, using Gröbner bases, to compute the length and the dimension of Reed-Muller-type codes over affine algebraic toric sets parameterized by monomials. Then we compute the basic parameters of affine cartesian codes, and construct a cartesian code, over a degenerate torus with prescribed parameters and a certain type. Finally we show some examples with Macaulay 2.0 and construct some tables illustrating the main results.

3.1 Parameterized affine codes

Let K be a finite field. In this section we introduce the concept of an *affine algebraic toric set* parameterized by monomials, it will be denoted by X^*. We give an algebraic method, using Gröbner bases, to compute the length and the dimension of $C_{X^*}(d)$, the parameterized affine code of degree d on the set X^*. If $\mathbb{Y}$ is the projective closure of X^*, it is shown that $C_{X^*}(d)$ has the same basic parameters that $C_{\mathbb{Y}}(d)$, the *parameterized projective code* on the set Y. We show how to compute the vanishing ideals of X^* and $\mathbb{Y}$.

Let $K = \mathbb{F}_q$ be a finite field with q elements and let $x^{v_1}, \ldots, x^{v_s}$ be a finite set of monomials. As usual if $v_i = (v_{i1}, \ldots, v_{in}) \in \mathbb{N}^n$, then we set

$$x^{v_i} = x_1^{v_{i1}} \cdots x_n^{v_{in}}, \qquad i = 1, \ldots, s,$$

where $x_1, \ldots, x_n$ are the indeterminates of a ring of polynomials with coefficients in K. Consider the following set parameterized by these monomials

$$X^* := \{(x_1^{v_{11}} \cdots x_n^{v_{1n}}, \ldots, x_1^{v_{s1}} \cdots x_n^{v_{sn}}) \in K^s |\, x_i \in K^* \text{ for all } i\},$$

where $K^* = K\backslash\{0\}$. We call X^* an *affine algebraic toric set* parameterized by $x^{v_1}, \ldots, x^{v_s}$. The set X^* is a multiplicative group under componentwise multiplication.

Let $\mathbb{P}^s_K$ be a projective space over the field K. Consider the algebraic toric set

$$\mathbb{Y} := \{[(1, x_1^{v_{11}} \cdots x_n^{v_{1n}}, \ldots, x_1^{v_{s1}} \cdots x_n^{v_{sn}})] \,|\, x_i \in K^* \text{ for all } i\} \subset \mathbb{P}^s_K,$$

Notice that Y is parameterized by $x^{v_0}, x^{v_1}, \ldots, x^{v_s}$, where $v_0 = 0$. Also notice that $\mathbb{Y}$ is the projective closure of X^* because K is a finite field.

Computing the dimension and length of $C_{X^*}(d)$

Theorem 3.1.1. (Combinatorial Nullstellensatz) *Let $R = K[y_1, \ldots, y_n]$ be a polynomial ring over a field K, let $f \in R$, and let $a = (a_i) \in \mathbb{N}^n$. Suppose that the coefficient of y^a in f is non-zero and $\deg(f) = a_1 + \cdots + a_n$. If $S_1, \ldots, S_n$ are subsets of K, with $|S_i| > a_i$ for all i, then there are $s_1 \in S_1, \ldots, s_n \in S_n$ such that $f(s_1, \ldots, s_n) \neq 0$.*

Lemma 3.1.2. *Let $K = \mathbb{F}_q$ and let G be a polynomial in $K[y_1, \ldots, y_n]$. If G vanishes on $(K^*)^n$ and $\deg_{y_i}(G) < q - 1$ for $i = 1, \ldots, n$, then $G = 0$.*

Proof. We proceed by contradiction. Assume that G is non-zero. Then, there is a monomial y^a that occurs in G with $\deg(G) = a_1 + \cdots + a_n$, where $a = (a_1, \ldots, a_n)$ and $a_i > 0$ for some i. We set $S_i = K^*$ for all i. As $\deg_{y_i}(G) < q - 1$ for all i, then $a_i < |S_i| = q - 1$ for all i. Thus, by the last theorem, there are $x_1, \ldots, x_n \in K^*$ so that $G(x_1, \ldots, x_n) \neq 0$, a contradiction to the fact that G vanishes on $(K^*)^n$. □

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

Lemma 3.1.3. *Let $B = K[t_1, \ldots, t_s, y_1, \ldots, y_n]$ be a polynomial ring over an arbitrary field K. If I' is a binomial ideal of B, then $I' \cap K[t_1, \ldots, t_s]$ is a binomial ideal.*

Proof. Let $S = K[t_1, \ldots, t_s]$ and let $\mathcal{G}$ be a Gröbner basis of I' with respect to the lexicographic order $y_1 > \cdots > y_n > t_1 > \cdots > t_s$. By Buchberger algorithm (see Theorem 1.3.24) the set $\mathcal{G}$ consists of binomials and by elimination theory (see Theorem 1.3.33) the set $\mathcal{G} \cap S$ is a Gröbner basis of $I' \cap S$. Hence $I' \cap S$ is a binomial ideal. See the proof of [29, Corollary 4.4, p. 32] for additional details. □

Theorem 3.1.4. *Let $B = K[t_1, \ldots, t_s, y_1, \ldots, y_n]$ be a polynomial ring over a finite field K with q elements. Then*

$$\mathbf{I}(X^*) = \left(t_1 - y^{v_1}, \ldots, t_s - y^{v_s}, y_1^{q-1} - 1, \ldots, y_n^{q-1} - 1\right) \cap S$$

and $\mathbf{I}(X^*)$ is a binomial ideal.

Proof. We set $I' = \left(t_1 - y^{v_1}, \ldots, t_s - y^{v_s}, y_1^{q-1} - 1, \ldots, y_n^{q-1} - 1\right) \subset B$. First we show the inclusion $\mathbf{I}(X^*) \subset I' \cap S$. Take a polynomial $F = F(t_1, \ldots, t_s)$ that vanishes on X^*. Let $>_{lex}$ be the lex order on B, suppose that $t_1 >_{lex} t_2 >_{lex} \cdots >_{lex} t_s >_{lex} y_1 >_{lex} \cdots >_{lex} y_n$. By the division algorithm we can write

$$F=\sum_{i=1}^{s} g_i(t_i-y^{v_i})+\sum_{i=1}^{n} h_i(y_i^{q-1}-1)+G(y_1,\ldots,y_n). \tag{3.1}$$

Where $\deg_{y_i}(G)<q-1$ for $i=1,\ldots,n$. Thus to show that $F\in I'\cap S$ we need only show that $G=0$. We claim that G vanishes on $(K^*)^n$. Take an arbitrary sequence $x_1,\ldots,x_n$ of elements of K^*. Making $t_i=x^{v_i}$ for all i in Eq. (3.1) and using that F vanishes on X^*, we obtain

$$0=F(x^{v_1},\ldots,x^{v_s})=\sum_{i=1}^{s} g_i'(x^{v_i}-y^{v_i})+\sum_{i=1}^{n} h_i(y_i^{q-1}-1)+G(y_1,\ldots,y_n), \tag{3.2}$$

where $g_i'=g_i(x^{v_1},\ldots,x^{v_s},y_1,\ldots,y_n)$. Since $(K^*,\,\cdot\,)$ is a group of order $q-1$, we can then make $y_i=x_i$ for all i in Eq. (3.2) to get that G vanishes on $(x_1,\ldots,x_n)$. This completes the proof of the claim. Therefore G vanishes on $(K^*)^n$ and $\deg_{y_i}(G)<q-1$ for all i. Hence $G=0$ by Lemma 3.1.2.

Next we show the inclusion $\mathbf{I}(X^*)\supset I'\cap S$. Take a polynomial f in $I'\cap S$. Then we can write

$$f=\sum_{i=1}^{s} g_i(t_i-y^{v_i})+\sum_{i=1}^{n} h_i(y_i^{q-1}-1) \tag{3.3}$$

for some polynomials $g_1,\ldots,g_s,h_1,\ldots,h_n$ in B. Take a point $P=(x^{v_1},\ldots,x^{v_s})$ in X^*. Making $t_i=x^{v_i}$ in Eq. (3.3), we get

$$f(x^{v_1},\ldots,x^{v_s})=\sum_{i=1}^{s} g_i'(x^{v_i}-y^{v_i})+\sum_{i=1}^{n} h_i'(y_i^{q-1}-1),$$

where $g_i'=g_i(x^{v_1},\ldots,x^{v_s},y_1,\ldots,y_n)$ and $h_i'=h_i(x^{v_1},\ldots,x^{v_s},y_1,\ldots,y_n)$. Hence making $y_i=x_i$ for all i, we get that $f(P)=0$. Thus f vanishes on X^*. □

For infinite fields, we can use the Combinatorial Nullstellensatz (see Theorem 3.1.1) to show the following description of $\mathbf{I}(X^*)$.

