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

Algebraic Methods for Parameterized and Cartesian Codes

A dissertation presented by

Hiram Habid López Valdez

to obtain the Degree of

Doctor in Science

in the Speciality of

Mathematics

Thesis Advisor: Dr. Rafael Heraclio Villarreal Rodríguez

Mexico City May 2016.

Centro de Investigación y de Estudios Avanzados
del Instituto Politécnico Nacional
Unidad Zacatenco
Departamento de Matemáticas

Métodos Algebraicos para Códigos Parametrizados y Cartesianos

Tesis que presenta

Hiram Habid López Valdez

para obtener el Grado de

Doctor en Ciencias

en la Especialidad de

Matemáticas

Director de Tesis: Dr. Rafael Heraclio Villarreal Rodríguez

Ciudad de México Mayo 2016.

To my wife Magdalena:

for her infinite love, I live in a colorful world.

Acknowledgements

I have an unending debt with my advisor Rafael Villarreal because he showed me a grain of sand of his knowledge, and it was much more than enough to get this Ph.D.

I am very grateful with Dr. Elisa Gorla because she received me for one year in the University of Neuchâtel, Switzerland. Unfortunately the mathematics that her research group and I studied during the visit are not shown in this work. She had a big influence in how this thesis is written; even more, the way how I now see, study and enjoy mathematics is largely thanks to her.

Many thanks for the time and the invaluable comments of the people who revised this work: Dr. Cícero Fernandes De Carvalho, Dr. Sudhir R. Ghorpade, Dr. Elisa Gorla, Dr. José Martínez Bernal, Dr. Carlos Rentería Márquez, Dr. Eliseo Sarmiento Rosales, Dr. Stefan Tohăneanu, Dr. Carlos Enrique Valencia Oleta and Dr. Rafael Heraclio Villarreal Rodríguez.

I thank Consejo Nacional de Ciencia y Tecnología, CONACyT, for the PhD scholarship and Universidad Autónoma de Aguascalientes, UAA, for the financial and moral support to get this Ph.D.

Abstract

Let $\mathcal{L}_\rho \subseteq \mathbb{Z}^n$ be a lattice (additive subgroup) and $\rho\colon \mathcal{L}_\rho \to K^*$ a partial character, with K a field. We prove that the lattice ideal $I(\rho)$ contains no monomials. For a fixed monomial order, there are a finite number of elements $a_1, \ldots, a_r$ in the lattice $\mathcal{L}_\rho$ such that the binomials $t^{a_1^+} - \rho(a_1)t^{a_1^-}, \ldots, t^{a_r^+} - \rho(a_r)t^{a_r^-}$ form a Gröbner basis of the lattice ideal. The initial ideal of this Gröbner basis is independent from the partial character, and so are the Hilbert function, the Hilbert series, the Hilbert polynomial, the index of regularity, the a-invariant and the degree of the lattice ideal. We give a proof that the lattice is generated by the elements $a_1, \ldots, a_r$ if and only if its lattice ideal is equal to the saturation of the ideal generated by the binomials $t^{a_1^+} - \rho(a_1)t^{a_1^-}, \ldots, t^{a_r^+} - \rho(a_r)t^{a_r^-}$ with respect to the monomial $t_1 \cdots t_n$. We prove that an ideal is binomial if and only if the ideal is characterized by a finite number of lattices and partial characters. If the lattice ideal is standard-graded of dimension 1, we show that its degree is the order of the torsion subgroup of the quotient group of the lattice. If the lattice ideal is ω-graded of dimension 1, we establish a complete intersection criterion in algebraic and geometric terms. In positive characteristic, it is shown that all ideals of this family are binomial set theoretic complete intersections; in characteristic zero, we show that an arbitrary lattice ideal which is a binomial set theoretic complete intersection is a complete intersection.

We study the complete intersection property, the index of regularity and the degree of vanishing ideals on degenerate tori over finite fields. We establish a correspondence between vanishing ideals and toric ideals associated to numerical semigroups. We give formulas for the degree and for the index of regularity of a complete intersection in terms of the Frobenius number and the generators of a numerical semigroup.

For affine evaluation codes parameterized by monomials over a finite field we give an algebraic method, using Gröbner bases, to compute their length and dimension. When the code is defined on a finite cartesian product of finite sets over an arbitrary field we find its dimension, length and minimum distance in terms of the cardinalities of the sets that define the cartesian product. Given a sequence of positive integers, we construct an evaluation code with prescribed parameters of a certain type in terms of these integers. We recover the formulas for the minimum distance of various families of evaluation codes, e.g., generalized Reed-Muller codes. For projective evaluation codes parameterized by a sequence of positive integers we compute length and regularity. If the projective code is defined by a nested cartesian set, we find its length, dimension and minimum distance. We give a relation between the parameters of generalized and projective Reed-Muller codes.

Resumen

Sean $\mathcal{L}_\rho \subseteq \mathbb{Z}^n$ una retícula (subgrupo aditivo) y $\rho\colon \mathcal{L}_\rho \to K^*$ un caracter parcial, con K un campo. Probamos que el ideal reticular $I(\rho)$ no contiene monomios. Para un orden monomial fijo, existen un número finito de elementos $a_1, \ldots, a_r$ en la retícula $\mathcal{L}_\rho$ tal que los binomios $t^{a_1^+} - \rho(a_1)t^{a_1^-}, \ldots, t^{a_r^+} - \rho(a_r)t^{a_r^-}$ forman una base de Gröbner del ideal reticular. El ideal inicial de esta base de Gröbner no depende del caracter, y tampoco la función de Hilbert, la serie de Hilbert, el polinomio de Hilbert, el índice de regularidad, el a-invariante y el grado del ideal reticular. Damos una prueba de que la retícula está generada por los elementos $a_1, \ldots, a_r$ si y solo si su ideal reticular es igual a la saturación del ideal generado por los binomios $t^{a_1^+} - \rho(a_1)t^{a_1^-}, \ldots, t^{a_r^+} - \rho(a_r)t^{a_r^-}$ con respecto al monomio $t_1 \cdots t_n$. Probamos que un ideal es binomial si y solo si el ideal está caracterizado por un número finito de retículas y caracteres parciales. Si el ideal reticular es estandar-graduado de dimensión 1, mostramos que su grado es el orden del subgrupo de torsión del grupo cociente de la retícula. Si el ideal reticular es ω-graduado de dimensión 1, establecemos un criterio de intersección completa en términos algebraicos y geométricos; en característica positiva, se muestra que todos los ideales de esta familia son intersecciones completas conjuntistas binomiales; en característica cero, mostramos que un ideal reticular que es una intersección completa conjuntista binomial es una intersección completa.

Estudiamos la propiedad de intersección completa, el índice de regularidad y el grado de ideales anuladores del toro degenerado sobre campos finitos. Establecemos una correspondencia entre ideales anuladores e ideales tóricos asociados a semigrupos numéricos. Damos fórmulas para el grado y para el índice de regularidad de una intersección completa en términos del número de Frobenius y los generadores de un semigrupo numérico.

Para códigos de evaluación afines parametrizados por monomios en un campo finito damos un método algebraico, usando bases de Gröbner, para calcular su longitud y dimensión. Si el código es definido por un producto cartesiano finito de conjuntos finitos en un campo arbitrario, calculamos su dimensión, longitud y distancia mínima en términos de las cardinalidades de los conjuntos. Construimos un código con parámetros prescritos de un cierto tipo en términos de una sucesión arbitraria de enteros positivos. Recobramos las fórmulas para la distancia mínima de varias familias de códigos, como los códigos Reed-Muller afines. Para códigos de evaluación proyectivos parametrizados por una sucesión de enteros positivos calculamos longitud y regularidad. Si el código proyectivo es definido por un conjunto cartesiano anidado, encontramos su longitud, dimensión y distancia mínima. Damos una relación entre los parámetros de los códigos Reed-Muller afines y proyectivos.

Introduction

There are two main topics for this thesis: **lattice ideals** and **coding theory**.

Let K be a field, $K^* := K \setminus \{0\}$ the multiplicative group of K and $S := K[t_1, \ldots, t_n]$ a polynomial ring over the field K with n variables. The concept of lattice ideal was introduced by Eisenbud and Sturmfels [16]. They defined this sort of ideals using a subgroup $\mathcal{L}_\rho$ of $\mathbb{Z}^n$ called *lattice* and a group homomorphism ρ from $\mathcal{L}_\rho$ to K^* called *partial character*. The *lattice ideal*, denoted by $I(\rho)$, is defined as

$$I(\rho) := \left(\left\{t^{a^+} - \rho(a)t^{a^-} \mid a \in \mathcal{L}_\rho\right\}\right) \subset S.$$

A *pure lattice ideal*, denoted by $I(\mathcal{L})$, is a lattice ideal associated with the *trivial partial character*, i.e. the partial character that sends all the lattice $\mathcal{L}$ to the identity element $1 \in K^*$. There are works, for instance [10, 29, 39, 40, 46], where properties about lattice ideals are given. In this thesis we are going to study arbitrary lattice ideals.

In Chapter 1 we introduce some important topics of commutative algebra, for instance Hilbert functions, Hilbert series, the degree and toric ideals. We define some sets that we use to define evaluation codes in Chapters 3 and 4. At the end of Chapter 1 we write a pair of small sections, one of them about graph theory and the second one about polyhedral sets.

By a *binomial* in S we mean a polynomial with at most two terms. A *binomial ideal* is an ideal of S generated by binomials. In Section 2.1 we introduce elementary facts about lattice ideals and the concept of congruence in a commutative semigroup with identity. The concept of congruence is useful because it allows us to introduce the concept of a simple component of an element f of S. The theory of congruences has been studied deeply by S. Eliahou [81] and R. Gilmer [84]. With this theory they prove important features about lattice ideals, for instance they show that the radical of a pure binomial ideal is again a pure binomial ideal. We use this theory to prove the following result, which is well-known for the case of pure lattice ideals.

Theorem 2.1.21 *Let K be a field and $\rho : \mathcal{L}_\rho \to K^*$ a partial character. The lattice ideal $I(\rho) = \left(\left\{t^{a^+} - \rho(a)t^{a^-} \mid a \in \mathcal{L}\right\}\right)$ contains no monomials.*

Using the concept of congruence we show in Theorem 2.1.22 that t_i is a regular element of $S/I(\rho)$ for all i. Thus at the end of Section 2.1 we give the following characterization of a lattice ideal in terms of zero divisors. This characterization is well-known for pure lattice ideals.

Theorem 2.1.23 *An ideal $I \subset S$ is a lattice ideal if and only if*

(i) *I is binomial,*

(ii) *I contains no monomials and*

(iii) *$t_i \notin \mathcal{Z}(S/I)$ for all i.*

If $a := (a_1, \ldots, a_n)$ is an element of $\mathbb{N}^n$, we set $t^a := t_1^{a_1} \cdots t_n^{a_n}$. In Section 2.2 we study some relations between $\mathcal{L}_\rho$ and $I(\rho)$. We prove for instance in Proposition 2.2.6 that $t^a - \lambda t^b$ is in $I(\rho)$ if and only if $a - b$ is $\mathcal{L}_\rho$ and $\lambda = \rho(a-b)$. Then we show the following result.

Theorem 2.2.7 $\mathcal{L}_\rho = \mathbb{Z}\{a_1, \ldots, a_r\}$ *if and only if*

$$I(\rho) = \left(t^{a_1^+} - \rho(a_1)t^{a_1^-}, \ldots, t^{a_r^+} - \rho(a_r)t^{a_r^-}\right) : (t_1 \cdots t_n)^\infty .$$

Then we show a lattice ideal is characterized by a unique lattice and a unique partial character.

Theorem 2.2.9 *Let ρ be a partial character on a lattice $\mathcal{L}_\rho$ and let $I(\rho)$ be its lattice ideal. If $I(\rho) = \left(t^{a_1} - \lambda_1 t^{b_1}, \ldots, t^{a_r} - \lambda_r t^{b_r}\right)$, then $\mathcal{L}_\rho = \mathbb{Z}\{a_1 - b_1, \ldots, a_r - b_r\}$ and $\rho(a_i - b_i) = \lambda_i$, for $i = 1, \ldots, r$. In particular, if L is a lattice ideal, there are a unique lattice $\mathcal{L}_\rho$ and a unique partial character ρ on the lattice $\mathcal{L}_\rho$ such that $L = I(\rho)$.*

At the end of Section 2.2 we have a pair of nice results. Proposition 2.2.12 tells if $I(\mathcal{L})$ is a standard graded pure lattice ideal and the initial ideal $LT(I(\mathcal{L}))$ is square-free, then $I(\mathcal{L})$ is a prime ideal and $S/I(\mathcal{L})$ is normal and Cohen-Macaulay. Example 2.2.13 shows the primary decompositions of lattice ideals is dependent from the partial character.

By [16, Corollary 2.5] we know that a binomial ideal containing no monomials is characterized by a lattice and a partial character. In some way we complement this result in Section 2.3. We show that a binomial ideal (without restrictions) can be always characterized by a finite number of lattices.

Theorem 2.3.4 *Let K be a field with characteristic different than 2. An ideal I of S is a binomial ideal if and only if there are m lattices $\mathcal{L}_i := \mathbb{Z}\{a_{i1} - b_{i1}, \ldots, a_{1r_i} - b_{1r_i}\}$ and m partial characters $\rho_i \colon \mathcal{L}_i \to K^*$ such that $I = I_1 + \cdots + I_m$, where*

$$I_i := \left(t^{a_{i1}} - \rho_i(a_{i1} - b_{i1})t^{b_{i1}}, \ldots, t^{a_{ir_i}} - \rho_i(a_{ir_i} - b_{ir_i})t^{b_{ir_i}}\right),$$

and for $i \neq j$, the ideal $I_i + I_j$ contains a monomial.

If the field has characteristic 2, in Remark 2.3.5 we show the binomial ideal depends of a lattice ideal and of a monomial ideal.

In Section 2.4 we prove that there are a finite number of elements of the lattice $\mathcal{L}_\rho$ such that this elements define a Gröbner basis of the lattice ideal $I(\rho)$. Then we give a procedure, which is based on the Buchberger's algorithm, to find the elements of $\mathcal{L}_\rho$ that define the Gröbner basis of $I(\rho)$. The main result of Section 2.4 is the following Theorem.

Theorem 2.4.1 *Let $\rho\colon \mathcal{L}_\rho \to K^*$ be a partial character and $\prec$ an arbitrary monomial order fixed on S. There are elements $a_1, \ldots, a_s$ of $\mathcal{L}_\rho$ such that*

$$\mathcal{G} := \left\{ t^{a_1^+} - \rho(a_1) t^{a_1^-}, \ldots, t^{a_s^+} - \rho(a_s) t^{a_s^-} \right\}$$

is a Gröbner basis of $I(\rho)$. In particular the reduced Gröbner basis has this form.

In [44] Morales and Thoma show the complete intersection property of $I(\rho)$ is independent from the partial character ρ. In Section 2.5 we prove that also the initial ideal of a lattice ideal is independent from the partial character.

Theorem 2.5.1 *Let $\rho\colon \mathcal{L}_\rho \to K^*$ be a partial character and $\prec$ an arbitrary monomial order fixed on S. The set $\mathcal{G} := \left\{ t^{a_1^+} - \rho(a_1) t^{a_1^-}, \ldots, t^{a_r^+} - \rho(a_r) t^{a_r^-} \right\}$ is a Gröbner basis of the lattice ideal $I(\rho)$ if and only if the set $\mathcal{G}' := \left\{ t^{a_1^+} - t^{a_1^-}, \ldots, t^{a_r^+} - t^{a_r^-} \right\}$ is a Gröbner basis of the pure lattice ideal $I(\mathcal{L}_\rho)$.*

As a consequence the Hilbert function, the Hilbert series, the Hilbert polynomial, the index of regularity, the a-invariant and the degree of the lattice ideal $I(\rho)$ are also independent from the partial character ρ.

Section 2.6 is dedicate to the case that the lattice ideal (I_ρ) is graded and has dimension 1. We prove in Lemma 2.6.9 that an element of the torsion group $T(\mathbb{Z}^n/\mathcal{L})$ can be represented in a unique way. Then we compute the degree of the lattice ideal (I_ρ). In order to compute the degree we can assume the partial character ρ is trivial because by Corollary 2.5.3 the degree is independent of the partial character.

Theorem 2.6.12 *If $I(\mathcal{L}) \subset S$ is a graded pure lattice ideal of dimension 1, then*

$$\deg S/I(\mathcal{L}) = |T(\mathbb{Z}^n/\mathcal{L})|.$$

Let ω be a vector with positive integer entries. If $I(\rho)$ is ω-graded of dimension 1, we establish a complete intersection criterion in algebraic and geometric terms. We only need to prove the result for the case the partial character is trivial, because in [44] is proved that the complete intersection property is independent of the partial character.

Theorem 2.6.31 *Let L be the pure lattice ideal of an ω-homogeneous lattice $\mathcal{L}$ in $\mathbb{Z}^n$. If $V(L, t_i) = \{0\}$ for all i, then L is a complete intersection if and only if there are homogeneous pure binomials $h_1, \ldots, h_{n-1}$ in L satisfying the following conditions:*

(i) $\mathcal{L} = \mathbb{Z}\left\{\widehat{h}_1, \ldots, \widehat{h}_{n-1}\right\}$.

(ii) $V(h_1, \ldots, h_{n-1}, t_i) = \{0\}$ *for all i.*

(iii) $h_i = t^{a_i^+} - t^{a_i^-}$ *for* $i = 1, \ldots, n-1$.