Proposition 3.1.5. *Let $B=K[t_1,\ldots,t_s,y_1,\ldots,y_n]$ be a polynomial ring over an infinite field K. Then*

$$\mathbf{I}(X^*)=(t_1-y^{v_1},\ldots,t_s-y^{v_s})\cap S.$$

Proposition 3.1.6. *The dimension and the length of $C_{X^*}(d)$ can be computed using Gröbner basis.*

Proof. By Lemma 1.4.13 we can find a generating set of $\mathbf{I}(\mathbb{Y})$ using Gröbner basis. Thus, using the computer algebra system *Macaulay*2 [10, 17], we can compute the Hilbert function and the degree of $S[u]/\mathbf{I}(\mathbb{Y})$, i.e., we can compute the dimension and the length of $C_{\mathbb{Y}}(d)$. Consequently, Theorem 2.3.2 allows to compute the dimension and the length of $C_{X^*}(d)$ using Gröbner basis. □

Putting the results of this section together we obtain the following procedure. For *Macaulay*2 that computes the dimension and the length of a parameterized affine code $C_{X^*}(d)$ of degree d.

```
R=GF(q)[y1,...,yn,t1,...,ts,u,MonomialOrder=>Eliminate n]
I'=ideal(t1-y1^{v_1},...,t_s-y^{s},y1^{q-1}-1,...,yn^{q-1}-1)
I(X^*)=ideal selectInSubring(1,gens gb I')
I(Y)'=homogenize(I(X^*),u)
S=GF(q)[t1,...,ts,u]
I(Y)=substitute(I(Y)',S)
degree I(Y)
hilbertFunction(d,I(Y))
```

Example 3.1.7. *Let X^* be the affine algebraic toric set parameterized by y_1y_2, y_2y_3, y_1y_3 and let $C_{X^*}(d)$ be its parameterized affine code of order d over the field $K = \mathbb{F}_5$. Using* Macaulay2*, together with the last procedure, we obtain:*

$$\begin{aligned}
\mathbf{I}(X^*) &= (t_3^4 - 1, t_2^2t_3^2 - t_1^2, t_1^2t_3^2 - t_2^2, t_2^4 - 1, t_1^2t_2^2 - t_3^2, t_1^4 - 1),\\
\mathbf{I}(\mathbb{Y}) &= (t_3^4 - t_4^4, t_2^2t_3^2 - t_1^2t_4^2, t_1^2t_3^2 - t_2^2t_4^2, t_2^4 - t_4^4, t_1^2t_2^2 - t_3^2t_4^2, t_1^4 - t_4^4),
\end{aligned}$$

d	1	2	3	4	5
$\lvert X^*\rvert$	32	32	32	32	32
$\dim C_{X^*}(d)$	4	10	20	29	32
$\delta_{X^*}(d)$	23	8			1

*The minimum distance was also computed with Macaulay*2*.*

3.2 Affine Cartesian codes

In this section, we are going to compute the basic parameters (dimension, length, minimum distance) of affine evaluation codes defined on a cartesian product of finite sets. Given a sequence of positive integers, we construct an evaluation code, over a degenerate torus, with prescribed parameters of a certain type. As an application of our results, we recover the formulas for the minimum distance of various families of evaluation codes.

Let K be an arbitrary field and let $A_1, \ldots, A_n$ be a collection of non-empty subsets of K with a finite number of elements. Consider the following finite sets: (a) the *cartesian product*

$$X^* := A_1 \times \cdots \times A_n \subset K^n,$$

and (b) the *projective closure* of X^*

$$\mathbb{Y} := \{[(1, \gamma_1, \ldots, \gamma_n)] \mid \gamma_i \in A_i \text{ for all } i\} \subset \mathbb{P}^n_K,$$

where $\mathbb{P}_K^n$ is a projective space over the field K. We also consider X, the image of $X^* \setminus \{0\}$ under the map $K^n \setminus \{0\} \mapsto \mathbb{P}_K^{n-1}$, $\gamma \mapsto [\gamma]$. In what follows d_i denotes $|A_i|$, the cardinality of A_i for $i = 1, \dots, n$. We may always assume that $2 \leq d_i \leq d_{i+1}$ for all i (see Proposition 3.2.5).

Lemma 3.2.1. *Let f_i be the polynomial $\prod_{\gamma \in A_i}(t_i - \gamma)$ for $1 \leq i \leq n$. Then*

$$\mathbf{I}(X^*) = (f_1, \dots, f_n).$$

Proof. "$\supseteq$" This inclusion is clear because f_i vanishes on X^* by construction. "$\subseteq$" Take f in $\mathbf{I}(X^*)$. Let $>$ be the reverse lexicographical order on the monomials of $S = K[t_1, \dots, t_n]$. By the division algorithm (see Theorem 1.3.4), we can write

$$f = g_1 f_1 + \cdots + g_n f_n + G,$$

where each of the terms of G is not divisible by any of the leading monomials $t_1^{d_1}, \dots, t_n^{d_n}$, i.e., $\deg_{t_i}(G) < d_i$ for all i. As G belongs to $\mathbf{I}(X^*)$, by Lemma 3.1.2, we get that $G = 0$. Thus, $f \in (f_1, \dots, f_n)$. □

Let $S[u] = K[t_1, \dots, t_n, u]$ and $h_{\mathbb{Y}}(t) = \sum_{i=0}^{k-1} c_i t^i \in \mathbb{Z}[t]$ be the *Hilbert polynomial* of $\mathbf{I}(\mathbb{Y})$ of degree

$$k - 1 = \dim(S[u]/\mathbf{I}(\mathbb{Y})) - 1.$$

Then $h_{\mathbb{Y}}(d) = H_{\mathbb{Y}}(d)$ for $d \gg 0$, see Hilbert Theorem. The integer $c_{k-1}(k-1)!$, denoted by $\deg(S[u]/\mathbf{I}(\mathbb{Y}))$, is called the *degree* or *multiplicity* of $S[u]/\mathbf{I}(\mathbb{Y})$.

Definition 3.2.2. A homogeneous ideal $I \subset S$ is called a *complete intersection* if there exists homogeneous polynomials $g_1, \dots, g_r$ such that $I = (g_1, \dots, g_r)$, where r is the height of I.

Proposition 3.2.3. (a) $\mathbf{I}(\mathbb{Y}) = (\prod_{\gamma \in A_1}(t_1 - u\gamma), \dots, \prod_{\gamma \in A_n}(t_n - u\gamma))$.

(b) $\mathbf{I}(\mathbb{Y})$ *is a complete intersection.*

(c) $\operatorname{reg} S[u]/\mathbf{I}(\mathbb{Y}) = \sum_{i=1}^{n}(d_i - 1)$ *and* $\deg(S[u]/\mathbf{I}(\mathbb{Y})) = |\mathbb{Y}| = d_1 \cdots d_n$.

Proof. (a) For $i = 1, \dots, n$, we set $f_i = \prod_{\gamma \in A_i}(t_i - \gamma)$. Let $>$ be the reverse lexicographical order on the monomials of $S[u]$. Since $f_1, \dots, f_n$ form a Gröbner basis with respect to this order, by Lemma 3.2.1 and Theorem 1.4.13, the vanishing ideal $\mathbf{I}(\mathbb{Y})$ is equal to $(f_1^h, \dots, f_n^h)$, where $f_i^h = \prod_{\gamma \in A_i}(t_i - u\gamma)$ is the homogenization of f_i with respect to a new variable u. Part (b) follows from (a) because $\mathbf{I}(\mathbb{Y})$ is an ideal of height n [12]. (c) This part follows directly from [9, Corollary 2.6]. □

Cartesian Evaluation Codes In this part we compute the basic parameters of cartesian codes and give some applications. If d is at most $\sum_{i=1}^{n}(d_i-1)$, we show an upper bound in terms of $d_1,\ldots,d_n$ on the number of roots, over X^*, of polynomials in $S_{\leq d}$ which do not vanish at all points of X^*.