If $I(\rho)$ is a pure lattice ideal, it is ω-graded of dimension 1, and K has positive characteristic, then we show $I(\rho)$ is a pure binomial set theoretic complete intersection.

Proposition 2.6.34 *If K is a field of positive characteristic and $L \subset S$ is a ω-graded pure lattice ideal of dimension 1, then L is a pure binomial set theoretic complete intersection.*

If K has characteristic zero, we prove that in the set of pure lattice ideals the property binomial set theoretic complete intersection implies complete intersection.

Theorem 2.6.37 *Let $L \subset S$ be an arbitrary pure lattice ideal of height r. If $\operatorname{char}(K) = 0$ and $\operatorname{rad}(L) = \operatorname{rad}(g_1, \ldots, g_r)$ for some pure binomials $g_1, \ldots, g_r$, then $L = (g_1, \ldots, g_r)$.*

Define

$$\mathcal{Q} := \{[(x_1^{v_{11}} \cdots x_s^{v_{1s}}, \ldots, x_1^{v_{n1}} \cdots x_s^{v_{ns}})] \mid x_i \in K^* \text{ for all } i\} \subset \mathbb{P}^{n-1},$$

the *projective algebraic toric set* parameterized by the non-negative vectors $v_1, \ldots, v_n$. The *vanishing ideal* of $\mathcal{Q}$, denoted by $I(\mathcal{Q})$, is the ideal of S generated by the homogeneous polynomials that vanish on $\mathcal{Q}$. This ideal has very important applications in coding theory as we will see below. We prove in Lemma 2.6.39 that there is a unique homogeneous lattice $\mathcal{L}$ such that $I(\mathcal{Q}) = I(\mathcal{L})$. So at the end of Section 2.6 we apply previous results of this work about graded lattice ideals of dimension 1 and compute the degree of $I(\mathcal{L})$. Also we give a pair of complete intersection criterions of the vanishing ideal $I(\mathcal{Q})$.

Let $v := \{v_1, \ldots, v_n\}$ be a sequence of positive integers and

$$\mathcal{T} := \{[(x_1^{v_1}, \ldots, x_n^{v_n})] \mid x_i \in K^* \text{ for all } i\} \subset \mathbb{P}^{n-1}$$

the *projective degenerate torus* of type v. The vanishing ideal $I(\mathcal{T})$ plays a important role in coding theory, as we will see in Chapters 3 and 4.

In what follows β denotes a generator of the cyclic group $(K^*, \cdot)$, d_i denotes $o(\beta^{v_i})$, the order of β^{v_i} for $i = 1, \ldots, n$, and $\mathcal{S}$ denotes the semigroup $\mathbb{N}d_1 + \cdots + \mathbb{N}d_n$. If $d_1, \ldots, d_n$ are relatively prime, $\mathcal{S}$ is called a *numerical semigroup*. We will see below that the algebra of $I(\mathcal{T})$ is closely related to the algebra of the toric ideal of the semigroup ring

$$K[\mathcal{S}] := K[y_1^{d_1}, \ldots, y_1^{d_n}] \subset K[y_1],$$

where $K[y_1]$ is a polynomial ring. Recall that the toric ideal of $K[\mathcal{S}]$, denoted by P, is the kernel of the following epimorphism of K-algebras

$$\varphi\colon S := K[t_1, \ldots, t_n] \longrightarrow K[\mathcal{S}], \qquad f \xmapsto{\varphi} f(y_1^{d_1}, \ldots, y_1^{d_n}).$$

Thus, $S/P \simeq K[\mathcal{S}]$. Since $K[y_1]$ is integral over $K[\mathcal{S}]$ we have $\operatorname{ht}(P) = n-1$. The ideal P is graded if one gives degree d_i to variable t_i. For $n = 3$, the first non-trivial case, this type of toric ideals were studied by Herzog [30]. For $n \geq 4$, these toric ideals have been studied by many authors [4, 6, 12, 15, 17, 58].

In Section 2.7 we relate some of the algebraic invariants and properties of $I(\mathcal{T})$ with those of P and $\mathcal{S}$. The most well-known properties that P and $I(\mathcal{T})$ have in common is that both are Cohen-Macaulay graded lattice ideals of dimension 1 [30, 49].

Some of the key facts that allow to link the properties of P and $I(\mathcal{T})$ are Propositions 2.7.4 and 2.7.5. Proposition 2.7.4 says that the homogeneous lattices of P and $I(\mathcal{T})$ are closely related. Proposition 2.7.5 affirms that if $g_1, \ldots, g_m$ is a set of generators for P consisting of binomials, then $h_1, \ldots, h_m$ is a set of generators for $I(\mathcal{T})$, where h_k is the binomial obtained from g_k after t_i is substituted by $t_i^{d_i}$ for $i = 1, \ldots, n$. As a consequence, Corollary 2.7.6 says that if $n = 3$, then $I(\mathcal{T})$ is minimally generated by 2 or 3 binomials. If $I(\mathcal{T})$ is a complete intersection, the following result shows that a minimal generating set for $I(\mathcal{T})$ consisting of binomials corresponds to a minimal generating set for P consisting of binomials, and viceversa.

Theorem 2.7.8 (a) *If $I(\mathcal{T})$ is a complete intersection generated by binomials $h_1, \ldots, h_{n-1}$, then P is a complete intersection generated by binomials $g_1, \ldots, g_{n-1}$ such that h_i is equal to $g_i(t_1^{d_1}, \ldots, t_n^{d_n})$ for all i.* (b) *If P is a complete intersection generated by binomials $g_1, \ldots, g_{n-1}$, then $I(\mathcal{T})$ is a complete intersection generated by binomials $h_1, \ldots, h_{n-1}$, where h_i is equal to $g_i(t_1^{d_1}, \ldots, t_n^{d_n})$ for all i.*

We show in Corollary 2.7.9 that $I(\mathcal{T})$ is a complete intersection if and only if P is a complete intersection. The *Frobenius number* of a numerical semigroup is the largest integer not in the semigroup. For complete intersections, in the following result we give a formula that relates the index of regularity of $S/I(\mathcal{T})$ with the Frobenius number of the numerical semigroup generated by $o(\beta^{rv_1}), \ldots, o(\beta^{rv_n})$, where r is the greatest common divisor of $d_1, \ldots, d_n$.

Corollary 2.7.14 (i) $\deg(S/I(\mathcal{T})) = d_1 \cdots d_n / \gcd(d_1, \ldots, d_n)$.

(ii) *If $I(\mathcal{T})$ is a complete intersection, then*

$$\operatorname{reg} S/I(\mathcal{T}) = \gcd(d_1, \ldots, d_n)\, g(\mathcal{S}') + \textstyle\sum_{i=1}^n d_i - (n-1),$$

where $g(\mathcal{S}')$ denotes the Frobenius number of the numerical semigroup $\mathcal{S}'$ generated by $o(\beta^{rv_1}), \ldots, o(\beta^{rv_n})$; and r is the greatest common divisor of $d_1, \ldots, d_n$.

The Frobenius number occurs in many branches of mathematics and is one of the most studied invariants in the theory of semigroups. A great deal of effort has been directed at the effective computation of this number, see the monograph of Ramírez-Alfonsín [48].

The complete intersection property of P has been nicely characterized, using the notion of a binary tree [4, 6] and the notion of *suites distinguées* [12]. For $n = 3$, there is a classical result of [30] showing an algorithm to construct a generating set for P. Thus we obtain various classifications of the complete intersection property of $I(\mathcal{T})$. Furthermore, in [4] an effective algorithm is given to determine whether P is a complete intersection. This algorithm has been implemented in the distributed library cimonom.lib [5] of Singular [65]. Therefore we can use this algorithm and some results of this thesis, in special Corollary 2.7.9, to determine whether $I(\mathcal{T})$ is a complete intersection. For instance see Example 2.7.15. If $I(\mathcal{T})$ is a complete intersection, this algorithm returns the generators of P and the Frobenius number. As a byproduct, we can construct interesting examples of complete intersection vanishing ideals. For instance see Example 2.7.17.

At the end of Section 2.7 we also give a way to compute the ideal $I(\mathcal{T})$ in terms of the d_i's and a saturation with respect to the monomial $t_1 \cdots t_n$.

Proposition 2.7.20 *Let I' be the ideal $(t_i^{c_{ij}} - t_j^{c_{ij}} \,|\, 1 < i < j \leq n)$, where $c_{ij} := \operatorname{lcm}\{d_i, d_j\}$. If $\gcd(d_1, \ldots, d_n) = 1$, then $I(\mathcal{T}) = I' \colon (t_1 \cdots t_n)^{\infty}$.*

It is worth mentioning that our results of this Section 2.7 could be applied to coding theory, for instance, Theorem 4.1.1 is an application, because potentially good evaluation codes can occur only if the index of regularity satisfies certain constraints. The basic parameters of evaluation codes arising from complete intersections have been studied in [14, 22, 28, 37, 38, 54, 55]. See below for a detailed explanation of this fact.

Before to start with the introduction to linear codes we would like to make an extra comment. There is a series of results where a binomial ideal is associated to a given linear code. Thus properties of the code are obtained in terms of the ideal. For instance. Given a linear code C over $\mathbb{F}_2$, in [8] the authors associate a binomial ideal $I(C)$ to C. Then they prove that it is possible to decode and to compute the minimum distance of C from a reduced Gröbner basis of $I(C)$. In [53] Saleemi and Zimmermann associate a binomial ideal to any code over $\mathbb{F}_p$, where p is a prime. The authors study the minimal generators and Gröbner bases for this sort of ideals. The same authors, Saleemi and Zimmermann, complement their previous work in this topic and write [52], where they associate a binomial ideal to any code over $\mathbb{F}_4$. The authors find the reduced Gröbner basis with respect to the lex order. Finally, given a linear code C over any finite field $\mathbb{F}_q$, in [42] Márquez-Corbella et al associate a binomial ideal $I(C)$ to C. They prove that a reduced Gröbner basis relative to a degree-compatible ordering gives a complete decoding algorithm. In this thesis we study linear codes with lattice ideals, and every lattice ideal is a binomial ideal, but the approach is different to which we just describe. In the works that we just describe the authors associate a binomial ideal to a linear code, and then properties of the code are obtained from the associated ideal. What we do, it is to study evaluation codes. An evaluation code has by definition an associated ideal, which is a binomial ideal, in fact, it is a lattice ideal. We obtain some properties of the evaluation code in terms of the lattice ideal. Until here everything looks very similar, but the big difference is that the ideals are different, they come from a very different point of view as we will see below.

Let $K := \mathbb{F}_q$ be a finite field. A *linear code* (*code* for short) of *length* m, is a linear subspace C of the vector space K^m. Such a code is also called a *q-ary* code. If $q = 2$ or $q = 3$, the code is described as a *binary code*, or a *ternary code* respectively. This sort of codes can be studied as affine variety codes [20, Proposition 1], which are introduced also in the same work.

The *dimension* of a code C, denoted by $\dim_K C$, is the dimension of C as K-vector space. The dimension and the length of a code C are two of the *basic parameters* of a linear code. A third basic parameter is the *minimum distance*, which is given by

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

where $\|v\|$ is the number of non-zero entries of vector v.

The basic parameters of a code C are related by the *Singleton bound* for the minimum distance

$$\delta(C) \leq |C| - \dim_K C + 1.$$

A linear code is called *maximum distance separable* (MDS for short) if equality holds in the Singleton bound.

The length of a code is usually the "easiest" parameter to compute. The minimum distance is related with the number of errors that a code can solve, and to find it is consider a NP-hard problem [60]. We use different results in order to find the minimum distance, as "Combinatorial Nullstellensatz" [1, Theorem 1.2] or variety of an ideal [9, Proposition 2.3]. We are interested in *evaluation codes*, which are codes that depend of a set of points. When the set of points is a subset of an affine space (projective space), the code is called *affine evaluation code* (*projective evaluation code*). Define the following sets.

- An *affine set* $\mathcal{X}^* \subseteq \mathbb{A}^n$, where $\mathbb{A}^n := K^n$ is an *affine space* over the field K.
- $\overline{\mathcal{X}^*} := \{[(\mathbf{a}, 1)] \,|\, \mathbf{a} \in \mathcal{X}^*\} \subseteq \mathbb{P}^n$, the *projective closure* of $\mathcal{X}^*$.
- $\mathcal{X}$, the image of $\mathcal{X}^* \setminus \{0\}$ under the map $\mathbb{A}^n \setminus \{0\} \mapsto \mathbb{P}^{n-1}$, $\gamma \mapsto [\gamma]$.

Let $S := K[t_1, \ldots, t_n]$ be a polynomial ring with the standard grading, $S_{\leq d}$ the K-vector space of all polynomials of S of degree at most d and $\mathbf{a}_1, \ldots, \mathbf{a}_m$ the points of $\mathcal{X}^*$. The *evaluation map*

$$\mathrm{ev}_d \colon S_{\leq d} \longrightarrow K^{|\mathcal{X}^*|}, \qquad f \mapsto (f(\mathbf{a}_1), \ldots, f(\mathbf{a}_m)),$$

defines a linear map of K-vector spaces. The image of ev_d in $K^{|\mathcal{X}^*|}$, denoted by $C_{\mathcal{X}^*}(d)$, defines a K-vector subspace. Permitting an abuse of language, we are referring to $C_{\mathcal{X}^*}(d)$ as a linear code, even though in some cases we use a field K that might not be finite, as in Section 3.3, where K has no restrictions. We call $C_{\mathcal{X}^*}(d)$ the *affine evaluation code* (*affine code* for short) of degree d on the set $\mathcal{X}^*$. Affine codes are special types of affine Reed-Muller codes in the sense of [99, p. 37]. The basic parameters of affine codes are:

- The length of $C_{\mathcal{X}^*}(d)$ is $|\mathcal{X}^*|$.
- The dimension of $C_{\mathcal{X}^*}(d)$ is $\dim_K C_{\mathcal{X}^*}(d)$.
- The minimum distance of $C_{\mathcal{X}^*}(d)$ is

  $$\delta_{\mathcal{X}^*}(d) = \min\{\|\varphi_d(f)\| \colon \varphi_d(f) \neq 0; f \in S_{\leq d}\},$$

  where $\|\varphi_d(f)\|$ is the number of non-zero entries of $\varphi_d(f)$. This means that in order to find the minimum distance, we need to find the polynomial of degree d with the greatest number of zeros in $\mathcal{X}^*$.

Some families of evaluation codes –including several variations of Reed-Muller codes– have been studied extensively using commutative algebra methods (e.g., Hilbert functions, resolutions, Gröbner bases), see [13, 14, 22, 27, 38, 49, 50, 51, 56, 59]. In Chapter 3 we use these methods to study some families of affine codes.

The *vanishing ideal* of $\mathcal{X}^*$, denoted by $I(\mathcal{X}^*)$, is the ideal of S generated by the polynomials that vanish on all $\mathcal{X}^*$. A key observation that allows to use commutative algebra methods in the study evaluation codes is that the kernel of the evaluation map ev_d is precisely $S_{\leq d} \cap I(\mathcal{X}^*)$. Thus, using commutative algebra methods and algebraic invariants (Hilbert functions, Hilbert series, Gröbner bases, degree, regularity) of $I(\mathcal{X}^*)$, as is seen in the references given above, or in [38, 49, 51, 54, 55], the algebra of $S/I(\mathcal{X}^*)$ is related to the basic parameters of $C_{\mathcal{X}^*}(d)$. Below we will clarify some more the role of commutative algebra in coding theory.

The *Hilbert function* of $S/I(\mathcal{X}^*)$ is given by

$$H_{\mathcal{X}^*}(d) := \dim_K(S_{\leq d}/I(\mathcal{X}^*) \cap S_{\leq d}),$$

and $H_{\mathcal{X}^*}(d)$ is precisely the dimension of $C_{\mathcal{X}^*}(d)$. The Krull dimension of $S/I(\mathcal{X}^*)$ is denoted by $\dim(S/I(\mathcal{X}^*))$ and its Hilbert polynomial by $h_{\mathcal{X}^*}(t)$.

The *vanishing ideal* of $\overline{\mathcal{X}^*}$, denoted by $I(\overline{\mathcal{X}^*})$, is the ideal of $S[u]$ generated by the homogeneous polynomials that vanish on $\overline{\mathcal{X}^*}$, where $u := t_{n+1}$ is a new variable and $S[u] := \oplus_{d \geq 0} S[u]_d$ is a polynomial ring, with the standard grading, over the field K. Let $\mathbf{p}_1, \ldots, \mathbf{p}_m$ be a set of representatives for the points of $\overline{\mathcal{X}^*}$ and let $f_0(t_1, \ldots, t_{n+1}) = t_1^d$. The evaluation map

$$\mathrm{ev}'_d \colon S[u]_d \longrightarrow K^{|\overline{\mathcal{X}^*}|}, \qquad f \mapsto \left(\frac{f(\mathbf{p}_1)}{f_0(\mathbf{p}_1)}, \ldots, \frac{f(\mathbf{p}_m)}{f_0(\mathbf{p}_m)}\right),$$

defines a linear map of K-vector spaces. If $\mathbf{p}'_1, \ldots, \mathbf{p}'_m$ is another set of representatives, then there are $\lambda_1, \ldots, \lambda_m$ in K^* such that $\mathbf{p}'_i = \lambda_i \mathbf{p}_i$ for all i. Thus, $f(\mathbf{p}'_i)/f_0(\mathbf{p}'_i) = f(\mathbf{p}_i)/f_0(\mathbf{p}_i)$ for $f \in S[u]_d$ and $1 \leq i \leq m$. This means that the map ev'_d is independent of the set of representatives that we choose for the points of $\overline{\mathcal{X}^*}$. In what follows we choose $(\mathbf{a}_1, 1), \ldots, (\mathbf{a}_m, 1)$ as a set of representatives for the points of $\overline{\mathcal{X}^*}$. The image of ev'_d, denoted by $C_{\overline{\mathcal{X}^*}}(d)$, defines a linear code that we call a *projective evaluation code* (*projective code* for short) of degree d on the set $\overline{\mathcal{X}^*}$.