We begin by computing some of the basic parameters of $C_{X^*}(d)$, the cartesian evaluation code of degree d on X^*.

Theorem 3.2.4. *The length of $C_{X^*}(d)$ is $d_1\cdots d_n$, its minimum distance is 1 for $d\geq\sum_{i=1}^{n}(d_i-1)$, and its dimension is*

$$H_{X^*}(d)=\binom{n+d}{d}-\sum_{1\leq i\leq n}\binom{n+d-d_i}{d-d_i}+\sum_{i<j}\binom{n+d-(d_i+d_j)}{d-(d_i+d_j)}-$$
$$\sum_{i<j<k}\binom{n+d-(d_i+d_j+d_k)}{d-(d_i+d_j+d_k)}+\cdots+(-1)^n\binom{n+d-(d_1+\cdots+d_n)}{d-(d_1+\cdots+d_n)}.$$

Proof. The length of $C_{X^*}(d)$ is $|X^*|=d_1\cdots d_n$. We set $r=\sum_{i=1}^{n}(d_i-1)$. By Proposition 3.2.3, the regularity of $\mathbf{I}(\mathbb{Y})$ is equal to r, i.e., $H_{\mathbb{Y}}(d)=|\mathbb{Y}|$ for $d\geq r$. We know that $|X^*|=|\mathbb{Y}|$, thus, by Lemma 2.3.1, $H_{X^*}(d)=|X^*|$ for $d\geq r$, i.e., $C_{X^*}(d)=K^{|X^*|}$ for $d\geq r$. Hence $\delta_{X^*}(d)=1$ for $d\geq r$. By Proposition 3.2.3, the ideal $\mathbf{I}(\mathbb{Y})$ is a complete intersection generated by n homogeneous polynomials $f_1,\ldots,f_n$ of degrees $d_1,\ldots,d_n$. Thus, applying [9, Corollary 2.6] and using the equality $H_{X^*}(d)=H_{\mathbb{Y}}(d)$, we obtain the required formula for the dimension. □

Proposition 3.2.5. *If $d_1=1$ and $X'=A_2\times\cdots\times A_n$, then $C_{X^*}(d)=C_{X'}(d)$ for $d\geq 1$.*

Proof. Let α be the only element of A_1 and let Y' be the projective closure of X'. Then, by Proposition 3.2.3, we get

$$\mathbf{I}(Y)=(t_1-u\alpha,f_2^h,\ldots,f_n^h)\ \text{ and }\ \mathbf{I}(Y')=(f_2^h,\ldots,f_n^h),$$

where $f_i^h=\prod_{\gamma\in A_i}(t_i-u\gamma)$ for $i=2,\ldots,n$. Since $\mathbf{I}(\mathbb{Y})$ and $\mathbf{I}(Y')\subseteq K[t_2,\ldots,t_n,u]$ have the same Hilbert function, we get that the dimension and the length of $C_{X^*}(d)$ and $C_{X'}(d)$ are the same. Thus, to show the equality $C_{X^*}(d)=C_{X'}(d)$, it suffices to show the inclusion "$\subset$". Any element of $C_{X^*}(d)$ has the form

$$W=(f(\alpha,Q_1),\ldots,f(\alpha,Q_m)),$$

where $Q_1,\ldots,Q_m$ are the points of X' and $f\in S_{\leq d}$. If $\widetilde{f}$ is the polynomial $f(\alpha,t_2,\ldots,t_n)$, then $\widetilde{f}$ is in $K[t_2,\ldots,t_n]_{\leq d}$ and $f(\alpha,Q_i)=\widetilde{f}(Q_i)$ for all i. Thus, W is in $C_{X'}(d)$, as required. □

Since permuting the sets $A_1,\ldots,A_n$ does not affect neither the parameters of the corresponding cartesian evaluation codes, nor the invariants of the corresponding vanishing ideal, by Proposition 3.2.5 we may always assume that $2\leq d_i\leq d_{i+1}$ for all i, where $d_i=|A_i|$.

For $G \in S$, we denote the zero set of G in X^* by $Z_{X^*}(G)$. We begin with a general bound that will be refined later in this section. The proof of [24, Lemma 3A, p. 147] can be easily adapted to obtain the following auxiliary result.

Lemma 3.2.6. *Let $0 \neq G = G(t_1, \ldots, t_n) \in S$ be a polynomial of total degree d. If $d_i \leq d_{i+1}$ for all i, then*

$$|Z_{X^*}(G)| \leq \begin{cases} d_2 \cdots d_n d & \text{if } n \geq 2, \\ d & \text{if } n = 1. \end{cases}$$

Proof. By induction on $n + d \geq 1$. If $n + d = 1$, then $n = 1$, $d = 0$ and the result is obvious. If $n = 1$, then the result is clear because G has at most d roots in K. Thus, we may assume $d \geq 1$ and $n \geq 2$. We can write G as

$$G = G(t_1, \ldots, t_n) = G_0(t_1, \ldots, t_{n-1}) + G_1(t_1, \ldots, t_{n-1})t_n + \cdots + G_r(t_1, \ldots, t_{n-1})t_n^r, \quad (\dagger)$$

where $G_r \neq 0$ and $0 \leq r \leq d$. Let $\beta_1, \ldots, \beta_{d_1}$ be the elements of A_1. We set

$$H_k = H_k(t_2, \ldots, t_n) := G(\beta_k, t_2, \ldots, t_n) \quad \text{for} \quad 1 \leq k \leq d_1.$$

Case (I): $H_k(t_2, \ldots, t_n) = 0$ for some $1 \leq k \leq d_1$. From Eq. ($\dagger$) we get

$$H_k(t_2, \ldots, t_n) = G_0(\beta_k, t_2, \ldots, t_{n-1}) + G_1(\beta_k, t_2, \ldots, t_{n-1})t_n + \cdots + G_r(\beta_k, t_2, \ldots, t_{n-1})t_n^r = 0.$$

Therefore $G_i(\beta_k, t_2, \ldots, t_{n-1}) = 0$ for $i = 0, \ldots, r$. Hence $t_1 - \beta_k$ divides $G_i(t_1, \ldots, t_{n-1})$ for all i. Thus, by Eq. ($\dagger$), we can write

$$G(t_1, \ldots, t_n) = (t_1 - \beta_k)G'(t_1, \ldots, t_n)$$

for some $G' \in S$. Notice that $\deg(G') + n = d - 1 + n < d + n$. Hence, by induction, we get

$$|Z_{X^*}(G)| \leq |Z_{X^*}(t_1 - \beta_k)| + |Z_{X^*}(G'(t_1, \ldots, t_n))| \leq d_2 \cdots d_n + d_2 \cdots d_n(d-1) = d_2 \cdots d_n d.$$

Case (II): $H_k(t_2, \ldots, t_n) \neq 0$ for $1 \leq k \leq d_1$. Observe the inclusion

$$Z_{X^*}(G) \subset \bigcup_{k=1}^{d_1} (\{\beta_k\} \times Z(H_k)),$$

where $Z(H_k) = \{a \in A_2 \times \cdots \times A_n \mid H_k(a) = 0\}$. As $\deg(H_k) + n - 1 < d + n$ and $d_i \leq d_{i+1}$ for all i, then by induction

$$|Z_{X^*}(G)| \leq \sum_{k=1}^{d_1} |Z(H_k)| \leq d_1 d_3 \cdots d_n d \leq d_2 d_3 \cdots d_n d,$$

as required. □

Lemma 3.2.7. *Let $d_1,\ldots,d_{n-1},d',d$ be positive integers such that $d=\sum_{i=1}^{k}(d_i-1)+\ell$ and $d'=\sum_{i=1}^{k'}(d_i-1)+\ell'$ for some integers k,k',ℓ,ℓ' satisfying that $0\leq k,k'\leq n-2$ and $1\leq \ell\leq d_{k+1}-1$, $1\leq \ell'\leq d_{k'+1}-1$. If $d'\leq d$ and $d_i\leq d_{i+1}$ for all i, then $k'\leq k$ and*

$$-d_{k'+1}\cdots d_{n-1}+\ell' d_{k'+2}\cdots d_{n-1}\leq -d_{k+1}\cdots d_{n-1}+\ell d_{k+2}\cdots d_{n-1}, \qquad (*)$$

where $d_{k+2}\cdots d_{n-1}=1$ (resp., $d_{k'+2}\cdots d_{n-1}=1$) if $k=n-2$ (resp., $k'=n-2$).

Proof. First we show that $k'\leq k$. If $k'>k$, from the equality

$$\ell=(d-d')+\ell'+[(d_{k+1}-1)+\cdots+(d_{k'+1}-1)],$$

we obtain that $\ell\geq d_{k+1}$, a contradiction. Thus, $k'\leq k$. Since $d_{k+2}\cdots d_{n-1}$ is a common factor of each term of Eq. $(*)$, we need only show the equivalent inequality:

$$d_{k+1}-\ell\leq (d_{k'+1}-\ell')d_{k'+2}\cdots d_{k+1}. \qquad (**)$$

If $k=k'$, then $d_{k'+2}\cdots d_{k+1}=1$ and $d-d'=\ell-\ell'\geq 0$. Hence, $\ell\geq\ell'$ and Eq. $(**)$ holds. If $k\geq k'+1$, then

$$d_{k+1}-\ell\leq d_{k+1}\leq d_{k'+2}\cdots d_{k+1}\leq d_{k'+2}\cdots d_{k+1}(d_{k'+1}-\ell').$$

Thus, Eq. $(**)$ holds. □

Lemma 3.2.8. *If $0\neq G\in S$. Then, there are $r\geq 0$ distinct elements $\beta_1,\ldots,\beta_r$ in A_n and $G'\in S$ such that*

$$G=(t_n-\beta_1)^{a_1}\cdots(t_n-\beta_r)^{a_r}G',\qquad a_i\geq 1 \textit{ for all } i,$$

and $G'(t_1,\ldots,t_{n-1},\gamma)\neq 0$ for any $\gamma\in A_n$.

Proof. Fix a monomial ordering in S. If the degree of G is zero, we set $r=0$ and $G=G'$. Assume that $\deg(G)>0$. If $G(t_1,\ldots,t_{n-1},\gamma)\neq 0$ for all $\gamma\in A_n$, we set $G=G'$ and $r=0$. If $G(t_1,\ldots,t_{n-1},\gamma)=0$ for some $\gamma\in A_n$, then by the division algorithm there are F and H in S such that $G=(t_n-\gamma)F+H$, where H is a polynomial whose terms are not divisible by the leading term of $t_n-\gamma$, i.e., H is a polynomial in $K[t_1,\ldots,t_{n-1}]$. Thus, as $G(t_1,\ldots,t_{n-1},\gamma)=0$, we get that $H=0$ and $G=(t_n-\gamma)F$. Since $\deg(F)<\deg(G)$, the result follows using induction on the total degree of G. □

Proposition 3.2.9. *Let $G=G(t_1,\ldots,t_n)\in S$ be a polynomial of total degree $d\geq 1$ such that $\deg_{t_i}(G)\leq d_i-1$ for $i=1,\ldots,n$. If $d_i\leq d_{i+1}$ for all i and $d=\sum_{i=1}^{k}(d_i-1)+\ell$ for some integers k,ℓ such that $1\leq\ell\leq d_{k+1}-1$, $0\leq k\leq n-1$, then*

$$|Z_{X^*}(G)|\leq d_{k+2}\cdots d_n(d_1\cdots d_{k+1}-d_{k+1}+\ell),$$

where we set $d_{k+2}\cdots d_n=1$ if $k=n-1$.

Proof. We proceed by induction on n. By Lemma 3.2.8, there are $r \geq 0$ distinct elements $\beta_1, \ldots, \beta_r$ in A_n and $G' \in S$ such that

$$G = (t_n - \beta_1)^{a_1} \cdots (t_n - \beta_r)^{a_r} G', \qquad a_i \geq 1 \text{ for all } i,$$

and $G'(t_1, \ldots, t_{n-1}, \gamma) \neq 0$ for any $\gamma \in A_n$. Notice that $r \leq \sum_{i=1}^{r} a_i \leq d_n - 1$ because the degree of G in t_n is at most $d_n - 1$. We may assume that $A_n = \{\beta_1, \ldots, \beta_{d_n}\}$. Let d_i' be the degree of $G'(t_1, \ldots, t_{n-1}, \beta_i)$ and let $d' = \max\{d_i' | \ r+1 \leq i \leq d_n\}$.

Case (I): Assume $n = 1$. Then, $k = 0$ and $d = \ell$. Then $|Z_{X^*}(G)| \leq \ell$ because a non-zero polynomial in one variable of degree d has at most d roots.

Case (II): Assume $n \geq 2$ and $k = 0$. Then, $d = \ell \leq d_1 - 1$. Hence, by Lemma 3.2.6, we get

$$|Z_{X^*}(G)| \leq d_2 \cdots d_n d = d_2 \cdots d_n \ell = d_{k+2} \cdots d_n (d_1 \cdots d_{k+1} - d_{k+1} + \ell),$$

as required.

Case (III): Assume $n \geq 2$, $k \geq 1$ and $d' = 0$. Then, $|Z_{X^*}(G)| = r d_1 \cdots d_{n-1}$. Thus, it suffices to show the inequality

$$r d_1 \cdots d_{n-1} \leq d_1 \cdots d_n - d_{k+1} \cdots d_n + \ell d_{k+2} \cdots d_n.$$

All terms of this inequality have $d_{k+2} \cdots d_{n-1}$ as a common factor. Hence, this case reduces to showing the following equivalent inequality

$$r d_1 \cdots d_{k+1} \leq d_n (d_1 \cdots d_{k+1} - d_{k+1} + \ell).$$

We can write $d_n = r + 1 + \delta$ for some $\delta \geq 0$. If we substitute d_n by $r + 1 + \delta$, we get the equivalent inequality

$$d_{k+1}(r+1) \leq \ell r + d_1 \cdots d_{k+1} + \ell + \delta d_1 \cdots d_{k+1} - \delta d_{k+1} + \delta \ell.$$

We can write $d = r + \delta_1$ for some $\delta_1 \geq 0$. Next, if we substitute r by $\sum_{i=1}^{k}(d_i - 1) + \ell - \delta_1$ on the left hand side of this inequality, we get

$$0 \leq \ell[r + 1 + \delta - d_{k+1}] + d_{k+1}[d_1 \cdots d_k - 1 - \textstyle\sum_{i=1}^{k}(d_i - 1) + \delta_1] + \delta[d_1 \cdots d_{k+1} - d_{k+1}].$$

Since $r + 1 + \delta - d_{k+1} \geq r + 1 + \delta - d_n = 0$ and $k \geq 1$, this inequality holds. This completes the proof of this case.

Case (IV): Assume $n \geq 2$, $k \geq 1$ and $d' \geq 1$. We may assume that $\beta_{r+1}, \ldots, \beta_m$ are the elements β_i of $\{\beta_{r+1}, \ldots, \beta_{d_n}\}$ such that $G'(t_1, \ldots, t_{n-1}, \beta_i)$ has positive degree. We set

$$G_i' = G'(t_1, \ldots, t_{n-1}, \beta_i)$$

for $r + 1 \leq i \leq m$. Notice that $d = \sum_{i=1}^{r} a_i + \deg(G') \geq r + d' \geq d_i'$. The polynomial

$$H := (t_n - \beta_1)^{a_1} \cdots (t_n - \beta_r)^{a_r}$$

has exactly $rd_1\cdots d_{n-1}$ roots in X^*. Hence, counting the roots of G' that are not in $Z_{X^*}(H)$, we obtain:

$$|Z_{X^*}(G)| \leq rd_1\cdots d_{n-1} + \sum_{i=r+1}^{m} |Z(G_i')|, \tag{$\star$}$$

where $Z(G_i')$ is the set of zeros of G_i' in $A_1 \times \cdots \times A_{n-1}$. For each $r+1 \leq i \leq m$, we can write $d_i' = \sum_{i=1}^{k_i'}(d_i - 1) + \ell_i'$, with $1 \leq \ell_i' \leq d_{k_i'+1} - 1$. The proof of this case will be divided in three subcases.

Subcase (IV.a): Assume $\ell \geq r$ and $k = n-1$. The degree of G_i' in the variable t_j is at most $d_j - 1$ for $j = 1, \ldots, n-1$. Hence, by Lemma 3.1.2, the non-zero polynomial G_i' cannot be the zero-function on $A_1 \times \cdots \times A_{n-1}$. Therefore, $|Z(G_i')| \leq d_1\cdots d_{n-1} - 1$ for $r+1 \leq i \leq m$. Thus, by Eq. ($\star$), we get the required inequality

$$|Z_{X^*}(G)| \leq rd_1\cdots d_{n-1} + (d_n - r)(d_1\cdots d_{n-1} - 1) \leq d_1\cdots d_n - d_n + \ell,$$

because in this case $d_{k+2}\cdots d_n = 1$ and $\ell \geq r$.