We use the algebraic invariants (regularity, degree, Hilbert function) of the graded ring $S[u]/I(\overline{\mathcal{X}^*})$ as a tool to study the described codes. It is a fact that this graded ring has the same invariants that the affine ring $S/I(\mathcal{X}^*)$ [65, Remark 5.3.16]. The *Hilbert function* of $S[u]/I(\overline{\mathcal{X}^*})$ is given by

$$H_{\overline{\mathcal{X}^*}}(d) := \dim_K(S[u]_d/I(\overline{\mathcal{X}^*}) \cap S[u]_d).$$

The Krull dimension of $S[u]/I(\overline{\mathcal{X}^*})$ is denoted by $\dim(S[u]/I(\overline{\mathcal{X}^*}))$ and its Hilbert polynomial by $h_{\overline{\mathcal{X}^*}}(t)$. According to [86, Lecture 13], or [21], we have that $H_{\overline{\mathcal{X}^*}}(d) = |\overline{\mathcal{X}^*}|$ for $d \geq |\overline{\mathcal{X}^*}|-1$. This means that $|\overline{\mathcal{X}^*}|$ is the degree of $S[u]/I(\overline{\mathcal{X}^*})$ in the sense of algebraic geometry [86, p. 166]. The *index of regularity* of $S[u]/I(\overline{\mathcal{X}^*})$, denoted by $\mathrm{reg}\left(S[u]/I(\overline{\mathcal{X}^*})\right)$, is the least integer $\ell \geq 0$ such that $H_{\overline{\mathcal{X}^*}}(d) = |\overline{\mathcal{X}^*}|$ for $d \geq \ell$. The knowledge of the regularity of $S[u]/I(\overline{\mathcal{X}^*})$ is important because the code $C_{\mathcal{X}^*}(d)$ coincides with the underlying vector space $K^{|\mathcal{X}^*|}$ for $d \geq \mathrm{reg}\,(S[u]/I(\overline{\mathcal{X}^*}))$, and has, accordingly, minimum distance equal to 1. Thus, potentially good codes $C_{\mathcal{X}^*}(d)$ can occur only if $1 \leq d < \mathrm{reg}(S[u]/I(\overline{\mathcal{X}^*}))$.

The basic parameters of different types of Reed-Muller codes (or evaluation codes) over finite fields have been computed in a number of cases. If $\mathcal{X} = \mathbb{P}^n$, the parameters of $C_{\mathcal{X}}(d)$ are described in [56, Theorem 1]. If $\mathcal{X}$ is the image of $\mathbb{A}^n$ under the map $\mathbb{A}^n \to \mathbb{P}^n$, $x \mapsto [(x, 1)]$, the parameters of $C_{\mathcal{X}}(d)$ are described in [13, Theorem 2.6.2]. If $\mathcal{X} \subset \mathbb{P}^n$ is a set parameterized by monomials arising from the edges of a clutter and the vanishing ideal of $\mathcal{X}$ is a complete intersection, the parameters of $C_{\mathcal{X}}(d)$ are described in [54].

In Proposition 3.1.3 we give a short proof of the well-known result that says that the codes $C_{\mathcal{X}^*}(d)$ and $C_{\overline{\mathcal{X}^*}}(d)$ have the same basic parameters. Then we show in Corollary 3.1.5 a pair of properties of two of the basic parameters of $C_{\mathcal{X}^*}(d)$: the dimension is an increasing function until it reaches a constant value equal to $|\mathcal{X}^*|$ and the minimum distance is a decreasing function until it reaches a constant value equal to 1. In both cases the functions depend of d.

Let $v_1, \ldots, v_n$ be a sequence of vectors in $\mathbb{N}^s$ with $v_i = (v_{i1}, \ldots, v_{is})$ for $1 \leq i \leq n$ and

$$\mathcal{Q}^* := \{(x_1^{v_{11}} \cdots x_s^{v_{1s}}, \ldots, x_1^{v_{n1}} \cdots x_s^{v_{ns}}) \in \mathbb{A}^n |\, x_i \in K^* \text{ for all } i\},$$

the *affine algebraic toric set* parameterized by the vectors $v_1, \ldots, v_n$ on $\mathbb{A}^n$. The affine code of degree d on the set $\mathcal{Q}^*$, denoted by $C_{\mathcal{Q}^*}(d)$, is called a *parameterized affine code* of degree d on the set $\mathcal{Q}^*$. Parameterized affine codes are special types of affine Reed-Muller codes in the sense of [99, p. 37]. If $s = n = 1$ and $v_1 = 1$, then $\mathcal{Q}^* = K^*$ and we obtain the classical Reed-Solomon code of degree d [98, p. 42].

Let $\overline{\mathcal{Q}^*}$ be the projective closure of $\mathcal{Q}^*$. One of the main theorems of Section 3.2 talks about the length of $\mathcal{Q}^*$.

Theorem 3.2.1 *The length of* $C_{\mathcal{Q}^*}(d)$ *is* $\deg(S[u]/I(\overline{\mathcal{Q}^*}))$.

In Theorem 3.2.9 we show how to compute the vanishing ideal of $\mathcal{Q}^*$ when K is a finite field. In Proposition 3.2.10 we prove it for infinite fields. Then we use these pairs of results to compute some basic parameters of $C_{\mathcal{Q}^*}(d)$.

Corollary 3.2.12 *The dimension and the length of* $C_{\mathcal{Q}^*}(d)$ *can be computed using Gröbner basis.*

If $C_{\mathcal{X}^*_G}(d)$ is a parameterized code associated to a graph G, Theorem 3.2.16 tell us how to compute the length of this code.

Let K be an arbitrary field, $\mathbb{A}^n := K^n$ an affine space over the field K, $S := K[t_1, \ldots, t_n]$ a polynomial ring over K with n variables and $\Lambda_1, \ldots, \Lambda_n$ a collection of non-empty subsets of K with a finite number of elements. Consider the following finite sets: (a) an *affine cartesian product*

$$\mathcal{C}^* := \Lambda_1 \times \cdots \times \Lambda_n \subset \mathbb{A}^n,$$

and (b) the projective closure of $\mathcal{C}^*$

$$\overline{\mathcal{C}^*} := \{[(\lambda_1, \ldots, \lambda_n, 1)] \,|\, \lambda_i \in \Lambda_i \text{ for all } i\} \subset \mathbb{P}^n,$$

where $\mathbb{P}^n$ is a projective space over the field K. For $i = 1, \ldots, n$, we define $d_i := |\Lambda_i|$, the cardinality of Λ_i. We may always assume that $2 \leq d_i \leq d_{i+1}$ for all i (see Proposition 3.3.6). The vanishing ideal of $\overline{\mathcal{C}^*}$, denoted by $I\left(\overline{\mathcal{C}^*}\right)$, consists of all homogeneous polynomials f of S that vanish on the set $\overline{\mathcal{C}^*}$.

We show in Proposition 3.3.3 that $I\left(\overline{\mathcal{C}^*}\right)$ is a complete intersection. Then we use [14, Corollary 2.6] and in the same proposition we give explicit formulas, in terms of the d_i's, for a set of generators, for the Hilbert series, for the index of regularity and for the degree of the ideal $I\left(\overline{\mathcal{C}^*}\right)$.

The code defined by $\mathcal{C}^*$, denoted by $C_{\mathcal{C}^*}(d)$, is called an *affine cartesian code* of degree d on the set $\mathcal{C}^*$. We compute the length and the dimension of affine cartesian codes.

Theorem 3.3.5 *The length of $C_{\mathcal{C}^*}(d)$ 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*

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

Then in Proposition 3.3.10 and Corollary 3.3.11 we show upper bounds in terms of $d_1, \ldots, d_n$ for the number of roots, over $\mathcal{C}^*$, of polynomials in S which do not vanish at all points of $\mathcal{C}^*$. Thus we come to one of the main theorems of Section 3.3, a formula for the minimum distance of $C_{\mathcal{C}^*}(d)$ in terms of the d_i's.

Theorem 3.3.12 *Let K be a field and let $C_{\mathcal{C}^*}(d)$ be the cartesian evaluation code of degree d on the finite set $\mathcal{C}^* := \Lambda_1 \times \cdots \times \Lambda_n \subset K^n$. If $2 \leq d_i \leq d_{i+1}$ for all i, with $d_i := |\Lambda_i|$, and $d \geq 1$, then the minimum distance of $C_{\mathcal{C}^*}(d)$ is given by*

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

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 general, the problem of computing the minimum distance of a linear code is difficult because it is NP-hard [60]. The basic parameters of evaluation codes over finite fields have been computed in a number of cases. Our main results provide unifying tools to treat some of these cases. As an application, if T is a projective torus in $\mathbb{P}^n$ over a finite field K, we recover in Corollary 3.3.13 a formula proved in [54] for the minimum distance of $C_T(d)$. If $\overline{\mathbb{A}^n}$ is the image of $\mathbb{A}^n$ under the map $\mathbb{A}^n \to \mathbb{P}^n$, $x \mapsto [(x, 1)]$, we also recover in

Corollary 3.3.14 a formula given in [13] for the minimum distance of $C_{\overline{\mathbb{A}^n}}(d)$. If $\mathcal{X} = \mathbb{P}^n$, the parameters of $C_{\mathcal{X}}(d)$ are described in [56, Theorem 1] (see also [35]), notice that in this case $\mathcal{X}$ does not arise as the projective closure of some cartesian product $\mathcal{C}^*$.

It should be mentioned that we do not know of any efficient decoding algorithm for the family of cartesian codes. The reader is referred to [33], [76, Chapter 9],[100] and the references there for some available decoding algorithms for some families of linear codes.

At the end of Section 3.3 we consider cartesian codes over degenerate tori. Given a non-decreasing sequence of positive integers $d_1 \leq \cdots \leq d_n$, there exists a finite field K such that d_i divides $q-1$ for all i. We use this field to construct a cartesian code over a degenerate torus with previously fixed parameters, expressed in terms of $d_1, \ldots, d_n$.

Theorem 3.3.17 *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 an affine degenerate torus $\mathcal{T}^*$ such that the length of $C_{\mathcal{T}^*}(d)$ is $d_1 \cdots d_n$, its dimension is*

$$\dim_K C_{\mathcal{T}^*}(d) = \binom{n+d}{d} - \sum_{1 \leq i \leq n} \binom{n+d-d_i}{d-d_i} + \sum_{i<j} \binom{n+d-(d_i+d_j)}{d-(d_i+d_j)} -$$
$$\sum_{i<j<k} \binom{n+d-(d_i+d_j+d_k)}{d-(d_i+d_j+d_k)} + \cdots + (-1)^n \binom{n+d-(d_1+\cdots+d_n)}{d-(d_1+\cdots+d_n)},$$

its minimum distance is 1 *if* $d \geq \sum_{i=1}^{n}(d_i-1)$, *and*

$$\delta_{\mathcal{T}^*}(d) = (d_{k+1}-\ell)d_{k+2}\cdots d_n \quad \textit{if} \quad d \leq \textstyle\sum_{i=1}^{n}(d_i-1)-1,$$

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

As a byproduct, we obtain formulas for the basic parameters of any affine evaluation code over an affine degenerate torus (see Definition 1.2.7). Thus, we are also recovering the main results of [25, 26] (Remark 3.3.18).

Let $K := \mathbb{F}_q$ be a finite field with q elements, $\mathbb{P}^n$ a projective pace over the field $K, S := K[t_0, \ldots, t_n]$ a polynomial ring over the field K with $n+1$ variables and S_d the K-vector space of all homogeneous polynomials of S of degree d union the zero polynomial. Let $\mathcal{X}$ be a subset of $\mathbb{P}^n$ and $\mathbf{p}_1, \ldots, \mathbf{p}_m$ the points of $\mathcal{X}$ written with standard representation for projective points, that is, zeros to the left and the first nonzero entry equal 1.

The *evaluation map*

$$\varphi_d \colon S_d \longrightarrow K^{|\mathcal{X}|}, \qquad f \mapsto (f(\mathbf{p}_1), \ldots, f(\mathbf{p}_m)),$$

defines a linear map of K-vector spaces. The image, denoted by $C_{\mathcal{X}}(d)$, defines a linear code, i.e., a K-vector subspace. We call $C_{\mathcal{X}}(d)$ the *projective evaluation code* (*projective code* for short) of degree d on the set $\mathcal{X}$. The *dimension*, the *length* and *the minimum distance* of projective codes are defined of analogous way to affine codes. Also the degree and the regularity have the same interpretation. All the projective codes treated in this thesis are a generalization of projective Reed-Muller codes in the sense of [35] or [56, Def. 1, p. 1568].

Let $v := \{v_1, \ldots, v_n\}$ be a sequence of positive integers and $\mathcal{T} := \{[(x_1^{v_1}, \ldots, x_n^{v_n})] \mid x_i \in K^* \text{ for all } i\} \subseteq \mathbb{P}^{n-1}$ a projective degenerate torus of type v. The projective code associated with $\mathcal{T}$, denoted by $C_{\mathcal{T}}(d)$, is called a *parameterized projective code* of degree d.

The linear code $C_{\mathcal{T}}(d)$ has length $|\mathcal{T}|$. The index of regularity of $S/I(\mathcal{T})$ is important because good codes $C_{\mathcal{T}}(d)$ can occur only if $1 \leq d < \operatorname{reg}(S/I(\mathcal{T}))$. Let β be a generator of the cyclic group $(K^*, \cdot)$, and d_i denotes $o(\beta^{v_i})$, the order of β^{v_i} for $i = 1, \ldots, n$. We compute the length of $C_{\mathcal{T}}(d)$ and we give a condition over d in order to good codes can appear in terms of a Frobenius number.

Theorem 4.1.1 (i) *The length of $C_{\mathcal{T}}(d)$ is $d_1 \cdots d_n / \gcd(d_1, \ldots, d_n)$.*

(ii) *If $I(\mathcal{T})$ is a complete intersection, then good codes $C_{\mathcal{T}}(d)$ can occur only if*

$$d \leq \gcd(d_1, \ldots, d_n)\, g(\mathcal{S}') + \textstyle\sum_{i=1}^n d_i - (n-1),$$

where $g(\mathcal{S}')$ denotes the Frobenius number of the numerical semigroup $\mathcal{S}'$ generated by $o(\beta^{rv_1}), \ldots, o(\beta^{rv_n})$; and r is the greatest common divisor of $d_1, \ldots, d_n$.

Let $K := \mathbb{F}_q$ be a finite field, and let $\Lambda_0, \Lambda_1, \ldots, \Lambda_n$ be a collection of non-empty subsets of K such that (i) for all $i = 0, \ldots, n$ we have $0 \in \Lambda_i$, and (ii) for every $i = 1, \ldots, n$ we have $\frac{\Lambda_j}{\Lambda_{i-1}} \subset \Lambda_j$ for $j = i, \ldots, n$. Under these conditions, a *projective cartesian product*

$$\mathcal{C} := [\Lambda_0 \times \Lambda_1 \times \cdots \times \Lambda_n] = \{[(\lambda_0, \cdots, \lambda_n)] \mid a_j \in \Lambda_j \text{ for all } j\} \subset \mathbb{P}^n,$$

is called a *projective nested cartesian set*. The projective code $C_{\mathcal{C}}(d)$ is called a *projective nested cartesian code*. For $i = 0, \ldots, n$, define $d_i := |\Lambda_i|$, the cardinality of Λ_i. We shall always assume that $2 \leq d_i \leq d_{i+1}$ for all i. The case $d_1 = \cdots = d_j = 1$ will be treated separately in Lemma 4.2.5. We give an explicit formula in terms of the d_i's for the length and the dimension.

Theorem 4.2.3 *The length of $C_{\mathcal{C}}(d)$ is $m := 1 + \sum_{i=1}^n d_i \cdots d_n$.*

Theorem 4.2.9 *The dimension of $C_{\mathcal{C}}(d)$ is given by*

$$\begin{aligned}\dim_K C_{\mathcal{C}}(d) = \sum_{j=0}^{n} \Bigg[&\binom{j+d-1}{d-1} - \sum_{n+1-j \leq i \leq n} \binom{j+d-1-d_i}{d-1-d_i} + \\ &\sum_{i<j} \binom{j+d-1-(d_i+d_j)}{d-1-(d_i+d_j)} - \sum_{i<j<k} \binom{j+d-1-(d_i+d_j+d_k)}{d-1-(d_i+d_j+d_k)} \\ &+ \cdots + (-1)^j \binom{j+d-1-(d_{n+1-j}+\cdots+d_n)}{d-1-(d_{n+1-j}+\cdots+d_n)} \Bigg].\end{aligned}$$

Then we find a Gröbner basis for the vanishing ideal $I(\mathcal{C})$.