Subcase (IV.b): Assume $\ell > r$ and $k \leq n-2$. Then, we can write

$$d - r = \sum_{i=1}^{k}(d_i - 1) + (\ell - r)$$

with $1 \leq \ell - r \leq d_{k+1} - 1$. Since $d_i' \leq d - r$ for $i = r+1, \ldots, m$, by applying Lemma 3.2.7 to the sequence $d_1, \ldots, d_{n-1}, d_i', d - r$, we get $k_i' \leq k$ for $r+1 \leq i \leq m$. By induction hypothesis we can bound $|Z(G_i')|$. Then, using Eq. ($\star$) and Lemma 3.2.7, we obtain:

$$\begin{aligned} |Z_{X^*}(G)| &\leq rd_1\cdots d_{n-1} + \sum_{i=r+1}^{m} d_{k_i'+2}\cdots d_{n-1}(d_1\cdots d_{k_i'+1} - d_{k_i'+1} + \ell_i') \\ &\leq rd_1\cdots d_{n-1} + (d_n - r)[(d_{k+2}\cdots d_{n-1})(d_1\cdots d_{k+1} - d_{k+1} + \ell - r)]. \end{aligned}$$

Thus, by factoring out the common term $d_{k+2}\cdots d_{n-1}$, we need only show the inequality:

$$\begin{aligned} rd_1\cdots d_{k+1} + (d_n - r)(d_1\cdots d_{k+1} - d_{k+1} + \ell - r) \leq& \\ d_n(d_1\cdots d_{k+1} - d_{k+1} + \ell).& \end{aligned}$$

After simplification, we get that this inequality is equivalent to $r(d_n - d_{k+1} + \ell - r) \geq 0$. This inequality holds because $d_n \geq d_{k+1}$ and $\ell > r$.

Subcase (IV.c): Assume $\ell \leq r$. We can write $d - r = \sum_{i=1}^{s}(d_i - 1) + \widetilde{\ell}$, where $1 \leq \widetilde{\ell} \leq d_{s+1} - 1$ and $s \leq k$. Notice that $s < k$. Indeed, if $s = k$, then from the equality

$$d - r = \sum_{i=1}^{s}(d_i - 1) + \widetilde{\ell} = \sum_{i=1}^{k}(d_i - 1) + \ell - r \tag{$\star\star$}$$

we get that $\widetilde{\ell} = \ell - r \geq 1$, a contradiction. Thus, $s \leq n-2$. As $d - r \geq d_i'$, by applying Lemma 3.2.7 to $d_1, \ldots, d_{n-1}, d_i', d - r$, we have $k_i' \leq s \leq n-2$ for $i = r+1, \ldots, m$. By induction hypothesis we can bound $|Z(G_i')|$. Therefore, using Eq. ($\star$) and Lemma 3.2.7, we obtain:

$$\begin{aligned} |Z_{X^*}(G)| &\leq rd_1\cdots d_{n-1}+\sum_{i=r+1}^{m}[d_1\cdots d_{n-1}-d_{k_i'+1}\cdots d_{n-1}+d_{k_i'+2}\cdots d_{n-1}\ell_i'] \\ &\leq rd_1\cdots d_{n-1}+(d_n-r)[d_1\cdots d_{n-1}-d_{s+1}\cdots d_{n-1}+d_{s+2}\cdots d_{n-1}\widetilde{\ell}\,]. \end{aligned}$$

Thus, we need only show the inequality

$$rd_1\cdots d_{n-1}+(d_n-r)[d_1\cdots d_{n-1}-d_{s+1}\cdots d_{n-1}+d_{s+2}\cdots d_{n-1}\widetilde{\ell}\,]\leq \\ d_1\cdots d_n-d_{k+1}\cdots d_n+d_{k+2}\cdots d_n\ell.$$

After cancelling out some terms, we get the following equivalent inequality:

$$d_{k+1}\cdots d_n-d_{k+2}\cdots d_n\ell\leq(d_n-r)[d_{s+1}\cdots d_{n-1}-d_{s+2}\cdots d_{n-1}\widetilde{\ell}\,]. \qquad (\ddagger)$$

The proof now reduces to show this inequality.

Subcase (IV.c.1): Assume $k=n-1$. Then, Eq. ($\ddagger$) simplifies to

$$d_n-\ell\leq(d_n-r)[d_{s+1}\cdots d_{n-1}-d_{s+2}\cdots d_{n-1}\widetilde{\ell}\,].$$

Since $d_n\geq r+1$, it suffices to show the inequality

$$r+1-\ell\leq d_{s+2}\cdots d_{n-1}(d_{s+1}-\widetilde{\ell}\,).$$

From Eq. ($\star\star$), we get

$$r+(1-\ell)=\ell-\widetilde{\ell}+\sum_{i=s+1}^{n-1}(d_i-1)+(1-\ell)=-\widetilde{\ell}+d_{s+1}+\sum_{i=s+2}^{n-1}(d_i-1).$$

Hence, the last inequality is equivalent to

$$\sum_{i=s+2}^{n-1}(d_i-1)\leq(d_{s+2}\cdots d_{n-1}-1)(d_{s+1}-\widetilde{\ell}).$$

This inequality holds because $d_{s+2}\cdots d_{n-1}\geq\sum_{i=s+2}^{n-1}(d_i-1)+1$.

Subcase (IV.c.2): Assume $k\leq n-2$. By canceling out the common term $d_{k+2}\cdots d_{n-1}$ in Eq. ($\ddagger$), we obtain the following equivalent inequality

$$d_{k+1}d_n-d_n\ell\leq(d_n-r)(d_{s+2}\cdots d_{k+1})(d_{s+1}-\widetilde{\ell}\,).$$

We rewrite this inequality as

$$r(d_{s+2}\cdots d_{k+1})(d_{s+1}-\widetilde{\ell}\,)\leq d_n[(d_{s+2}\cdots d_{k+1})(d_{s+1}-\widetilde{\ell}\,)-d_{k+1}]+\ell d_n.$$

Since $d_n \geq r+1$ it suffices to show the inequality

$$\begin{aligned} & r(d_{s+2}\cdots d_{k+1})(d_{s+1}-\widetilde{\ell}\,) \leq \\ & \qquad r[(d_{s+2}\cdots d_{k+1})(d_{s+1}-\widetilde{\ell}\,)-d_{k+1}]+[(d_{s+2}\cdots d_{k+1})(d_{s+1}-\widetilde{\ell}\,)-d_{k+1}]+\ell d_n. \end{aligned}$$

After a quick simplification, this inequality reduces to

$$(r+1)d_{k+1} \leq (d_{s+2}\cdots d_{k+1})(d_{s+1}-\widetilde{\ell}\,)+\ell d_n.$$

From Eq. ($\star\star$), we get $r+1=(-\widetilde{\ell}+d_{s+1})+(\ell+\sum_{i=s+2}^{k}(d_i-1))$. Hence, the last inequality is equivalent to

$$d_{k+1}\sum_{i=s+2}^{k}(d_i-1) \leq d_{k+1}(d_{s+2}\cdots d_k-1)(d_{s+1}-\widetilde{\ell}\,)+\ell(d_n-d_{k+1}).$$

This inequality holds because $d_{s+2}\cdots d_k \geq \sum_{i=s+2}^{k}(d_i-1)+1$. This completes the proof of the proposition. □

Corollary 3.2.10. *Let $d\geq 1$ be an integer. If $d_i \leq d_{i+1}$ for all i and $d=\sum_{i=1}^{k}(d_i-1)+\ell$ for some integers k,ℓ such that $1\leq \ell \leq d_{k+1}-1$ and $0\leq k\leq n-1$, then*

$$\max\{|Z_{X^*}(F)|\colon F\in S_{\leq d};\ F\not\equiv 0\} \leq d_{k+2}\cdots d_n(d_1\cdots d_{k+1}-d_{k+1}+\ell).$$

Proof. Let $F=F(t_1,\ldots,t_n)\in S$ be an arbitrary polynomial of total degree $d'\leq d$ such that $F(P)\neq 0$ for some $P\in X^*$. We can write $d'=\sum_{i=1}^{k'}(d_i-1)+\ell'$ with $1\leq \ell' \leq d_{k'+1}-1$ and $0\leq k'\leq k$. Let $<$ be the graded reverse lexicographical order on the monomials of S. In this order $t_1>\cdots>t_n$. For $1\leq i\leq n$, let f_i be the polynomial $\prod_{\gamma\in A_i}(t_i-\gamma)$. Recall that $d_i=|A_i|$, i.e., f_i has degree d_i. By the division algorithm [1, Theorem 1.5.9, p. 30], we can write

$$F=h_1f_1+\cdots+h_nf_n+G', \tag{††}$$

for some $G'\in S$ with $\deg_{t_i}(G')\leq d_i-1$ for $i=1,\ldots,n$ and $\deg(G')=d''\leq d'$. If G' is a constant, by Eq. (††) and using that $0\neq F(P)=G'(P)$, we get $Z_{X^*}(F)=\emptyset$. Thus, we may assume that the polynomial G' has positive degree d''. We can write $d''=\sum_{i=1}^{k''}(d_i-1)+\ell''$, where $1\leq \ell''\leq d_{k''+1}$ and $0\leq k''\leq k'$. Notice that $Z_{X^*}(F)=Z_{X^*}(G')$. By Proposition 3.2.9, and applying Lemma 3.2.7 to the sequences $d_1,\ldots,d_n,d'',d'$ and $d_1,\ldots,d_n,d',d$, we obtain

$$\begin{aligned} |Z_{X^*}(F)|=|Z_{X^*}(G')| &\leq d_1\cdots d_n-d_{k''+1}\cdots d_n+d_{k''+2}\cdots d_n\ell'' \\ &\leq d_1\cdots d_n-d_{k'+1}\cdots d_n+d_{k'+2}\cdots d_n\ell' \\ &\leq d_1\cdots d_n-d_{k+1}\cdots d_n+d_{k+2}\cdots d_n\ell. \end{aligned}$$

Thus, $|Z_{X^*}(F)|\leq d_1\cdots d_n-d_{k+1}\cdots d_n+d_{k+2}\cdots d_n\ell$, as required. □

We come to the main result of this section.

Theorem 3.2.11. [21] *Let K be a field and let $C_{X^*}(d)$ be the cartesian evaluation code of degree d on the finite set $X^* = A_1 \times \cdots \times A_n \subset K^n$. If $2 \leq d_i \leq d_{i+1}$ for all i, with $d_i = |A_i|$, and $d \geq 1$, then the minimum distance of $C_{X^*}(d)$ is given by*

$$\delta_{X^*}(d) = \begin{cases} (d_{k+1} - \ell)\, d_{k+2} \cdots d_n & \text{if } d \leq \sum\limits_{i=1}^{n} (d_i - 1) - 1, \\ 1 & \text{if } d \geq \sum\limits_{i=1}^{n} (d_i - 1), \end{cases}$$

where $k \geq 0$, ℓ are the unique integers such that $d = \sum_{i=1}^{k} (d_i - 1) + \ell$ and $1 \leq \ell \leq d_{k+1} - 1$.

Proof. If $d \geq \sum_{i=1}^{n} (d_i - 1)$, then the minimum distance of $C_{X^*}(d)$ is equal to 1 by Theorem 3.2.4. Assume that $1 \leq d \leq \sum_{i=1}^{n} (d_i - 1) - 1$. We can write

$$A_i = \{\beta_{i,1}, \beta_{i,2}, \ldots, \beta_{i,d_i}\}, \qquad i = 1, \ldots, n.$$

For $1 \leq i \leq k+1$, consider the polynomials

$$f_i = \begin{cases} (\beta_{i,1} - t_i)(\beta_{i,2} - t_i) \cdots (\beta_{i,d_i - 1} - t_i) & \text{if } 1 \leq i \leq k, \\ (\beta_{k+1,1} - t_{k+1})(\beta_{k+1,2} - t_{k+1}) \cdots (\beta_{k+1,\ell} - t_{k+1}) & \text{if } i = k+1. \end{cases}$$

The polynomial $G = f_1 \cdots f_{k+1}$ has degree d and $G(\beta_{1,d_1}, \beta_{2,d_2}, \ldots, \beta_{n,d_n}) \neq 0$. From the equality

$$\begin{aligned} Z_{X^*}(G) \;=\; & [(A_1 \setminus \{\beta_{1,d_1}\}) \times A_2 \times \cdots \times A_n] \cup \\ & [\{\beta_{1,d_1}\} \times (A_2 \setminus \{\beta_{2,d_2}\}) \times A_3 \times \cdots \times A_n] \cup \\ & \qquad \vdots \\ & [\{\beta_{1,d_1}\} \times \cdots \times \{\beta_{k-1,d_{k-1}}\} \times (A_k \setminus \{\beta_{k,d_k}\}) \times A_{k+1} \times \cdots \times A_n] \cup \\ & [\{\beta_{1,d_1}\} \times \cdots \times \{\beta_{k,d_k}\} \times \{\beta_{k+1,1}, \ldots, \beta_{k+1,\ell}\} \times A_{k+2} \times \cdots \times A_n], \end{aligned}$$

we get that the number of zeros of G in X^* is given by:

$$|Z_{X^*}(G)| = \sum_{i=1}^{k} (d_i - 1)(d_{i+1} \cdots d_n) + \ell d_{k+2} \cdots d_n = d_1 \cdots d_n - d_{k+1} \cdots d_n + \ell d_{k+2} \cdots d_n.$$

We know that $|X^*| = d_1 \cdots d_n$. Therefore

$$\begin{aligned} \delta_{X^*}(d) &= \min\{\|\mathrm{ev}_d(F)\| \colon \mathrm{ev}_d(F) \neq 0; F \in S_{\leq d}\} = |X| - \max\{|Z_{X^*}(F)| \colon F \in S_{\leq d};\, F \not\equiv 0\} \\ &\leq d_1 \cdots d_n - |Z_{X^*}(G)| = (d_{k+1} - \ell)\, d_{k+2} \cdots d_n, \end{aligned}$$

where $\|\mathrm{ev}_d(F)\|$ is the number of non-zero entries of $\mathrm{ev}_d(F)$ and $F \not\equiv 0$ means that F is not the zero function on X^*. Thus

$$\delta_{X^*}(d) \leq (d_{k+1} - \ell) d_{k+2} \cdots d_n.$$

The reverse inequality follows at once from Corollary 3.2.10. □

In a very recent paper, Bishnoi, Clark, Potukuchi and Schmitt give another proof of the formula ([4], Theorem 5.2) for $\delta_{X^*}(d)$ using a result of Alon and Fürendi [2], Theorem 5. Another proof of this formula using Gröbner bases can be found in [6], Proposition 2.3 and in [22].

As a consequence of Theorem 3.2.11, we recover the following formula for the minimum distance of a parameterized code over a projective torus.

Corollary 3.2.12. *[26, Theorem 3.5] Let $K=\mathbb{F}_q$ be a finite field with $q\neq 2$ elements. If $\mathbb{T}$ is a projective torus in $\mathbb{P}^n$ and $d\geq 1$, then the minimum distance of $C_{\mathbb{T}}(d)$ is given by*

$$\delta_{\mathbb{T}}(d)=\begin{cases}(q-1)^{n-k-1}(q-1-\ell) & \text{if } \ d\leq (q-2)n-1,\\ \qquad 1 & \text{if } \ d\geq (q-2)n,\end{cases}$$

where k and ℓ are the unique integers such that $k\geq 0$, $1\leq \ell\leq q-2$ and $d=k(q-2)+\ell$.

Proof. If $A_i=K^*$ for $i=1,\ldots,n$, then $X^*=(K^*)^n$, $Y=\mathbb{T}$, and $d_i=q-1$ for all i. Since $\delta_{X^*}(d)=\delta_Y(d)$, the result follows at once from Theorem 3.2.11. □

As another consequence of our main result, we recover a formula for the minimum distance of an evaluation code over an affine space.