Proposition4.2.14*Let $\mathcal{C} := [\Lambda_0 \times \cdots \times \Lambda_n]$ be a projective nested cartesian set. The set $\mathcal{G} := \left\{ t_i \prod_{\lambda_j \in \Lambda_j} (t_j - \lambda_j t_i), i < j; i, j = 0, \ldots, n \right\}$ is a Gröbner basis for $I(\mathcal{C})$.*

In Lemma 4.2.15 we give an upper bound for the minimum distance, and we give an explicit formula that we think it is the exact value.

Conjecture 4.2.16 *If $\mathcal{C}$ is the projective nested cartesian set over $\Lambda_0, \ldots, \Lambda_n$, then the minimum distance of $C_{\mathcal{C}}(d)$ is given by*

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

where $0 \leq k \leq n-1$ and $0 \leq \ell < d_{k+1} - 1$ are the unique integers such that $d - 1 = \sum\limits_{i=1}^{k} (d_i - 1) + \ell$.

We prove that the previous formula is true if we assume that every Λ_i is a field.

Theorem 4.2.23 *If $\mathcal{C}$ is the projective nested product of fields over $K_0, \ldots, K_n$, then the minimum distance of $C_{\mathcal{C}}(d)$ is given by*

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

where $0 \leq k \leq n-1$ and $0 \leq \ell < d_{k+1} - 1$ are the unique integers such that

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

At the end of Section 4.2 we give a relation between projective cartesian codes and affine cartesian codes. In particular, we show that there exists a relation between the basic parameters of generalized Reed-Muller codes and the basic parameters of projective Reed-Muller codes.

Corollary 4.2.25 *Let $K_0, \ldots, K_n$ be subfields of K such that $\mathcal{C} := [K_0 \times K_1 \times \cdots \times K_n]$ is a projective nested product of fields and $\mathcal{C}_i^* := K_{n+1-i} \times \cdots \times K_n \subseteq \mathbb{A}^i$, where $i = 1 \ldots, n$. If*

$$C_{\mathcal{C}}(d) \quad \text{is a} \quad [|\mathcal{C}|\,, \dim C_{\mathcal{C}}(d), \delta_{\mathcal{C}}(d)]\text{-code}$$

and

$$C_{\mathcal{C}_i^*}(d) \quad \text{is a} \quad \left[|\mathcal{C}_i^*|\,, \dim C_{\mathcal{C}_i^*}(d), \delta_{\mathcal{C}_i^*}(d)\right]\text{-code,}$$

then

$$|\mathcal{C}| = \sum_{i=0}^{n} |\mathcal{C}_i^*|\,, \qquad \dim C_{\mathcal{C}}(d) = \sum_{i=0}^{n} \dim C_{\mathcal{C}_i^*}(d-1) \qquad \text{and} \qquad \delta_{\mathcal{C}}(d) = \delta_{\mathcal{C}_n^*}(d-1),$$

where $\mathcal{C}_0^* := [1]$ *and* $\delta_{\mathcal{C}_n^*}(0) := d_1 \cdots d_n$.

Corollary 4.2.26 (Relationship between Generalized and Projective Reed-Muller codes). *If the Projective Reed-Muller code*

$$PC_d(n,q) \quad \textit{is a} \quad [|\mathbb{P}^n|, \dim C_{\mathbb{P}^n}(d), \delta_{\mathbb{P}^n}(d)] \text{ - } \textit{code}$$

and for $i = 1, \ldots, n$ *the Generalized Reed-Muller code*

$$GC_d(i,q) \quad \textit{is a} \quad \left[\left|\mathbb{A}^i\right|, \dim C_{\mathbb{A}^i}(d), \delta_{\mathbb{A}^i}(d)\right] \text{ - } \textit{code}\ ,$$

then

$$|\mathbb{P}^n| = \sum_{i=0}^{n} \left|\mathbb{A}^i\right|, \qquad \dim C_{\mathbb{P}^n}(d) = \sum_{i=0}^{n} \dim C_{\mathbb{A}^i}(d-1) \qquad \textit{and} \qquad \delta_{\mathbb{P}^n}(d) = \delta_{\mathbb{A}^n}(d-1),$$

where $\ell_{\mathbb{A}^0} := 1, k_{\mathbb{A}^0}(d) := 1$ *and* $\delta_{\mathbb{A}^n}(0) := q^n$.

For all unexplained terminology and additional information, we refer to [16] for the theory of lattice ideals; [57, 75, 78, 86, 97, 102] for commutative algebra, the theory of Gröbner bases, Hilbert functions, and toric ideals; [88, 98, 99] for the theory of linear codes; and [22, 23, 24, 27, 51] for the theory of Reed-Muller codes and evaluation codes.

Contents

Acknowledgements **vii**

Abstract **ix**

Resumen **xi**

Introduction **xiii**

1 Preliminaries **1**

1.1 Commutative algebra 2

1.1.1 Cohen-Macaulay rings and modules 2

1.1.2 Gröbner basis 4

1.1.3 Hilbert functions 8

1.1.4 Toric ideals 13

1.2 Algebraic geometry 15

1.3 Graph theory 17

1.4 Polyhedral sets 19

2 Lattice Ideals **21**

2.1 Identifying lattice ideals 22

2.2 Relation between a lattice and its lattice ideal 28

2.3 Binomial ideals in terms of lattice ideals 32

2.4 Gröbner basis of lattice ideals 35

2.5 Algebraic invariants of lattice ideals 37

2.6 Graded lattice ideals of dimension 1 39

2.6.1 The degree 39

Examples 45

2.6.2 A complete intersection criterion 47

2.6.3 Vanishing ideals over finite fields 51

2.7 Vanishing ideals on projective degenerate tori over finite fields 53

3 Affine Codes 61

3.1 Elementary concepts about affine codes 62

3.2 Parameterized affine codes 64

3.2.1 Length and dimension (Theoretically) 64

3.2.2 Length and dimension (Computation) 66

3.2.3 The parameterized code associated to a graph 70

3.3 Affine cartesian codes 70

3.3.1 Complete intersections and algebraic invariants 71

3.3.2 Cartesian evaluation codes 73

3.3.3 Cartesian codes over affine degenerate tori 82

4 Projective Codes 85

4.1 Parameterized projective codes 85

4.2 Projective nested cartesian codes 86

4.2.1 Length 87

4.2.2 Dimension 87

4.2.3 Minimum distance 93

A Main Results of The Thesis 103

A.1 Main results of Chapter 2 103

A.2 Main results of Chapter 3 105

A.3 Main results of Chapter 4 107

Bibliography 109

Notation 116

Index 118

Chapter 1

Preliminaries

In this chapter we introduce some important topics of commutative algebra. For instance we introduce Hilbert functions and the notion of degree. We are going to recall some well-known results about the behavior of Hilbert functions of graded ideals. In particular we recall a standard method, using Hilbert series, to compute the degree.

Toric ideals are well-known and well-studied objects in commutative algebra. In this chapter we study some technics used for toric ideals in order to obtain results about some vanishing ideals in Sections 2.6 and 2.7.

We define the sets that we use to define some evaluation codes, the main topic of Chapters 3 and 4.

Small section about graph theory is introduced here in order to understand only Subsection 3.2.3. In other words, if you do not want to read Subsection 3.2.3, you do not need to study this small section.

Finally we write a section about polyhedral sets. The reason is because in Subsection 2.6.1 we compute the degree of a family of lattice ideals and we make this computation in terms of the relative volume of a lattice polytope.

From start to finish we shall use the following symbology and terminology.

$\mathbb{Z}$	integers.
$\mathbb{R}$	real numbers.
$\mathbb{Z}_{\geq d}, \mathbb{R}_{\geq d}$	integers $\geq d$, real numbers $\geq d$.
$\mathbb{N}, \mathbb{R}_+, \mathbb{N}_+$	abbreviation for $\mathbb{Z}_{\geq 0}, \mathbb{R}_{\geq 0}, \mathbb{Z}_{\geq 1}$.
$\mathbb{F}_q$	a finite field with q elements.
$\mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$	multiplicative group of a finite field with q elements.
K	a field.
$K^* := K \setminus \{0\}$	multiplicative group of the field K.
S	a polynomial ring $K[t_1, \ldots, t_n]$ over K with n indeterminates.
$S_{\leq d}$	polynomials of S of degree at most d.
S_d	homogeneous polynomials of S of degree d union the zero polynomial.
t^a	abbreviation for the monomial $t_1^{a_1} \cdots t_n^{a_n}$, where $a := (a_i) \in \mathbb{N}^n$.

1.1 Commutative algebra

In this section we are going to introduce the following topics of commutative algebra: Cohen-Macaulay rings, Gröbner basis, Hilbert functions and toric ideals. All these topics will be very important tools for all the thesis. First for the study of lattice ideals and then for coding theory.

There are very good references to learn commutative algebra. We use mainly [65, 68, 73, 75, 78, 82, 83, 89, 90, 102, 103].

Let R be a ring, K a field and $S := K[t_1, \ldots, t_n]$ a polynomial ring over the field K with n indeterminates.

The *Krull dimension* of R, denoted by $\dim(R)$, is defined to be the supremum of the *lengths* of all strictly ascending chains of primes:

$$\dim(R) := \sup\{r \mid \text{ there is a chain of primes } \mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_r \text{ in } R\}.$$

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

$$\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_r = \mathfrak{p}$$

which end at $\mathfrak{p}$; note that $\dim(R_\mathfrak{p}) = \mathrm{ht}(\mathfrak{p})$. The *height* of an ideal I of R, denoted by $\mathrm{ht}(I)$, is defined as

$$\mathrm{ht}(I) := \min\{\mathrm{ht}(\mathfrak{p}) \mid I \subset \mathfrak{p} \text{ and } \mathfrak{p} \text{ prime}\}.$$

In general, for an arbitrary ideal I of R we have $\dim(R/I)+\mathrm{ht}(I) \leq \dim(R)$; the difference $\dim(R) - \dim(R/I)$ is called the *codimension* of I and $\dim(R/I)$ is called the *dimension* of I.

Definition 1.1.1 An ideal $I \subset S$ is called a *complete intersection* if there exist $f_1, \ldots, f_r$ in S such that $I = (f_1, \ldots, f_r)$, where r is the height of I.

1.1.1 Cohen-Macaulay rings and modules

We introduce some special types of rings and modules called Cohen-Macaulay. Let R be a ring, K a field and $S := K[t_1, \ldots, t_n]$ a polynomial ring over the field K with n indeterminates. The main references for Cohen-Macaulay modules are [73, 78, 80, 102, 103].

Definition 1.1.2 Let M be an R-module.

- An element $x \in R$ is a *zero divisor* of M if there is $0 \neq y \in M$ such that $xy = 0$. If x is not a zero divisor, we call x a *regular element* of M. The set of zero divisors of M is denoted by $\mathcal{Z}(M)$. Note that if I is an ideal of S, then

$$\mathcal{Z}(S/I) = \{f \in S \mid \text{ there is } g \notin I \text{ with } f \cdot g \in I\}.$$

- A sequence $\underline{\theta} := \theta_1, \ldots, \theta_r$ in R is called a *regular sequence* of M or an *M-regular sequence* if $(\underline{\theta})M \neq M$ and $\theta_i \notin \mathcal{Z}\left(M/\left(\theta_1, \ldots, \theta_{i-1}\right) M\right)$ for all i.

- The *annihilator* of M is given by

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

  if $y \in M$ the *annihilator* of y is $\operatorname{ann}(y) = \operatorname{ann}(Ry)$.

- The *dimension* of M is

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

  and the *codimension* of M is

$$\operatorname{codim}(M) := \dim(R) - \dim(M).$$

- M has *finite length* if there is a *composition series*

$$(0) = M_0 \subset M_1 \subset \ldots \subset M_r = M,$$

  where M_i/M_{i-1} is a nonzero *simple module* (that is, M_i/M_{i-1} has no proper submodules other than (0)) for all i. Note that M_i/M_{i-1} must be cyclic and thus isomorphic to $R/\mathfrak{m}$, for some maximal ideal $\mathfrak{m}$. The number r is independent of the composition series and is called the *length* of M, it is usually denoted by $\ell_R(M)$ or simply $\ell(M)$.

Proposition 1.1.3 *Let M be an R-module and let I be an ideal of R such that $IM \neq M$. If $\underline{\theta} = \theta_1, \ldots, \theta_r$ is an M-regular sequence in I, then $\underline{\theta}$ can be extended to a maximal M-regular sequence in I.*

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

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

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

Lemma 1.1.4 ([103, Lemma 2.3.6]) *Let M be a module over a local ring $(R, \mathfrak{m})$. If $\theta_1, \ldots, \theta_r$ is an M-regular sequence in $\mathfrak{m}$, then $r \leq \dim(M)$.*

Definition 1.1.5 Let $(R, \mathfrak{m})$ be a local ring and $M \neq 0$ an R-module.

- The *depth* of M, denoted by $\operatorname{depth}(M)$, is the length of any maximal regular sequence on M, which is contained in $\mathfrak{m}$.
- M is called a *Cohen-Macaulay module* (C-M for short) if $\operatorname{depth}(M) = \dim(M)$.
- R is called a *Cohen-Macaulay ring* if R is C-M as an R-module.
- Assume that M has dimension d. A *system of parameters* (s.o.p for short) of M is a set of elements $\theta_1, \ldots, \theta_d$ in $\mathfrak{m}$ such that

$$\ell_R \left(M / \left(\theta_1, \ldots, \theta_d \right) M \right) < \infty.$$

Definition 1.1.6 Let R be an arbitrary Noetherian ring and M an R-module.

- M is a *Cohen-Macaulay module* if $M_{\mathfrak{m}}$ is a C-M module for all maximal ideals $\mathfrak{m} \in \operatorname{Supp}(M)$. So we consider the zero module to be Cohen-Macaulay.
- As in the local case, R is a *Cohen-Macaulay ring* if R is C-M as an R-module.

Proposition 1.1.7 ([102, Proposition 1.3.17]) *Let M be a module of dimension d over a local ring $(R, \mathfrak{m})$ and let $\underline{\theta} = \theta_1, \ldots, \theta_d$ be a system of parameters of M. Then M is C-M if and only if $\underline{\theta}$ is an M-regular sequence.*

Proposition 1.1.8 ([102, Lemma 1.3.18]) *Let $(R, \mathfrak{m})$ be a local ring and let $(f_1, \ldots, f_r)$ be an ideal of height equal to r. Then there are $f_{r+1}, \ldots, f_d$ in $\mathfrak{m}$ such that $f_1, \ldots, f_d$ is a system of parameters of R.*

1.1.2 Gröbner basis

In this subsection we review some basic facts and definitions on Gröbner bases. The main references for Gröbner bases are [65, 68, 75, 78], there the reader will find a detailed discussion of Gröbner bases and the missing proofs of this subsection.

Let R be a ring, K a field and $S := K[t_1, \ldots, t_n]$ a polynomial ring over the field K with n indeterminates. A *polynomial* of S can be defined as a finite sum of terms. The presentation of a polynomial as a linear combination of monomials is unique only up to an order of the summands, due to the commutativity of the addition. We can make this order unique by choosing an order on the set of monomials.

Definition 1.1.9 A *monomial order* on S is any relation $\succ$ on $\mathbb{N}^n$, or equivalently, any relation on the set of monomials $\operatorname{Mon}(S) := \{t^a \mid a \in \mathbb{N}^n\}$ satisfying the following three conditions.

(i) $\succ$ is a total order ($t^a \succ t^b$ or $t^a = t^b$ or $t^a \prec t^b$).

(ii) If $t^a \succ t^b$ and $c \in \mathbb{N}^n$, then $t^c t^a \succ t^c t^b$.

(iii) $\succ$ is a well-ordering on $\mathbb{N}^n$. This means that every nonempty subset of $\mathbb{N}^n$ has a smallest element under $\succ$.

Some monomial orders are listed in the next definition.

Definition 1.1.10 Monomials orders.

- *Lexicographical order* $\succ_{lex}$

$$t^a \succ_{lex} t^b \Longleftrightarrow \exists 1 \leq i \leq n : a_1 = b_1, \ldots, a_{i-1} = b_{i-1}, a_i > b_i.$$

- *Reverse lexicographical order* $\succ_{revlex}$

$$t^a \succ_{revlex} t^b \Longleftrightarrow \exists 1 \leq i \leq n : a_n = b_n, \ldots, a_{i+1} = b_{i+1}, a_i < b_i$$

- *Degree lexicographical order* $\succ_{Dp}$

$$t^a \succ_{Dp} t^b \Longleftrightarrow \qquad \deg t^a > \deg t^b \qquad \text{or} \qquad \left(\deg t^a = \deg t^b \text{ and } t^a \succ_{lex} t^b\right).$$

- *Degree reverse lexicographical order* $\succ_{dp}$

$$t^a \succ_{dp} t^b \Longleftrightarrow \qquad \deg t^a > \deg t^b \qquad \text{or} \qquad \left(\deg t^a = \deg t^b \text{ and } t^a \succ_{revlex} t^b\right).$$

Definition 1.1.11 Let $f := \sum_a \alpha_a t^a$ be a nonzero polynomial in S and let $\succ$ be a monomial order on S.

- The *multidegree* of f is denoted and defined by

$$\text{multideg}(f) := \max \{a \mid \alpha_a \neq 0\},$$

  where max is taken with respect to $\succ$.

- The *degree* of f is denoted and defined by

$$\deg_{\prec}(f) := \sum_{i=1}^{n} (\text{multideg}(f))_i .$$

  Observe that $\deg_{\prec}(t^a) = a_1 + \cdots + a_n$.