Corollary 3.2.13. [8, Theorem 2.6.2] *Let $K=\mathbb{F}_q$ be a finite field and let Y be the image of $\mathbb{A}^n$ under the map $\mathbb{A}^n\to\mathbb{P}^n$, $x\mapsto[(x,1)]$. If $d\geq 1$, the minimum distance of $C_Y(d)$ is given by:*

$$\delta_Y(d)=\begin{cases}(q-\ell)q^{n-k-1} & \text{if } \ d\leq n(q-1)-1,\\ \qquad 1 & \text{if } \ d\geq n(q-1),\end{cases}$$

where k and ℓ are the unique integers such that $k\geq 0$, $1\leq \ell\leq q-1$ and $d=k(q-1)+\ell$.

Proof. If $A_i=K$ for $i=1,\ldots,n$, then $X^*=K^n=\mathbb{A}^n$ and $d_i=q$ for all i. Since $\delta_{X^*}(d)=\delta_Y(d)$, the result follows at once from Theorem 3.2.11. □

Example 3.2.14. *If $X^*=\mathbb{F}_2^n$, then the basic parameters of $C_{X^*}(d)$ are given by*

$$|X^*|=2^n,\quad \dim C_{X^*}(d)=\textstyle\sum_{i=0}^{d}\binom{n}{i},\quad \delta_{X^*}(d)=2^{n-d},\qquad 1\leq d\leq n.$$

Example 3.2.15. *Let $K=\mathbb{F}_9$ be a field with 9 elements. Assume that $A_i=K$ for $i=1,\ldots,4$. For certain values of d, the basic parameters of $C_{X^*}(d)$ are given in the following table:*

d	1	2	3	4	5	10	16	20	28	31	32
$\lvert X^*\rvert$	6561	6561	6561	6561	6561	6561	6561	6561	6561	6561	6561
$\dim C_{X^*}(d)$	5	15	35	70	126	981	3525	5256	6526	6560	6561
$\delta_{X^*}(d)$	5832	5103	4374	3645	2916	567	81	45	5	2	1

Cartesian Codes Over Degenerate Tori Given a non decreasing sequence of positive integers $d_1, \ldots, d_n$, we construct a cartesian code, over a degenerate torus, with prescribed parameters in terms of $d_1, \ldots, d_n$.

Definition 3.2.16. *Let $K = \mathbb{F}_q$ be a finite field and let $v = (v_1, \ldots, v_n)$ be a sequence of positive integers. The set*

$$X^* = \{(x_1^{v_1}, \ldots, x_n^{v_n}) \,|\, x_i \in K^* \textit{ for all } i\} \subseteq K^n,$$

is called a degenerate torus of type v.

The main result of this section is:

Theorem 3.2.17. *Let $2 \leq d_1 \leq \cdots \leq\ d_n$ be a sequence of integers. Then, there is a finite field $K = \mathbb{F}_q$ and a degenerate torus X^* such that the length of $C_{X^*}(d)$ is $d_1 \cdots d_n$, its dimension is*

$$\dim_K\, C_{X^*}(d) = \binom{n+d}{d} - \sum_{1\leq i\leq n} \binom{n+d-d_i}{d-d_i} + \sum_{i<j} \binom{n+d-(d_i+d_j)}{d-(d_i+d_j)} -$$
$$\sum_{i<j<k} \binom{n+d-(d_i+d_j+d_k)}{d-(d_i+d_j+d_k)} + \cdots + (-1)^n \binom{n+d-(d_1+\cdots+d_n)}{d-(d_1+\cdots+d_n)},$$

its minimum distance is 1 if $d \geq \sum_{i=1}^n (d_i - 1)$, and

$$\delta_{X^*}(d) = (d_{k+1} - \ell) d_{k+2} \cdots d_n \quad \textit{if} \quad d \leq \textstyle\sum_{i=1}^n (d_i - 1) - 1,$$

where $k \geq 0$, ℓ are the unique integers such that $d = \sum_{i=1}^k (d_i - 1) + \ell$ and $1 \leq \ell \leq d_{k+1} - 1$.

Proof. Pick a prime number p relatively prime to $m = d_1 \cdots d_n$. Then, by Euler formula, $p^{\varphi(m)} \equiv 1 \pmod m$, where φ is the Euler function. We set $q = p^{\varphi(m)}$. Hence, there exists a finite field $\mathbb{F}_q$ with q elements such that d_i divides $q-1$ for $i = 1, \ldots, n$. We set $K = \mathbb{F}_q$.

Let β be a generator of the cyclic group $(K^*, \cdot)$. There are positive integers $v_1, \ldots, v_n$ such that $q - 1 = v_i d_i$ for $i = 1, \ldots, n$. Notice that d_i is equal to $o(\beta^{v_i})$, the order of β^{v_i} for $i = 1, \ldots, n$. We set $A_i = \langle \beta^{v_i} \rangle$, where $\langle \beta^{v_i} \rangle$ is the subgroup of K^* generated by β^{v_i}. If X^* is the cartesian product of $A_1, \ldots, A_n$, it not hard to see that X^* is given by

$$X^* = \{(x_1^{v_1}, \ldots, x_n^{v_n}) \,|\, x_i \in K^* \text{ for all } i\} \subset \mathbb{A}^n,$$

i.e., X^* is a degenerate torus of type $v = (v_1, \ldots, v_n)$. The length of $|X^*|$ is $d_1 \cdots d_n$ because $|A_i| = d_i$ for all i. The formulae for the dimension and the minimum distance of $C_{X^*}(d)$ follow from Theorems 3.2.4 and 3.2.11. □

Remark 3.2.18. *Let $K = \mathbb{F}_q$ be a finite field and let β be a generator of the cyclic group $(K^*, \cdot)$. If X^* is a degenerate torus of type $v = (v_1, \ldots, v_n)$, then X^* is the cartesian product of $A_1, \ldots, A_n$, where A_i is the cyclic group generated by β^{v_i}. Thus, if $d_i = |A_i|$ for $i = 1, \ldots, n$, the affine evaluation code over X^* is a cartesian code. Hence, according to Theorem 3.2.4 and 3.2.11, the basic parameters of $C_{X^*}(d)$ can be computed in terms of $d_1, \ldots, d_n$ as in Theorem 3.2.17. Therefore, we are recovering the main results of [14, 15].*

As an illustration of Theorem 3.2.17 consider the following example.

Example 3.2.19. *Consider the sequence $d_1 = 2$, $d_2 = 5$, $d_3 = 9$. The prime number $q = 181$ satisfies that d_i divides $q - 1$ for all i. In this case $v_1 = 90$, $v_2 = 36$, $v_3 = 20$. The basic parameters of the cartesian codes $C_{X^*}(d)$, over the degenerate torus*

$$X^* = \{(x_1^{90}, x_2^{36}, x_3^{20}) |\, x_i \in \mathbb{F}_{181}^* \quad \textit{for } i = 1, 2, 3\},$$

are shown in the following table. Notice that the regularity of $\mathbf{I}(\mathbb{Y})$ is 13.

d	1	2	3	4	5	6	7	8	9	10	11	12	13
$\lvert X^*\rvert$	90	90	90	90	90	90	90	90	90	90	90	90	90
$\dim C_{X^*}(d)$	4	9	16	25	35	45	55	65	74	81	86	89	90
$\delta_{X^*}(d)$	45	36	27	18	9	8	7	6	5	4	3	2	1

Notice that if $K' = \mathbb{F}_9$, and we pick subsets A_1, A_2, A_3 of K' with $|A_1| = 2$, $|A_2| = 5$, $|A_3| = 9$, the cartesian evaluation code $C_{X'}(d)$, over the set $X' = A_1 \times A_2 \times A_3$, has the same parameters that $C_{X^*}(d)$ for any $d \geq 1$.