- The *total degree* of f is denoted and defined by

$$\deg_{total}(f) := \max \{\deg_{\prec}(t^a) \in \mathbb{N} \mid \alpha_a \neq \mathbf{0}\},$$

  where max is taken in $\mathbb{N}$.

- The *degree with respect to* t_i of f is denoted and defined by

$$\deg_{t_i}(f) := \deg_{\prec}(f(1,\ldots,1,t_i,1,\ldots,1)).$$

- The *leading coefficient* of f is denoted and defined by

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

  The *leading monomial* of f is denoted and defined by

$$\mathrm{LM}(f) := t^{\mathrm{multideg}(f)}.$$

  The *leading term* of f is denoted and defined by

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

Proposition 1.1.12 (Division algorithm on S [75, Theorem 3, pag 64]) *Fix a monomial order $\succ$ on S, and let $\mathcal{F} := \{f_1,\ldots,f_r\}$ be an ordered r-tuple of polynomials in S. Then every $f \in S$ can be written as*

$$f = g_1 f_1 + \cdots g_r f_r + \overline{f}^{\mathcal{F}},$$

where $g_i, \overline{f}^{\mathcal{F}} \in S$, and either $\overline{f}^{\mathcal{F}} = 0$ or $\overline{f}^{\mathcal{F}}$ is a linear combination, with coefficients in K, of monomials, none of which is divisible by any of $LT(f_1),\ldots,LT(f_r)$. We will call $\overline{f}^{\mathcal{F}}$ the remainder of f by the ordered r-tuple $\mathcal{F} = \{f_1,\ldots,f_r\}$. Furthermore, if $g_i f_i \neq 0$, then we have

$$multideg(f) \succ= multideg(g_i f_i).$$

Definition 1.1.13 Fix a monomial order $\succ$ on S and let $I \subset S$ be an ideal other than $\{0\}$. We denote by $\mathrm{LT}(I)$ the *initial ideal*, i.e., the ideal generated by the leading terms (with respect to $\prec$) of the elements of I.

Definition 1.1.14 A finite subset $\mathcal{G} := \{g_1,\ldots,g_r\}$ of an ideal $I \subset S$ is said to be a *Gröbner basis* if

$$(LT(g_1),\ldots,LT(g_r)) = LT(I).$$

Equivalently, but more informally, $\mathcal{G}$ is a Gröbner basis of I if and only if the leading term of any element of I is divisible by one of the $LT(g_i)$.

Proposition 1.1.15 [75, Corollary 6, pag 77] *Fix a monomial order on S. Then every ideal I of S other than $\{0\}$ has a Gröbner basis. Furthermore, any Gröbner basis of an ideal I is a set of generators of I.*

Gröbner basis are useful, among others things, because it can tell us when an element of S is a member of an ideal I.

Proposition 1.1.16 [65, Proposition 1.6.7 (1)] *Fix a monomial order on S. Let $\mathcal{G}$ be a Gröbner basis of an ideal $I \subset S$ and let $f \in S$. Then $f \in I$ if and only if the remainder on division of f by $\mathcal{G}$ is zero, i.e.,*

$$f \in I \qquad \textit{if and only if} \qquad \overline{f}^{\mathcal{G}} = 0.$$

Given an ideal I we would like to find a Gröbner basis for this ideal, to solve this problem we need the following tools.

Definition 1.1.17 Fix a monomial order on S and let $f, g \in S$ be nonzero polynomials.

(i) Assume $\text{multideg}(f) = a$ and $\text{multideg}(g) = b$. Define $c := (c_1, \ldots, c_n)$ and $\gamma := (\gamma_1, \ldots, \gamma_n)$, where $c_i := \max\{a_i, b_i\}$ and $\gamma_i := \min\{a_i, b_i\}$ for each i. We call t^c the *least common multiple* of LM(f) and LM(g), and it is denoted by $\text{lcm}(\text{LM}(f), \text{LM}(g))$. t^γ is called the *greatest common divisor* of LM(f) and LM(g), and it is denoted by $\text{gcd}(\text{LM}(f), \text{LM}(g))$.

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

$$\text{S}(f, g) := \frac{t^c}{\text{LT}(f)} \cdot f - \frac{t^c}{\text{LT}(g)} \cdot g.$$

S-polynomials are important because they can tell us when a set of generators of an ideal I is a Gröbner basis.

Proposition 1.1.18 (Buchberger's Criterion [75, Theorem 6, pag 85]) *Fix a monomial order on S and let $I := (g_1, \ldots, g_r)$ be an ideal of S. Then $\mathcal{G} := \{g_1, \ldots, g_r\}$ is a Gröbner basis of I if and only if for all pairs i, j we have that $\overline{S(g_i, g_j)}^{\mathcal{G}}$ is zero.*

By Proposition 1.1.15 we know that a Gröbner basis of an ideal I always exists. Furthermore by Proposition 1.1.18 we have a criterion to identify if a set of generators of an ideal is also a Gröbner basis. Given an ideal I, the following remarkable algorithm uses these previous facts to give a method to find a Gröbner basis of I.

Proposition 1.1.19 (Buchberger's Algorithm [75, Theorem 2, pag 90]) *Fix a monomial order on S and let $I := (f_1, \ldots, f_s)$ be an ideal of S. A Gröbner basis of I can be con-*

structured in a finite number of steps by the following algorithm:

Data*:* $\mathcal{F} := \{f_1, \ldots, f_s\}$
Result*: A Gröbner basis* $\mathcal{G} := \{g_1, \ldots, g_r\}$ *of* I*, with* $\mathcal{F} \subset \mathcal{G}$
$\mathcal{G} := \mathcal{F}$*;*
repeat
  $\mathcal{G}' := \mathcal{G}$
  for *each pair* $\{f, g\}$, $f \neq g$ *in* $\mathcal{G}'$ **do**
    $f^* := \overline{S(f, g)}^{\mathcal{G}'}$
    if $f^* \neq 0$ **then**
      $\mathcal{G} := \mathcal{G} \cup \{f^*\}$
    end
  end
until $\mathcal{G} = \mathcal{G}'$ *;*

Definition 1.1.20 Fix a monomial order on S. We have two special sorts of Gröbner basis.

(i) A *minimal Gröbner basis* of I is a Gröbner basis $\mathcal{G}$ of I such that the following conditions are satisfied.

  (a) $\mathrm{LC}(g) = 1$ for all $g \in \mathcal{G}$.

  (b) For all $g \in \mathcal{G}$, $\mathrm{LT}(g) \notin \mathrm{LT}(\mathcal{G} - \{g\})$.

(ii) A *reduced Gröbner basis* of I is a Gröbner basis $\mathcal{G}$ of I such that the following conditions are satisfied.

  (a) $\mathrm{LC}(g) = 1$ for all $g \in \mathcal{G}$.

  (b) For all $g \in \mathcal{G}$, no monomial of g lies in $\mathrm{LT}(\mathcal{G} - \{g\})$.

The "problem" with a Gröbner basis of an ideal I is that it is not unique, but the reduced Gröbner basis are unique.

Proposition 1.1.21 [75, Proposition 6, pag 92] *Let* $I \neq \{0\}$ *be an ideal. Then, for a given monomial order,* I *has a unique reduced Gröbner basis.*

1.1.3 Hilbert functions

We introduce Hilbert functions and the notion of degree. We will recall some well-known results about the behavior of Hilbert functions of graded ideals. In particular we recall a standard method, using Hilbert series, to compute the degree. The main references for Hilbert functions are [65, 68, 75, 78].

Definition 1.1.22 We call a ring R *graded* if there are additive subgroups R_d for $d \in \mathbb{N}$ with $R = \bigoplus R_d$ and $R_d R_m \subset R_{d+m}$ for all $d, m \in \mathbb{N}$. The elements of R_d are called *homogeneous elements of degree d*.

Definition 1.1.23 An ideal I of a graded ring $R := \bigoplus R_d$ is called a *graded ideal* or a *homogeneous ideal* if it is generated by homogeneous elements.

Lemma 1.1.24 [65, Lemma 2.2.7] *Let I be an ideal of a graded ring $R := \bigoplus R_d$. The following conditions are equivalents.*

(i) *I is a graded ideal.*

(ii) *I is graded with the induced grading, that is, $I = \bigoplus_d (R_d \cap I)$.*

(iii) *Let $f := \sum f_d$ be a element of R, with $f_d \in R_d$. Then $f \in I$ if and only if $f_d \in I$ for all d.*

Example 1.1.25 Let see how S can be graded.

(i) If we take $S_0 := K$ and for $d > 0$ we construct S_d as the K-vector space generated by the monomials t^a with $\deg(t^a) = d$, then S has the *standard grading* $S := \bigoplus S_d$. If I is a graded ideal of S, we say that I is *standard graded*.

(ii) If now we take a vector of positive integers $\omega := (\omega_1, \ldots, \omega_n)$, then S has the *grading induced by* ω, or the *grading induced by setting* $\deg(t_i) := \omega_i$ for $i = 1, \ldots, n$, if we make $S := \bigoplus S_d$, where S_d is the K-vector space generated by all monomials t^a, with $\langle \omega, a \rangle = d$. In this case we say that S is *ω-graded*. If I is a graded ideal of S, we say that I is *ω-graded*.

Definition 1.1.26 Assume $S := K[t_1, \ldots, t_n] = \bigoplus_{d=0}^{\infty} S_d$ has the standard grading and let I be a graded ideal of S.

(i) The *Hilbert function* of S/I, denoted by H_I, is given by

$$H_I(d) := \dim_K (S/I)_d = \dim_K S_d / I_d,$$

where $I_d := I \cap S_d$ is the degree d part of I.

(ii) The *Hilbert series* of S/I, denoted by HP_I, is given by

$$HP_I(t) := \sum_{d \geq 0} H_I(d) \cdot t^d.$$

Remark 1.1.27 When I is a monomial ideal, $H_I(d)$ is the number of monomials not in I of degree d, and by [75, Proposition 8, pag 452], for d sufficiently large, we can express the Hilbert function of I in the form

$$H_I(d) = \sum_{i=1}^{r} b_i \binom{d}{r-i}.$$

Proposition 1.1.28 [75, Proposition 9, pag 463] *Let I be a homogeneous ideal and let $\succ$ be a monomial order on S. Then the monomial ideal $LT(I)$ has the same Hilbert function as I.*

Definition 1.1.29 (Same hypothesis that Definition 1.1.26) Using Remark 1.1.27 and Proposition 1.1.28 we can define the *Hilbert polynomial* of S/I as the unique polynomial $h_I(t) := \sum_{i=0}^{k-1} c_i t^i \in \mathbb{Q}[t]$ such that for d sufficiently large we have

$$H_I(d) = h_I(d).$$

Definition 1.1.30 (Same hypothesis that Definition 1.1.26) Let $h_I(t) := \sum_{i=0}^{k-1} c_i t^i \in \mathbb{Q}[t]$ be the Hilbert polynomial of S/I.

(i) If $\dim(S/I) \geq 1$, the integer $c_{k-1}(k-1)!$, denoted by $\deg(S/I)$, is called the *degree* of S/I or the *degree* of I.

(ii) If $\dim(S/I) = 0$, the integer $\dim_K(S/I)$ is called the *degree* of S/I.

Thanks to Hilbert-Serre's theorem we can extract a lot of information from the Hilbert series.

Proposition 1.1.31 (Hilbert-Serre [68, Corollary 20.8]) *Assume S has the standard grading and let I be a graded ideal of S. Then*

(i) The Hilbert series of I can be written uniquely in the form $HP_I(t) = \frac{p(t)}{(1-t)^k}$, where $p(t) \in \mathbb{Z}[t], p(1) \neq 0$ and $n \geq k \geq 0$.

(ii) The Hilbert polynomial $h_I(t)$ has degree $k-1$ and has leading coefficient $p(1)/(k-1)!$. Furthermore for $d \geq \deg(p(t)) - k + 1$ we have $H_I(d) = h_I(d)$ (function and polynomial agree).

(iii) $k = \dim(S/I)$.

(iv) $\deg(S/I) = p(1)$.

The following result is about the behavior of the Hilbert function and it will be useful for our research.

Lemma 1.1.32 (a) *If $S_i = I_i$ for some $i \geq 1$, then $S_d = I_d$ for all $d \geq i$.*

(b) *If* $\dim\, S/I \geq 1$*, then $H_I(i) > 0$ for $i \geq 0$.*

Proof. (a) It suffices to prove the case $d = i + 1$. As $I_{i+1} \subset S_{i+1}$, we need only show $S_{i+1} \subset I_{i+1}$. Take a monomial f in S_{i+1}. Then, $f = t_1^{a_1} \cdots t_s^{a_s}$ with $\sum_{i=1}^{s} a_i = i + 1$ and $a_j > 0$ for some j. Thus, $f \in S_1 S_i$. As $S_1 S_i = S_1 I_i \subset I_{i+1}$, we get $f \in I_{i+1}$.

(b) The Hilbert polynomial h_I of S/I has degree $\dim(S/I) - 1 \geq 0$. Hence, h_I is a non-zero polynomial. If $H_I(i) = \dim_K(S/I)_i = 0$ for some i, then $S_i = I_i$. Thus, by (a), $H_I(d)$ vanishes for $d \geq i$, a contradiction because the Hilbert polynomial of S/I is non-zero. $\square$

Next, we recall and prove a general fact about 1-dimensional Cohen-Macaulay graded ideals: *the Hilbert function is increasing until it reaches a constant value*. This behavior was pointed out in [14, p. 456] (resp. [21, Remark 1.1, p. 166]) for finite (resp. infinite) fields, see also [11]. No proof was given in neither of these places, likely because the result is not hard to show.

Proposition 1.1.33 (i) *If* $\dim\, S/I \geq 2$ *and* $\operatorname{depth} S/I > 0$*, then $H_I(i) < H_I(i+1)$ for $i \geq 0$.*

(ii) *If* $\operatorname{depth} S/I = \dim\, S/I = 1$*, then there is an integer $r \geq 0$ such that*

$$1 = H_I(0) < H_I(1) < \cdots < H_I(r-1) < H_I(i) = \deg(S/I) \quad \textit{for } i \geq r.$$

Proof. Consider the algebraic closure $\overline{K}$ of the field K. We set

$$\overline{S} = S \otimes_K \overline{K} \quad \text{and} \quad \overline{I} = I\overline{S}.$$

By [57, Lemma 1.1], S/I and $\overline{S}/\overline{I}$ have the same Krull dimension, the same depth, and the same Hilbert function. Hence, replacing K by $\overline{K}$, we may assume that K is infinite. As S/I has positive depth, there is $h \in S_1$ which is a non zero-divisor of S/I. Applying the function $\dim_K(\cdot)$ to the exact sequence

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

we get $H_I(i+1) - H_I(i) = H(i+1) \geq 0$ for $i \geq 0$, where $H(i) = \dim_K(S/(h, I))_i$. We set $S' = S/(h, I)$. Notice that $\dim(S') = \dim(S/I) - 1$.

(i) If $H(i+1) = 0$ for some $i \geq 0$, then, by Lemma 1.1.32(a), $\dim_K(S') < \infty$. Hence S' is Artinian, i.e., $\dim(S') = 0$, a contradiction. Thus, $H_I(i+1) > H_I(i)$ for $i \geq 0$.

(ii) Since $\dim(S/I) = 1$, the Hilbert polynomial of S/I is a non-zero constant equal to $\deg(S/I)$. Let $r \geq 0$ be the first integer such that $H_I(r) = H_I(r+1)$, thus $S'_{r+1} = (0)$, i.e., $S_{r+1} = (h, I)_{r+1}$. Then, by Lemma 1.1.32(a), $S'_i = (0)$ for $i \geq r+1$. Hence, the Hilbert function of S/I is constant for $i \geq r$ and strictly increasing on $[0, r-1]$. $\square$

In words of Dr. David Eisenbud, "the *regularity* of an ideal in S is an important measure of how complicated the ideal is". This measure can be defined in terms of a *complex*. For the purpose of our work, we will take an equivalent definition of regularity, which is valid when S/I is Cohen-Macaulay [80, Proposition 4.2].

Definition 1.1.34 Assume S has the standard grading and let I be a graded ideal of S such that S/I is Cohen-Macaulay.

(i) The *index of regularity* of S/I, denoted by $\text{reg}(S/I)$, is the least integer $r \geq 0$ such that $h_I(d) = H_I(d)$ for $d \geq r$.

(ii) The integer $\text{reg}(S/I)-1$ is denoted by $a(S/I)$, or $a(I)$, and it is called the *a-invariant* of S/I, or *a-invariant* of I.

We can complete the Proposition1.1.31 using the hypothesis that S/I is Cohen-Macaulay.

Proposition 1.1.35 *Continuation of Proposition1.1.31 using the extra hypothesis that S/I is Cohen-Macaulay.*

(v) $a(S/I) = \deg(p(t)) - k$.

(vi) $\text{reg}(S/I) = \deg(p(t)) - k + 1$.

Thus, the computation of the dimension, degree, a-invariant or index of regularity is reduced to the computation of the Hilbert series of S/I. There are a number of computer algebra systems (*Macaulay*2 [61], *CoCoA* [63], *Singular [65]*) that compute the Hilbert series and the degree of S/I using Gröbner bases. Two excellent references to compute Hilbert series, using elimination of variables, are [3, 7].

Finally some definitions and a result that will be useful for this thesis.

Definition 1.1.36 Let I, J be ideals of S.

- The *ideal quotient* of I by J is defined as
$$I : J := \{f \in S \mid f \cdot J \subset I\}.$$
- The *saturation* of I with respect to J is
$$I : J^\infty := \{f \in S \mid \text{ there is } r \in \mathbb{N} \text{ such that } f \cdot J^r \subset I\}.$$
- In particular
$$I : (t_1 \cdots t_n)^\infty = \{f \in S \mid \text{ there is } r \in \mathbb{N} \text{ with } f \cdot (t_1 \cdots t_n)^r \in I\}.$$
- The *radical* of I, denoted by $\sqrt{I}$ or $\text{rad}(I)$, is the ideal
$$\sqrt{I} := \{f \in S \mid \text{ there is } r \in \mathbb{N} \text{ with } f^r \in I\}.$$

Proposition 1.1.37 *Let I be an ideal of S. The following hold.*

(a) [47] *If $LT(I)$is square-free, then* $\text{rad}(I) = I$.

(b) [82, Corollary 6.9] *If I is graded and $LT(I)$ is Cohen-Macaulay (resp. Gorenstein), then I is Cohen-Macaulay (resp. Gorenstein).*

1.1.4 Toric ideals

Toric ideals are well-known and well-studied objects in commutative algebra. In this section we study some technics used for toric ideals in order to obtain results about vanishing ideals of projective algebraic toric sets in Section 2.6 and projective degenerate torus in Section 2.7. Let K be a field, $S := K[t_1, \ldots, t_n]$ a polynomial ring over the field K with n indeterminates and $S' := K[x_1, \ldots, x_s]$ a polynomial ring with s indeterminates over the same field K. There is an isomorphism between the multiplicative semigroup of monomials of S' and the additive semigroup $\mathbb{N}^s$:

$$\begin{array}{rcl} \mathrm{Mon}(S') & \to & \mathbb{N}^s \\ x^a := x_1^{a_1} \cdots x_s^{a_s} & \to & a := (a_1, \ldots, a_s) \\ x^{a+b} := x^a x^b & \to & a + b. \end{array}$$

Let $\mathcal{F} := \{f_1 := x^{v_1}, \ldots, f_n := x^{v_n}\}$ be a finite set of n distinct monomials in S' with $f_i \neq 1$ for all i. The set $\mathcal{F}$ has a corresponding set of vectors in $\mathbb{N}^s$ under the previous isomorphism:

$$\mathcal{F} = \{x^{v_1}, \ldots, x^{v_n}\} \quad \to \quad \mathcal{A} := \{v_1, \ldots, v_n\}.$$

Definition 1.1.38 The *monomial subring* generated or spanned by $\mathcal{F}$ is denoted and defined by

$$K[\mathcal{F}] := \bigcap_{\mathcal{R} \in \mathfrak{R}} \mathcal{R},$$

where $\mathfrak{R}$ is the family of all subrings $\mathcal{R}$ of S' such that $K \cup \mathcal{F} \subset \mathcal{R}$.

The elements of $K[\mathcal{F}]$ are polynomial expressions with coefficients in K :

$$\sum_{finite} \alpha_a (x^{v_1})^{a_1} \cdots (x^{v_n})^{a_n},$$

where $\alpha_a \in K$ and $a := (a_1, \ldots, a_n) \in \mathbb{N}^n$.

Let $\mathbb{N}\mathcal{A} := \mathbb{N}v_1 + \cdots + \mathbb{N}v_n$ be the subsemigroup of $\mathbb{N}^s$ generated by the set $\mathcal{A}$. As K-vector space $K[\mathcal{F}]$ is generated by the set of monomials of the form x^a, with $a \in \mathbb{N}\mathcal{A}$. Consequently

$$K[\mathcal{F}] = K[\mathbb{N}\mathcal{A}] := K[\{x^a \mid a \in \mathbb{N}\mathcal{A}\}],$$

thus $K[\mathcal{F}]$ is the semigroup ring of $\mathbb{N}\mathcal{A}$. Assume that $S' := \oplus_{i \geq 0} S'_i$ has the standard grading. An important feature of $K[\mathcal{F}]$ is that it is a graded subring of S' with the grading given by

$$K[\mathcal{F}]_i := K[\mathcal{F}] \cap S'_i.$$

There is a graded epimorphism of K-algebras:

$$\begin{array}{rcl} \varphi : S & \longrightarrow & K[\mathcal{F}] \\ \varphi(t_i) & \longrightarrow & f_i, \end{array}$$

where S is graded by $\deg(t_i) := |v_i|$. Note that in general we have

$$\varphi(h(t_1,\ldots,t_n)) = h(f_1,\ldots,f_n), \text{ for all } h \in S.$$

The kernel of φ, denoted by $P_{\mathcal{F}}$, is called the *toric ideal* of $K[\mathcal{F}]$ with respect to $f_1,\ldots,f_n$. We also denote the toric ideal of $K[\mathcal{F}]$ by $I_{\mathcal{A}}$. We say that $I_{\mathcal{A}}$ is the toric ideal of $\mathcal{A}$.

Theorem 1.1.39 [102, Proposition 7.1.2] *$P_{\mathcal{F}}$ is a graded prime ideal generated by a finite set of pure binomials.*

Definition 1.1.40 If $\mathcal{F} := \{x^{v_1},\ldots,x^{v_n}\}$ is a set of monomials in S', the *associated matrix* of $K[\mathcal{F}]$, denoted by A, is the $s \times n$ matrix whose columns are the exponent vectors $v_1,\ldots,v_n$.

Corollary 1.1.41 [102, Corollary 7.1.4] *If A is the associated matrix of $K[\mathcal{F}]$, then*

$$P_{\mathcal{F}} = \left(\left\{t^{a^+} - t^{a^-} \mid a \in \mathbb{Z}^n \text{ and } Aa = 0\right\}\right).$$

This result can be restated as:

Corollary 1.1.42 *The toric ideal of $\mathcal{A} := \{v_1,\ldots,v_n\}$ is given by*

$$I_{\mathcal{A}} = \left(t^a - t^b \mid a := (a_i)\,, b := (b_i) \in \mathbb{N}^n, \sum a_i v_i = \sum b_i v_i\right) \subset S.$$

Corollary 1.1.43 [102, Corollary 7.1.5] *$P_{\mathcal{F}}$ has a Gröbner basis consisting of pure binomials with respect to any monomial ordering of the polynomial ring S.*

Definition 1.1.44 Let $\mathcal{F}$ be a finite set of monomials in S and let $P_{\mathcal{F}}$ be the toric ideal of $K[\mathcal{F}]$. A pure binomial $t^a - t^b \in P_{\mathcal{F}}$ is called *primitive* if there is no other pure binomial $t^\gamma - t^\delta \in P_{\mathcal{F}}$ such that t^γ divides t^a and t^δ divides t^b.

Lemma 1.1.45 [103, Lemma 8.33] *If f is a pure binomial in the reduced Gröbner basis of $P_{\mathcal{F}}$ with respect to some term order $\prec$, then f is a primitive binomial.*

Definition 1.1.46 The *universal Gröbner basis* of a toric ideal $P_{\mathcal{F}}$ is a finite set $\mathcal{U} \subset I$ which is a Gröbner basis of I with respect to all term orders.

Theorem 1.1.47 [103, Proposition 8.3.6] *If $P := P_{\mathcal{F}}$ is the toric ideal of a monomial subring $K[\mathcal{F}]$, then the set $\mathcal{G}_P$ of primitive pure binomials in P contains the universal Gröbner basis of $P_{\mathcal{F}}$.*

If $\mathcal{F}$ is a subset of $K(x_1, \ldots, x_s)$, we define $P_{\mathcal{F}}$ and $K[\mathcal{F}]$ of a similar way that when $\mathcal{F}$ is a subset of S'.

Theorem 1.1.48 [103, Proposition 8.2.12] *If $\mathcal{F} := \{f_1/g_1, \ldots, f_n/g_n\} \subset K(x_1, \ldots, x_s)$ is a set of rational functions with $f_i, g_i \in S'$ and $g_i \neq 0$ for all i, then the kernel of the homomorphism of K-algebras*

$$\begin{array}{rcl} \varphi : S = K[t_1, \ldots, t_n] & \longrightarrow & K[\mathcal{F}] \\ t_i & \longrightarrow & f_i/g_i, \end{array}$$

is the ideal

$$(g_1 t_1 - f_1, \ldots, g_n t_n - f_n, y g_1 \cdots g_n - 1) \cap S,$$

where y is an extra variable.

Theorem 1.1.49 *Let $\mathcal{F} := \{x^{v_i}\}_{i=1}^{r}$ be a set of distinct monomials in $K(x_1, \ldots, x_s)$ with $f_i \neq 1$ for all i.*

- ([97],[103, Theorem 9.6.16]) *If the initial ideal $LT(P_{\mathcal{F}})$ is generated by square-free monomials, then $K[\mathcal{F}]$ is normal.*
- ([31],[73, Theorem 6.3.5]) *If $K[\mathcal{F}]$ is normal, then $K[\mathcal{F}]$ is Cohen-Macaulay.*

Theorem 1.1.50 [103, Proposition 8.2.12] *If R is a polynomial ring over a field K and $f_1, \ldots, f_n$ are in R, then the kernel of the homomorphism of K-algebras*

$$\begin{array}{rcl} \varphi : S = K[t_1, \ldots, t_n] & \longrightarrow & K[f_1, \ldots, f_n] \\ t_i & \longrightarrow & f_i, \end{array}$$

is the ideal

$$(t_1 - f_1, \ldots, t_n - f_n) \cap S.$$

For toric ideals there are methods, implemented in *Normaliz* [62], to compute its Hilbert series and its degree using polyhedral geometry.

1.2 Algebraic geometry

Definitions that we introduce in this section are simple and can be found at all basic algebraic geometry book, for instance [75, 86]. Sets that we define in this section will be important to define some evaluation codes, the main topic of Chapters 3 and 4.

Let K be an arbitrary field, $K^* := K \setminus \{0\}$ the multiplicative group of K and $S := K[t_1, \ldots, t_n]$ a polynomial ring over K with n indeterminates.

Definition 1.2.1 Spaces.

(i) The *affine space* of dimension n over K, denoted by $\mathbb{A}^n_K$, is the cartesian product K^n of n-copies of K. If there is not ambiguity hazard about the field, we denote $\mathbb{A}^n_K$ only by $\mathbb{A}^n$.

(ii) The *projective space* of dimension n over K, denoted by $\mathbb{P}^n_K$, (or simply by $\mathbb{P}^n$ if there is not ambiguity hazard about the field) is defined as the quotient space

$$\left(K^{n+1} \setminus \{\mathbf{0}\}\right) / \sim,$$

where two points $\mathbf{a}, \mathbf{b}$ in $K^{n+1} \setminus \{\mathbf{0}\}$ are equivalent if there is $\lambda \in K$ such that $\mathbf{a} = \lambda \mathbf{b}$. It is usual to denote the equivalent class of $\mathbf{a}$ by $[\mathbf{a}]$.

Definition 1.2.2 Varieties.

(i) Given an ideal $I \subset S$, its *zero set* or *variety*, denoted by $V(I)$, is the set of all $\mathbf{a} \in \mathbb{A}^n$ such that $f(\mathbf{a}) = 0$ for all $f \in I$.

(ii) Given a homogeneous ideal $I \subset S[t_0]$, its *zero set* or *projective variety*, denoted by $V(I)$, is the set of all $\mathbf{p} \in \mathbb{P}^n_K$ such that $f(\mathbf{p}) = 0$ for all homogeneous polynomials $f \in I$.

Definition 1.2.3 Zariski Topologies.

(i) We can define a topology on $\mathbb{A}^n$, called the *Zariski topology on* $\mathbb{A}^n$, by defining the closed subsets to be the varieties. $\mathcal{X}^* \subset \mathbb{A}^n$ is open if and only if $\mathbb{A}^n \setminus \mathcal{X}^* = V(I)$, for some ideal $I \subset S$.

(ii) We can define a topology on $\mathbb{P}^n$, called the *Zariski topology on* $\mathbb{P}^n$, by defining the closed subsets to be the projective varieties. $\mathcal{X} \subset \mathbb{P}^n$ is open if and only if $\mathbb{P}^n \setminus \mathcal{X} = V(I)$, for some homogeneous ideal $I \subset S$.

Definition 1.2.4 Vanishing ideals.

(i) If $\mathcal{X}^*$ is a subset of $\mathbb{A}^n$, the *vanishing ideal* of $\mathcal{X}^*$, denoted by $I(\mathcal{X}^*)$, is the ideal of S generated by the polynomials that vanish at all points of $\mathcal{X}^*$.

(ii) If $\mathcal{X}$ is a subset of $\mathbb{P}^n$, the *vanishing ideal* of $\mathcal{X}$, denoted by $I(\mathcal{X})$, is the ideal of $S[t_0]$ generated by the homogeneous polynomials that vanish at all points of $\mathcal{X}$.

Definition 1.2.5 Let $\mathcal{X}^*$ be a subset of $\mathbb{A}^n$. The *projective closure* of $\mathcal{X}^*$, denoted by $\overline{\mathcal{X}^*}$, is defined as the closure of the set $\{[(\mathbf{a}, 1)] \mid \mathbf{a} \in \mathcal{X}^*\}$ in the Zariski topology of $\mathbb{P}^n$.

Remark 1.2.6 Note that if $\mathbf{a} := [(\mathbf{a}_1, \ldots, \mathbf{a}_n, 1)]$ and $\mathbf{b} := [(\mathbf{b}_1, \ldots, \mathbf{b}_n, 1)]$ are two points of $\mathbb{P}^n$, then $\{\mathbf{a}\} = V(I_\mathbf{a})$ and $\{\mathbf{b}\} = V(I_\mathbf{b})$, where $I_\mathbf{a} := (t_1 - \mathbf{a}_1 t_{n+1}, \ldots, t_n - \mathbf{a}_n t_{n+1})$ and $I_\mathbf{b} := (t_1 - \mathbf{b}_1 t_{n+1}, \ldots, t_n - \mathbf{b}_n t_{n+1})$. Thus $\{\mathbf{a}\} \cup \{\mathbf{b}\} = V(I_\mathbf{a} I_\mathbf{b})$. As a conclusion, if $\mathcal{X}^*$ is a finite subset of $\mathbb{A}^n$, then $\overline{\mathcal{X}^*} = \{[(\mathbf{a}, 1)] \mid \mathbf{a} \in \mathcal{X}^*\}$.

Definition 1.2.7 Let $\upsilon = \{\upsilon_1, \ldots, \upsilon_n\}$ be a sequence of positive integers.

- The set $T^* := \{(x_1, \ldots, x_n) \in \mathbb{A}^n \mid x_i \in K^*\}$ is called an *affine torus.*
- The set $T := \{[(x_1, \ldots, x_n)] \mid x_i \in K^*\} \subset \mathbb{P}^{n-1}$ is called a *projective torus.*
- The set $\mathcal{T}^* := \{(x_1^{\upsilon_1}, \ldots, x_n^{\upsilon_n}) \in \mathbb{A}^n | \, x_i \in K^* \text{ for all } i\}$ is called an *affine degenerate torus* of type υ on $\mathbb{A}^n$.
- The set $\mathcal{T} := \{[(x_1^{\upsilon_1}, \ldots, x_n^{\upsilon_n})] \,|\, x_i \in K^* \text{ for all } i\} \subset \mathbb{P}^{n-1}$ is called a *projective degenerate torus* of type υ on $\mathbb{P}^{n-1}$.

Definition 1.2.8 Let $\upsilon_1, \ldots, \upsilon_n$ be a sequence of vectors in $\mathbb{N}^s$ with $\upsilon_i = (\upsilon_{i1}, \ldots, \upsilon_{is})$ for $1 \leq i \leq n$.

- The set $\mathcal{Q}^* := \{(x_1^{\upsilon_{11}} \cdots x_s^{\upsilon_{1s}}, \ldots, x_1^{\upsilon_{n1}} \cdots x_s^{\upsilon_{ns}}) \in \mathbb{A}^n | \, x_i \in K^* \text{ for all } i\}$ is called an *affine algebraic toric set* parameterized by the vectors $\upsilon_1, \ldots, \upsilon_n$ on $\mathbb{A}^n$.
- The set $\mathcal{Q} := \{[(x_1^{\upsilon_{11}} \cdots x_s^{\upsilon_{1s}}, \ldots, x_1^{\upsilon_{n1}} \cdots x_s^{\upsilon_{ns}})] \,|\, x_i \in \mathbb{F}_q^* \text{ for all } i\} \subset \mathbb{P}^{n-1}$ is called a *projective algebraic toric set* parameterized by the vectors $\upsilon_1, \ldots, \upsilon_n$ on $\mathbb{P}^{n-1}$.

1.3 Graph theory

Concepts about graph theory are introduced in order to understand only Subsection 3.2.3. In other words, if you do not want to read Subsection 3.2.3, you do not study this section. The main references for graph theory are [72, 77].

A *graph* $\mathbf{G}$ is an ordered pair of disjoint finite sets $(\mathbf{V}, \mathbf{E})$ such that $\mathbf{E}$ is a subset of the set of unordered pairs of $\mathbf{V}$. The set $\mathbf{V}$ is the set of *vertices* and the set $\mathbf{E}$ is called the set of *edges*. In order to be more precise and to avoid confusions with different graphs, it is usual to write $V(\mathbf{G})$ and $E(\mathbf{G})$ for the vertex set and edge set of $\mathbf{G}$, respectively.