3.3 Examples with Macaulay 2.0

Example 3.3.1. *Let $K = \mathbb{F}_7$ and $v_1 = (1, 2, 3, 4), v_2 = (2, 5, 1, 2), v_3 = (1, 1, 1, 1)$. Consider the following affine algebraic toric set*

$$X^* = \{(y_1y_2^2y_3^3y_4^4, y_1^2y_2^5y_3y_4^2, y_1y_2y_3y_4) \in K^3 \mid y_i \in K^*\}.$$

We are going to use Theorem 3.1.4 and the Elimination theorem (see Theorem 1.3.33) to find the Hilbert function of $\mathbf{I}(X^*)$. Using Macaulay 2.0 we obtain:

```
i1 : p=7
o1 = 7
i2 : K=ZZ/p
o2 = K
o2 : QuotientRing
i3 : R=K[y1,y2,y3,y4,t1,t2,t3,MonomialOrder=>Eliminate 4]
o3 = R
o3 : PolynomialRing
i4 : I=ideal(t1-y1*y2^2*y3^3*y4^4,t2-y1^2*y2^5*y3*y4^2,t3-y1*y2*y3*y4,
y1^(p-1)-1,y2^(p-1)-1,y3^(p-1)-1,y4^(p-1)-1)

                   2  3  4           2  5     2
o4 = ideal (- y1*y2 y3 y4  + t1, - y1 y2 y3*y4  + t2, - y1*y2*y3*y4 + t3,
  6        6        6        6
y1  - 1, y2  - 1, y3  - 1, y4  - 1)

o4 : Ideal of R
i5 : P=ideal selectInSubring(1,gens gb I)



              6        6        6     6
o5 = ideal (t3  - 1, t2  - 1, t1  - t3 )
o5 : Ideal of R
i6 : S=K[t1,t2,t3]
o6 = S
o6 : PolynomialRing
i7 : J=substitute(P,S)

              6        6        6     6
o7 = ideal (t3  - 1, t2  - 1, t1  - t3 )
o7 : Ideal of S
i8 : J

              6        6        6     6
o8 = ideal (t3  - 1, t2  - 1, t1  - t3 )
o8 : Ideal of S
i9 : gb J
o9 = | t3^6-1 t2^6-1 t1^6-1 |
o9 : GroebnerBasis
i10 : i=1; while i< 19 do(print(hilbertFunction(i,J));i=i+1)
3
6
10
15
21
25
27
27
25
21
15
10
6
3
1
0
```

```
0
0
```

In the last part we can see the values of the Hilbert function, it is clear that the Hilbert polynomial is 0.

Example 3.3.2. *Let* $K = \mathbb{Q}$ *and* $I = \langle x^2 - y^2, zx - y, x^3 - z^2\rangle \subseteq K[x, y]$. *We use Macaulay 2.0 to compute the affine Hilbert function of* I.

```
i1 : K=QQ
o1 = QQ
o1 : Ring

  --  the class of all rational numbers

i2 : R=K[x,y,z]
o2 = R
o2 : PolynomialRing
i3 : I=ideal(x^2 - y^2,z*x - y,x^3 - z^2)

             2    2            3    2
o3 = ideal (x  - y , x*z - y, x  - z )
o3 : Ideal of R
i4 : i=1; while i< 8 do(print(hilbertFunction(i,I));i=i+1)
3
4
2
0
0
0
0
```

In the last part we can see the values of the Hilbert function, it is clear that the Hilbert polynomial is 0.

Example 3.3.3. *Let* $K = \mathbb{F}_{11}$ *and* $\mathbb{T} = \{[(x_1, x_2, x_3, x_4)] \mid x_i \in K^*\} \subseteq \mathbb{P}^3_K$ *be the projective torus. From Theorem 2.2.9 we know that*

$$\mathbf{I}(\mathbb{T}) = \langle x_2^{10} - x_1^{10}, x_3^{10} - x_1^{10}, x_4^{10} - x_1^{10}\rangle.$$

Using Macaulay 2.0 to compute the projective Hilbert function of $\mathbf{I}(\mathbb{T})$, *we obtain:*

```
i1 : p=11
o1 = 11
i2 : K=ZZ/p
o2 = K
o2 : QuotientRing
i3 : R=K[x1,x2,x3,x4]
o3 = R
o3 : PolynomialRing
i4 : I=ideal(x2^10 - x1^10,x3^10 - x1^10,x4^10 - x1^10)

                10     10       10     10       10     10
o4 = ideal (- x1   + x2  , - x1   + x3  , - x1   + x4  )
o4 : Ideal of R
i5 : i=1; while i<15 do(print(hilbertFunction(i,I));i=i+1)
4
10
20
35
56
84
120
165
220
283
352
425
500
```

In the last part we can see the values of the Hilbert function.

Example 3.3.4. *Let $K = \mathbb{Q}$, $A_1 = \{2, 4, 1\}$ and $A_2 = \{1, 3, 5\}$. Let $X^* = A_1 \times A_2$. For Lemma 3.2.1 we know that*

$$\mathbf{I}(X^*) = \langle (x-2)(x-4)(x-1), (y-1)(y-3)(y-5) \rangle.$$

We use Macaulay 2.0 to compute the affine Hilbert function of $\mathbf{I}(X^*)$.

```
i1 : K=QQ
o1 = QQ
o1 : Ring
```

```
  --  the class of all rational numbers

i2 : R=K[x,y]
o2 = R
o2 : PolynomialRing
i3 : I=ideal((x -2)*(x -4)*(x -1),(y -1)*(y -3)*(y -5))

             3     2             3     2
o3 = ideal (x  - 7x  + 14x - 8, y  - 9y  + 23y - 15)
o3 : Ideal of R
i4 : i=1; while i< 8 do(print(hilbertFunction(i,I));i=i+1)
2
3
2
1
0
0
0
```

In the last part we can see the values of the Hilbert function, it is clear that the Hilbert polynomial is 0*.*

Bibliography

[1] W. W. Adams and P. Loustaunau, *An Introduction to Gröbner Bases*, GSM **3**, American Mathematical Society, 1994.

[2] N. Alon and Z. Fürendi, *Covering the cube by affine hyperplanes*, European J. Combin. 14 (1993), 79-83.

[3] M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, Reading, MA, 1969.

[4] A. Bishno, P. L. Clark, A. Potukuchi and J. R. Schmitt, *On zeros of a polynomial in a finite grid*. Preprint, 2015, arXiv: 1503.05865.

[5] 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.

[6] C. Carvalho, *On the second Hamming weight of some Reed-Muller type codes*, Finite Fields Appl. 24 (2013), 88-94.

[7] D. Cox, J. Little and D. O'Shea, *Ideals, Varieties, and Algorithms*, Springer-Verlag, 2012.

[8] P. Delsarte, J. M. Goethals and F. J. MacWilliams, On generalized Reed–Muller codes and their relatives, Information and Control **16** (1970), 403–442.

[9] 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.

[10] 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.

[11] A. V. Geramita, *Notes of Agebraic Geometry.*

[12] 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.

[13] 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.

[14] M. González-Sarabia, C. Rentería and A. Sánchez-Hernández, Evaluation codes over a particular complete intersection, Int. Journal of Contemp. Math. Sciences **6** (2011), no. 29-32, 1497–1504.

[15] M. González-Sarabia, C. Rentería and A. Sánchez-Hernández, Minimum distance of some evaluation codes, Appl. Algebra Engrg. Comm. Comput. **24** (2013) 95-106.

[16] 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.

[17] D. Grayson and M. Stillman, *Macaulay*2, 1996. Available via anonymous ftp from `math.uiuc.edu`.

[18] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, 1977.

[19] Thomas W. Hungerford, *Algebra*, Graduate Texts in Mathematics, Springer-Verlag, New York, 1974.

[20] 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.

[21] H. H. López, C. Rentería and R. H. Villarreal, Affine cartesian codes, Des. Codes Cryptography. **71** (2014), no. 1, 5–19.

[22] J. Martínez-Bernal, Y. Pitones and R. H. Villarreal, *Footprint Functions of Complete Intersections.* Preprint, 2016, arXiv: 1601.07604.

[23] H. Matsumura, *Commutative Ring Theory*, Cambridge Studies in Advanced Mathematics **8**, Cambridge University Press, 1986.

[24] W. M. Schmidt, *Equations over finite fields, An elementary approach*, Lecture Notes in Mathematics **536**, Springer-Verlag, Berlin-New York, 1976.

[25] E. Sarmiento, *Parameterized Codes*, Tesis de Doctorado, Ciudad de México, Abril 2012.

[26] 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.

[27] A. Sørensen, Projective Reed–Muller codes, IEEE Trans. Inform. Theory **37** (1991), no. 6, 1567–1576.

[28] R. Stanley, Hilbert functions of graded algebras, Adv. Math. **28** (1978), 57–83.

[29] B. Sturmfels, *Gröbner Bases and Convex Polytopes*, University Lecture Series **8**, American Mathematical Society, Rhode Island, 1996.

[30] M. Tsfasman, S. Vladut and D. Nogin, *Algebraic geometric codes: basic notions*, Mathematical Surveys and Monographs **139**, American Mathematical Society, Providence, RI, 2007.

Notation

Index