Let $\mathbf{G} := (\mathbf{V}, \mathbf{E})$ be a graph and $\mathbf{e} := \{\mathbf{x}, \mathbf{y}\}$ an edge of $\mathbf{G}$, ($\mathbf{e}$ is also denoted by $\mathbf{xy}$) $\mathbf{e}$ is said to join the vertices $\mathbf{x}$ and $\mathbf{y}$ and we say that the vertices $\mathbf{x}$ and $\mathbf{y}$ are *adjacent vertices* of $\mathbf{G}$; it is also usual to say that $\mathbf{e}$ is *incident* with $\mathbf{x}$ and $\mathbf{y}$. The *degree* of a vertex $\mathbf{x}$ in $\mathbf{V}$, denoted by $\deg(\mathbf{x})$, is the number of incident edges with $\mathbf{x}$. A vertex with degree zero is called an *isolated vertex*. When all the vertices of $\mathbf{G}$ are isolated, $\mathbf{G}$ is called a *discrete graph*. A *complete graph* , denoted by $\mathcal{K}_n$, is a graph with n vertices in which every pair of vertices are adjacent vertices.

Let $\mathbf{G}$ be a graph. A graph $\mathbf{H}$ is called a *subgraph* of $\mathbf{G}$ if $V(\mathbf{H}) \subset V(\mathbf{G})$ and $E(\mathbf{H}) \subset E(\mathbf{G})$. A subgraph $\mathbf{H}$ of $\mathbf{G}$ is called a *subgraph induced* by $V(\mathbf{H})$, which is denoted by $\mathbf{G}[V(\mathbf{H})]$, or $\langle V(\mathbf{H}) \rangle$ or $\mathbf{G}_{V(\mathbf{H})}$, if $\mathbf{H}$ contains all the edges $\{\mathbf{x}, \mathbf{y}\} \in E(\mathbf{G})$ whenever $\mathbf{x}$ and $\mathbf{y}$ are elements of $V(\mathbf{H})$. A *spanning subgraph* is a subgraph $\mathbf{H}$ of $\mathbf{G}$ containing all the vertices of $\mathbf{G}$.

Definition 1.3.1 Let $\mathbf{G}$ be a graph. A *walk* of *length* r in $\mathbf{G}$ is an alternating sequence of vertices and edges

$$walk := \{\mathbf{x}_0, \mathbf{e}_1, \mathbf{x}_1, \ldots, \mathbf{e}_r, \mathbf{x}_r\},$$

where $\mathbf{e}_i := \{\mathbf{x}_{i-1}, \mathbf{x}_i\}$ is the edge joining the vertices $\mathbf{x}_{i-1}$ and $\mathbf{x}_i$. A *walk* may also be written $\{\mathbf{x}_0, \ldots, \mathbf{x}_r\}$ with the edges understood, or $\{\mathbf{e}_1, \ldots, \mathbf{e}_r\}$ with the vertices understood. If $\mathbf{x}_0 = \mathbf{x}_r$, the *walk* is called a *closed walk*. A *path* is a *walk* where all the vertices are different.

Definition 1.3.2 A *cycle* of *length* n, denoted by C_n, is a closed path $\{\mathbf{x}_0, \ldots, \mathbf{x}_n\}$ in which $n \geq 3$. A cycle is *even* (resp. *odd*) if its length is even (resp. odd). C_3 is called a *triangle*, C_4 a *square* and so on. A *forest* is an acyclic graph and a *tree* is a connected forest.

We say that a graph $\mathbf{G}$ is *connected* if for every pair of vertices $\mathbf{x}$ and $\mathbf{y}$ there is a path from $\mathbf{x}$ to $\mathbf{y}$. Notice that $\mathbf{G}$ has a vertex disjoint decomposition

$$\mathbf{G} = \mathbf{G}_1 \cup \mathbf{G}_2 \cup \cdots \cup \mathbf{G}_r, \qquad (**)$$

where $\mathbf{G}_1, \ldots, \mathbf{G}_r$ are the maximal (with respect to inclusion) connected subgraphs of $\mathbf{G}$. The $\mathbf{G}_i$'s in $**$ are called the *connected components* of $\mathbf{G}$. A connected component is called *even* (resp. *odd*) if its *order* (number of vertices) is even (resp. odd).

Let $\mathbf{G}$ be a graph. $\mathbf{G}$ is called *bipartite* if $V(\mathbf{G})$ can be partitioned into two disjoint subsets $\mathbf{V}_1$ and $\mathbf{V}_2$ such that every edge $\mathbf{xy}$ of $\mathbf{G}$ has the property that $\mathbf{x}$ is in $\mathbf{V}_1$ and $\mathbf{y}$ is in $\mathbf{V}_2$; the pair $(\mathbf{V}_1, \mathbf{V}_2)$ is called a *bipartition* of $\mathbf{G}$. If $\mathbf{G}$ is connected and bipartite, a bipartition of $\mathbf{G}$ is uniquely determined. The graph $\mathbf{G}$ is called a *complete bipartite graph* if $\mathbf{G}$ is bipartite and we have that $\mathbf{V}_1$ and $\mathbf{V}_2$ are completely joined, *i.e.* if $\mathbf{x}$ is in $\mathbf{V}_1$ and $\mathbf{y}$ is in $\mathbf{V}_2$ then $\mathbf{xy}$ is in $E(\mathbf{G})$; if $\mathbf{V}_1$ and $\mathbf{V}_2$ have m and n vertices respectively, we denote such a complete bipartite graph by $\mathcal{K}_{m,n}$. A *star* is a complete bipartite graph of the form $\mathcal{K}_{1,n}$.

Definition 1.3.3 The *distance* between two vertices $\mathbf{x}$ and $\mathbf{y}$ of a graph $\mathbf{G}$, denoted by $d(\mathbf{x}, \mathbf{y})$, is defined to be the minimum of the lengths of all possible paths from $\mathbf{x}$ to $\mathbf{y}$. If there is no path joining $\mathbf{x}$ and $\mathbf{y}$, then $d(\mathbf{x}, \mathbf{y}) := \infty$.

Proposition 1.3.4 [72, Theorem 4.7] *A graph* $\mathbf{G}$ *is bipartite if and only it contains no odd cycle.*

Let $\mathbf{G}$ and $\mathbf{H}$ be graphs. A mapping φ from $V(\mathbf{G})$ to $V(\mathbf{H})$ is called a *homomorphism* from the graph $\mathbf{G}$ to $\mathbf{H}$ if $\{\mathbf{x}, \mathbf{y}\} \in E(\mathbf{G})$ implies $\{\varphi(\mathbf{x}), \varphi(\mathbf{y})\} \in E(\mathbf{H})$ (so if $\{\mathbf{x}, \mathbf{y}\}$ is an edge then $\varphi(\mathbf{x}) \neq \varphi(\mathbf{y})$). Two graphs $\mathbf{G}$ and $\mathbf{H}$ are *isomorphic* if there is a bijective map ψ from $V(\mathbf{G})$ to $V(\mathbf{H})$ such that $\{\mathbf{x}, \mathbf{y}\} \in E(\mathbf{G})$ if and only if $\{\psi(\mathbf{x}), \psi(\mathbf{y})\} \in E(\mathbf{H})$; in this case ψ is called an *isomorphism* from $\mathbf{G}$ to $\mathbf{H}$. An isomorphism from $\mathbf{G}$ to itself is called an *automorphism*. A map taking graphs as arguments is called a *graph invariant* if it assigns equal values to isomorphic graphs. The number of vertices and the number of edges are two simple examples of graph invariants.

Note that by definition a graph does not contain a *loop*, a pair $\{\mathbf{x}, \mathbf{x}\}$ in the edge set ("an edge joining a vertex with itself"). Also a graph does not contain a pair $\{\mathbf{x}, \mathbf{y}\}$ that occurs several times in the edge set ("that is, several edges joining the same two vertices"). If we allow any of these type of relations at edges then $\mathbf{G}$ is called a *multigraph*. Most results on graphs carry over to multigraphs in a natural way. There are areas and notions in graph theory (such as plane duality and minors) where multigraphs arise more naturally than graphs. Terminology introduced earlier for graphs can be used correspondingly for multigraphs.

1.4 Polyhedral sets

In Subsection 2.6.1 we compute the degree of a family of lattice ideals. We make this computation in terms of the relative volume of a lattice polytope, for that reason there exists this section. The main references for polyhedral sets are [18, 69].

Definition 1.4.1 A point $\mathfrak{a} \in \mathbb{R}^n$ is called a *convex combination* of $\mathfrak{b}_1, \ldots, \mathfrak{b}_r \in \mathbb{R}^n$ if there are nonegative real numbers $\iota_1, \ldots, \iota_r$ such that

$$\mathfrak{a} = \iota_1 \mathfrak{b}_1 + \cdots + \iota_r \mathfrak{b}_r \qquad \text{and} \qquad \iota_1 + \cdots + \iota_r = 1.$$

Let $\mathfrak{B}$ be a subset of $\mathbb{R}^n$. The *convex hull* of $\mathfrak{B}$, denoted by $\mathrm{conv}(\mathfrak{B})$, is the set of all convex combinations of points of $\mathfrak{B}$. If $\mathfrak{B} = \mathrm{conv}(\mathfrak{B})$, we say that $\mathfrak{B}$ is a *convex set*.

Let $\mathcal{A} := \{a_1, \ldots, a_r\}$ be a finite subset of $\mathbb{Z}^n$. The convex hull of $\mathcal{A}, \mathcal{P} := \mathrm{conv}(\mathcal{A}) \subset \mathbb{R}^n$, is called a *lattice polytope*. The *dimension* of $\mathcal{P}$, denoted by $\dim(\mathcal{P})$, is equal to $\dim_{\mathbb{R}}(\mathbb{R}\mathcal{A}')$, the dimension as $\mathbb{R}$-vector space of $\mathbb{R}\mathcal{A}'$ (linear space spanned by $\mathcal{A}'$), where $\mathcal{A}' := \{0, a_2 - a_1, \ldots, a_r - a_1\}$. The *relative volume* of $\mathcal{P}$, denoted by $\mathrm{vol}(\mathcal{P})$, is given by

$$\mathrm{vol}(\mathcal{P}) := \lim_{i \to \infty} \frac{|\mathbb{Z}^n \cap i\mathcal{P}|}{i^d},$$

where $d := \dim(\mathcal{P}), i \in \mathbb{N}, i\mathcal{P} := \{ix \mid x \in \mathcal{P}\}$ and $|\cdot|$ denotes cardinality. When $d = n$, we recover the usual volume of $\mathcal{P}$ (see [83, p. 111] or [95, p. 238]).

Chapter 2

Lattice Ideals

Let K be a field and $S := K[t_1, \ldots, t_n]$ a polynomial ring with n variables over K. A *lattice* $\mathcal{L}_\rho$ is a subgroup of $\mathbb{Z}^n$ and a *partial character* ρ from $\mathcal{L}_\rho$ is a homomorphism from $\mathcal{L}_\rho$ to the multiplicative group $K^* := K \setminus \{0\}$.

We start this chapter introducing the lattice ideal $I(\rho)$; this is an ideal that depends of the lattice $\mathcal{L}_\rho$ and the partial character ρ. We prove that $I(\rho)$ contains no monomials. Then we give a characterization, an ideal I is a lattice ideal if and only if I is a binomial ideal, I contains no monomials and t_i is a non-zero divisor of S/I, for all $i = 1, \ldots, n$.

We show some relations between $\mathcal{L}_\rho$ and $I(\mathcal{L}_\rho)$. One of them is that $\mathcal{L}_\rho$ is generated by $a_1, \ldots, a_r$ if and only if $I(\mathcal{L}_\rho)$ is equal to the saturation of the ideal generated by the binomials $t^{a_1^+} - \rho(a_1)t^{a_1^-}, \ldots, t^{a_r^+} - \rho(a_r)t^{a_r^-}$ with respect to the monomial $t_1 \cdots t_n$. As another example, the height of $I(\rho)$ is the rank of $\mathcal{L}_\rho$.

By [16, Corollary 2.5] we know that a binomial ideal containing no monomials is characterized by a lattice. In some way we complement this result. If the field has characteristic different that 2, we show that a binomial ideal (without restrictions) can be characterized by a finite number of lattices. If the field has characteristic 2, we show that the binomial ideal depends of a lattice ideal and of a monomial ideal.

For a fixed but an arbitrary monomial order, the following main result of this chapter says that there are a finite number of elements $a_1, \ldots, a_r$ in the lattice $\mathcal{L}_\rho$ such that the binomials $t^{a_1^+} - \rho(a_1)t^{a_1^-}, \ldots, t^{a_r^+} - \rho(a_r)t^{a_r^-}$ form a Gröbner basis of $I(\rho)$. Then we adapt the Buchberger's algorithm to create a procedure that extends a set of generators of $\mathcal{L}_\rho$, $\{a_1, \ldots, a_r\}$, to a subset $\{a_1, \ldots, a_s\}$ of $\mathcal{L}_\rho$ such that $\left\{t^{a_1^+} - \rho(a_1)t^{a_1^-}, \ldots, t^{a_s^+} - \rho(a_s)t^{a_s^-}\right\}$ is a Gröbner basis of $I(\rho)$. As a very important application, we prove that a Gröbner basis, or more precisely the initial ideal of $I(\rho)$, is independent from ρ, and so are the Hilbert function, the Hilbert series, the Hilbert polynomial, the index of regularity, the a-invariant and the degree of $I(\rho)$.

We study an special case. We prove that if the lattice ideal $I(\rho)$ is standard-graded and has dimension 1, then the degree of this ideal is equal to $|T(\mathbb{Z}^n/\mathcal{L})|$. Let ω be a vector with positive integer entries. If $I(\rho)$ is ω-graded of dimension 1, we establish a complete intersection criterion in algebraic and geometric terms. If $I(\rho)$ is ω-graded of dimension 1, and K has positive characteristic, then we show that L is a pure binomial set theoretic complete intersection. If K has characteristic zero, we prove that in the set of pure lattice ideals the property binomial set theoretic complete intersection implies complete intersection. Let $v_1, \ldots, v_n$ be a sequence of vectors in $\mathbb{N}^s$ and $\mathcal{Q}$ the projective algebraic toric set parameterized by the vectors $v_1, \ldots, v_n$ on $\mathbb{P}^{n-1}$. We apply the results about graded pure lattice ideals of dimension 1 to the vanishing ideal $I(\mathcal{Q})$.

For the end of this chapter, let $v := \{v_1, \ldots, v_n\}$ be a sequence of positive integers and

$$\mathcal{T} := \{[(x_1^{v_1}, \ldots, x_n^{v_n})] \mid x_i \in K^* \text{ for all } i\} \subset \mathbb{P}^{n-1},$$

the projective degenerate torus of type v on $\mathbb{P}^{n-1}$. We study a complete intersection property, the index of regularity and the degree of the vanishing ideal of $\mathcal{T}$, $I(\mathcal{T})$. This ideal has very important consequences in mathematics, for instance in coding theory, as we will see in Chapters 3 and 4. We also give a way to compute the ideal $I(\mathcal{T})$ in terms of a saturation of an ideal with respect to the monomial $t_1 \cdots t_n$.

2.1 Identifying lattice ideals

Let K be a field and $S := K[t_1, \ldots, t_n]$ a polynomial ring with n variables over K. In this section we introduce the basic definitions about lattice ideals. Then we prove that a lattice ideal contains no monomials. Finally we show that an ideal I is a lattice ideal if and only if I is a binomial ideal, I contains no monomials and t_i is a non-zero divisor of S/I, for all $i = 1, \ldots, n$.

Definition 2.1.1 By a *binomial* in S we mean a polynomial with at most two terms, $\alpha t^a + \beta t^b$, where $\alpha, \beta \in K, a := (a_i), b \in \mathbb{N}^n$ and

$$t^a := t_1^{a_1} \cdots t_n^{a_n} \in S.$$

t^b is defined in a similar way. A *binomial ideal* is an ideal of S generated by binomials.

Definition 2.1.2 A binomial of the form $t^a - t^b$, with $a, b \in \mathbb{N}^n$, is called a *pure binomial.* An ideal generated by pure binomials is called a *pure binomial ideal.*

In the world of the mathematics there are at least two definitions of a lattice. For us a lattice is defined in the following way.

Definition 2.1.3 A subset $\mathcal{L} \subset \mathbb{Z}^n$ is a *lattice* if $\mathcal{L}$ is a subgroup of $\mathbb{Z}^n$. If $\mathcal{A}$ is a subset of $\mathbb{Z}^n$, $\mathbb{Z}\mathcal{A}$ denotes the lattice of $\mathbb{Z}^n$ generated by $\mathcal{A}$.

Definition 2.1.4 Concepts about partial characters.

(i) A *partial character* on $\mathbb{Z}^n$ is a homomorphism ρ from a lattice $\mathcal{L}_\rho$ of $\mathbb{Z}^n$ to the multiplicative group K^*.

(ii) Let ρ, ρ' be partial characters on $\mathbb{Z}^n$. We say ρ' is an *extension* of ρ if $\mathcal{L}_\rho \subset \mathcal{L}_{\rho'}$ and $\rho' \mid_{\mathcal{L}_\rho} = \rho$.

Whenever we speak about a partial character ρ, it is assumed that the domain of ρ is a lattice $\mathcal{L}_\rho \subset \mathbb{Z}^n$.

Definition 2.1.5 Given $c := (c_i) \in \mathbb{Z}^n$, we set $\operatorname{supp}(c) := \{i \mid c_i \neq 0\}$. The set $\operatorname{supp}(c)$ is called the *support* of c. The vector c can be uniquely written as $c = c^+ - c^-$, where c^+ (the *positive part* of c) and c^- (the *negative part* of c) are two nonnegative vectors with disjoint support. If t^a is a monomial, with $a := (a_i) \in \mathbb{N}^n$, we define the *support of the monomial* t^a as the set $\operatorname{supp}(t^a) := \{t_i \mid a_i > 0\}$. If $f := \alpha t^a + \beta t^b$ is a binomial, with $\alpha, \beta \in K^*$, we define the *support of the binomial* f as the set $\operatorname{supp}(f) := \operatorname{supp}(t^a) \cup \operatorname{supp}(t^b)$.

Definition 2.1.6 Given a partial character ρ, we define the *lattice ideal* of $\mathcal{L}_\rho$ as

$$I(\rho) := \left(\left\{t^{a^+} - \rho(a)t^{a^-} \mid a \in \mathcal{L}_\rho\right\}\right) \subset S.$$

In the case that ρ is a trivial partial character $\rho\colon \mathcal{L}_\rho \to K^*$, $a \to 1$, the lattice ideal $I(\rho)$ is denoted by $I(\mathcal{L})$, and is called a *pure lattice ideal.* The concept of lattice ideal is a natural generalization of a toric ideal [102, Corollary 7.1.4]. Lattice ideals have been studied extensively, see [16, 19, 91] and the references there.

The concept of congruence [15, 17, 81, 84, 102] is an useful tool for the study of lattices. We use this concept to compute a Gröbner basis of a lattice ideal.

Definition 2.1.7 A *congruence* in a commutative semigroup with identity $(\mathcal{S}, +)$ is an equivalence relation $\sim$ on $\mathcal{S}$ compatible with $+$, i.e., $a \sim b$ implies $a + c \sim b + c$.

Example 2.1.8 Let $\mathcal{L}$ be a lattice in $\mathbb{Z}^n$. If $a, b \in \mathbb{N}^n$, the relation $a \sim_{\mathcal{L}} b$ if and only if $a - b \in \mathcal{L}$ defines a congruence in $\mathbb{N}^n$. In this case we say that $\sim_{\mathcal{L}}$ is the *congruence determined* by $\mathcal{L}$.

Let $\sim$ be a congruence in $\mathbb{N}^n$. We say that two monomials t^a and t^b of S are *equivalent* under $\sim$ if $a \sim b$.

Definition 2.1.9 Let $\sim$ be a congruence in $\mathbb{N}^n$. A non-zero polynomial $f := \sum_a \lambda_a t^a$ in S is called *simple* with respect to $\sim$ if all its monomials, i.e., those t^a with non-zero coefficient λ_a, are pairwise equivalent under $\sim$.

Let $\sim$ be a congruence in $\mathbb{N}^n$. Given any polynomial $f \in S \setminus \{0\}$, we can group together its monomials by equivalence classes under $\sim$, thereby obtaining a decomposition

$$f = h_1 + \cdots + h_m,$$

with the property that each summand h_i is simple, and that no monomial in h_i is equivalent with a monomial in h_j if $j \neq i$. Such a decomposition of f as a sum of maximal simple subpolynomials is unique up to order. We will refer to the h_i's as the *simple components* of f respect to $\sim$.

The following notation is far to be nice, but it will be really needed for this chapter. We encourage to the reader to spend a pair of minutes in the next paragraph.

Definition 2.1.10 Let ρ be a partial character on $\mathbb{Z}^n, a, b_1, b_2$ elements of $\mathcal{L}_\rho$ and γ an element of $\mathbb{Z}^n$ such that $\gamma - b_2, \gamma - b_1 \in \mathbb{N}^n$. We define

$$\mathfrak{f}(a) := t^{a^+} - \rho(a)t^{a^-} \qquad \text{and} \qquad \mathfrak{g}(\gamma, b_1, b_2) := \rho(b_2)t^{\gamma - b_2} - \rho(b_1)t^{\gamma - b_1}.$$

Note that $\mathfrak{f}(a) = \mathfrak{g}(a^+, a, 0)$.

Lemma 2.1.11 *Let ρ be a partial character and let $\sim_{\mathcal{L}_\rho}$ be the congruence determined by $\mathcal{L}_\rho$. If $f \in I(\rho)$, then every simple component of f also belongs to $I(\rho)$.*

Proof. Each generator $\mathfrak{f}(a)$ of $I(\rho)$ is simple by definition, because $a^+ - a^- = a \in \mathcal{L}_\rho$. As f belongs to $I(\rho)$, f is of the form

$$f = f_1\mathfrak{f}(a_1) + \cdots + f_r\mathfrak{f}(a_r) = \sum_{i=1}^{r}\sum_{j} \lambda_{ij} t^{b_{ij}} \mathfrak{f}(a_i).$$

Every polynomial $t^{b_{ij}}\mathfrak{f}(a_i)$ is simple since the relation $\sim_{\mathcal{L}_\rho}$ is compatible with the sum. We group its monomials by equivalence classes under $\sim_{\mathcal{L}_\rho}$ and we get that every simple component h_i of f is a linear combination of some $t^{b_{ij}}\mathfrak{f}(a_i)$. Therefore every simple component h_i of f belongs to $I(\rho)$. $\square$

The previous result can be adapted to binomial ideals containing no monomials. Given a binomial $g := \alpha t^a - \beta t^b$, $\alpha, \beta \in K^*$, we set $\widehat{g} := a - b$. If $\beta = 0$, then we set $\widehat{g} := a$.

Lemma 2.1.12 *Let $I := (g_1, \ldots, g_r)$ be a binomial ideal of S such that g_i is no monomial. Then any simple component of $0 \neq f \in I$ with respect to $\sim_{\mathcal{G}}$ belongs to I, where $\mathcal{G} := \mathbb{Z}\{\widehat{g}_1, \ldots, \widehat{g}_r\}$.*

Proof. Each generator g_i of I is simple by definition. As f belongs to I, f is of the form

$$f = f_1 g_1 + \cdots + f_r g_r = \sum_{i=1}^{r}\sum_{j} \lambda_{ij} t^{a_{ij}} g_i.$$

Every polynomial $t^{a_{ij}}g_i$ is simple since the relation $\sim_{\mathcal{G}}$ is compatible with the sum. We group its monomials by equivalence classes under $\sim_{\mathcal{G}}$ and we get every simple component h_i of f is a linear combination of some $t^{a_{ij}}g_i$ and therefore every simple component belongs to I. $\square$

Definition 2.1.13 Let $(M, +)$ be an abelian group. The *torsion subgroup* of M, denoted by $T(M)$, is the set of all $x \in M$ such that $dx = 0$ for some $d \in \mathbb{N}_+$. The group M is *torsion free* if $T(M) = (0)$.

The following result tells when a pure lattice ideal is a toric ideal.

Theorem 2.1.14 [103, Theorem 8.2.22] *If $\mathcal{L}$ is a lattice of* rank r *in $\mathbb{Z}^n$, then the following conditions are equivalents.*

(a) *$I(\mathcal{L})$ is a toric ideal.*

(b) *$I(\mathcal{L})$ is a prime ideal.*

(c) *$\mathbb{Z}^n/\mathcal{L}$ is torsion-free.*

(d) *$\mathcal{L} = \ker_{\mathbb{Z}}(A)$ for some integral matrix A.*

For the rest of this section, let $\prec$ be an arbitrary monomial order fixed on S, $\mathcal{L}_\rho \subset \mathbb{Z}^n$ a lattice and $\rho : \mathcal{L}_\rho \to K^*$ a partial character. We denote the S-polynomial (Definition 1.1.17 (ii)) of f and g by $\mathrm{S}(f, g)$, and we write

$$\overline{f}^{\mathcal{F}}$$

for the remainder on division of f by the ordered r-tuple $\mathcal{F} := \{f_1, \ldots, f_r\} \subset S$.

Remark 2.1.15 If $\mathfrak{g}(\gamma, b_1, b_2)$ is a monomial, then it is the zero polynomial, because $\gamma - b_2 = \gamma - b_1$ implies $b_1 = b_2$ and $\mathfrak{g}(\gamma, b_1, b_2) = \mathfrak{g}(\gamma, b_1, b_1) = 0$.

Lemma 2.1.16 *If a_1, a_2 are elements of $\mathbb{Z}^n$, then there are γ, b_1, b_2 in $\mathbb{Z}^n$ with $\gamma - b_1, \gamma - b_2 \in \mathbb{N}^n$ such that*

$$S(f(a_1), f(a_2)) = g(\gamma, b_1, b_2).$$

Proof.

(i) If $a_1^+ \succ a_1^-$ and $a_2^+ \succ a_2^-$ then $\gamma := LCM(a_1^+, a_2^+)$ and $b_i := a_i, i = 1, 2$.

(ii) If $a_1^+ \prec a_1^-$ and $a_2^+ \prec a_2^-$ then $\gamma := LCM(a_1^-, a_2^-), b_1 := -a_2$ and $b_2 := -a_1$.

(iii) If $a_1^+ \succ a_1^-$ and $a_2^+ \prec a_2^-$ then $\gamma := LCM(a_1^+, a_2^-), b_1 := a_1$ and $b_2 := -a_2$.

(iv) If $a_1^+ \prec a_1^-$ and $a_2^+ \succ a_2^-$ then $\gamma := LCM(a_1^-, a_2^+), b_1 := a_2$ and $b_2 := -a_1$. $\square$

Lemma 2.1.17 *If a_1, a_2, a_3, γ_1 are elements of $\mathbb{Z}^n$ such that $\gamma_1 - a_2, \gamma_1 - a_3 \in \mathbb{N}^n$, then there are γ, b_1, b_2 in $\mathbb{Z}^n$ with $\gamma - b_1, \gamma - b_2 \in \mathbb{N}^n$ such that*

$$S(f(a_1), g(\gamma_1, a_2, a_3)) = g(\gamma, b_1, b_2).$$

Proof.

(i) If $a_1^+ \succ a_1^-$ and $\gamma_1 - a_2 \succ \gamma_1 - a_3$ then $\gamma := LCM(a_1^+, \gamma_1 - a_2), b_1 := a_1$ and $b_2 := a_3 - a_2$.

(ii) If $a_1^+ \succ a_1^-$ and $\gamma_1 - a_3 \succ \gamma_1 - a_2$ then $\gamma := LCM(a_1^+, \gamma_1 - a_3), b_1 := a_1$ and $b_2 := a_2 - a_3$.
Other cases are similar. □

Lemma 2.1.18 *Let a_1, a_2, a_3, a_4 be elements of $\mathcal{L}_\rho$ and γ_1, γ_2 elements of $\mathbb{Z}^n$ such that $\gamma_1 - a_1, \gamma_1 - a_2, \gamma_2 - a_3, \gamma_2 - a_4 \in \mathbb{N}^n$, then there are b_1, b_2 in $\mathcal{L}_\rho$ and γ in $\mathbb{Z}^n$ with $\gamma - b_1, \gamma - b_2 \in \mathbb{N}^n$ such that*

$$S(\mathfrak{g}(\gamma_1, a_1, a_2), \mathfrak{g}(\gamma_2, a_3, a_4)) = \mathfrak{g}(\gamma, b_1, b_2).$$

Proof. If $\gamma_1 - a_1 \succ \gamma_1 - a_2$ and $\gamma_2 - a_3 \succ \gamma_2 - a_4$ then $\gamma := LCM(\gamma_1 - a_1, \gamma_2 - a_3), b_1 := a_2 - a_1$ and $b_2 := a_4 - a_3$. Other cases are similar. □

Lemma 2.1.19 *The remainder after dividing $\mathfrak{g}(\gamma_1, a_1, a_2)$ by $\mathfrak{g}(\gamma_2, a_3, a_4)$ is of the form $\mathfrak{g}(\gamma_1, b_1, b_2)$.*

Proof. Assume $\gamma_1 - a_2 \succ \gamma_1 - a_1$ and $\gamma_2 - a_4 \succ \gamma_2 - a_3$. If $t^{\gamma_2 - a_4} \mid t^{\gamma_1 - a_2}$ then $b_2 := a_2 + a_3 - a_4$ and $b_1 := a_1$, otherwise $b_1 := a_1$ and $b_2 := a_2$. □

Proposition 2.1.20 *Let $\prec$ be an arbitrary monomial order on S. There is a Gröbner basis of $I(\rho)$ of the form*

$$\mathcal{G} := \left\{ \mathfrak{f}(a_1), \ldots, \mathfrak{f}(a_r), \mathfrak{g}(\gamma_{r+1}, b'_{r+1}, b_{r+1}), \ldots, \mathfrak{g}(\gamma_s, b'_s, b_s) \right\}.$$

Proof. S noetherian implies there are $a_1, \ldots, a_r$ elements of $\mathcal{L}_\rho$ such that

$$I(\rho) = (\mathfrak{f}(a_1), \ldots, \mathfrak{f}(a_r)).$$

By Lemmas 2.1.18 and 2.1.19 we have that the output in every step of the Buchberger's Algorithm (Proposition1.1.19) is of the form $\mathfrak{g}(\gamma, b_1, b_2)$. □

We come to one of the main results of this section.

Theorem 2.1.21 *Let K be a field and $\rho : \mathcal{L}_\rho \to K^*$ a partial character. The lattice ideal $I(\rho) = \left(\left\{ t^{a^+} - \rho(a) t^{a^-} \mid a \in \mathcal{L} \right\}\right)$ contains no monomials.*

Proof. By Proposition 2.1.20 there is a Gröbner basis $\mathcal{G}$ of $I(\rho)$ which consists of elements of the form $\mathfrak{f}(a_i)$ and $\mathfrak{g}(\gamma_j, b'_j, b_j)$. By Remark 2.1.15 $\mathcal{G}$ contains no monomials. Let t^a be a monomial of S. By Proposition 1.1.16 t^a belongs to $I(\rho)$ if and only if $\overline{t^a}^{\mathcal{G}} = 0$.

If $t^{a_i^+}$ divides t^a, then, by division algorithm,

$$t^a = t^{a-a_i^+}\mathfrak{f}(a_i) + \underbrace{\rho(a_i)t^{a-a_i}}_{remainder}. \qquad (*)$$

If $t^{\gamma_j - b_j}$ divides t^a, then, by division algorithm,

$$t^a = \frac{1}{\rho(b_j)} t^{a-\gamma_j+b_j}\mathfrak{g}(\gamma_j, b_j', b_j) + \underbrace{\rho(b_j' - b_j)t^{a-b_j'+b_j}}_{remainder}. \qquad (**)$$

In both cases the remainder is a non-zero term. If the remainder in Eq. $(*)$ is zero, the left-hand side of this equation is a monomial, but its right-hand side is a binomial, a contradiction. The same situation happens in Eq. $(**)$. Thus $\overline{t^a}^{\mathcal{G}} \neq 0$ and t^a, an arbitrary monomial of S, is not an element of $I(\rho)$. □

Theorem 2.1.22 *$t_i \notin \mathcal{Z}(S/I(\rho))$ for all i.*

Proof. By definition it suffices to show that if $t_i f \in I(\rho)$, with $i = 1, \ldots, n$, then $f \in I(\rho)$. By Lemma 2.1.11 we can assume $t_i f$ is simple and $f = \sum_{j=1}^r \lambda_j t^{a_j}$. By induction on r. Case $r = 1$ is not possible because $I(\rho)$ contains no monomials.

Case $r = 2$ $(\lambda_1, \lambda_2 \neq 0)$: $t_i f = \lambda_1 t_i t^{a_1} + \lambda_2 t_i t^{a_2} = \lambda_1 t_i t^{c_1}\left(t^{b_1^+} + \lambda t^{b_1^-}\right) \in I(\rho)$. As $b_1^+ - b_1^- = a_1 - a_2 \in \mathcal{L}$ then $\lambda_1 t_i t^{c_1}\mathfrak{f}(b_1) \in I(\rho)$. Thus $t_i f - \lambda_1 t_i t^{c_1}\mathfrak{f}(b_1) = \lambda_1 t_i t^{c_1}\left(t^{b_1^+} + \lambda t^{b_1^-}\right) - \lambda_1 t_i t^{c_1}\mathfrak{f}(b_1) = (\lambda + \rho(b_1))\lambda_1 t_i t^{c_1 + b_1^-} \in I(\rho)$. By Theorem 2.1.21 $\lambda = -\rho(b_1)$. Therefore $t_i f = \lambda_1 t_i t^{c_1}\mathfrak{f}(b_1)$ and $f = \lambda_1 t^{c_1}\mathfrak{f}(b_1) \in I(\rho)$.

Case $r = 3$ $(\lambda_1, \lambda_2, \lambda_3 \neq 0)$: $t_i f = \lambda_1 t_i t^{a_1} + \lambda_2 t_i t^{a_2} + \lambda_3 t_i t^{a_3} = \lambda_1 t_i t^{c_1}\left(t^{b_1^+} + \lambda t^{b_1^-}\right) + \lambda_3 t_i t^{a_3} \in I(\rho)$. As $b_1^+ - b_1^- = a_1 - a_2 \in \mathcal{L}$ then $\lambda_1 t_i t^{c_1}\mathfrak{f}(b_1) \in I(\rho)$. Thus

$$\begin{aligned} t_i\left(f - \lambda_1 t^{c_1}\mathfrak{f}(b_1)\right) &= t_i f - \lambda_1 t_i t^{c_1}\mathfrak{f}(b_1) \\ &= \lambda_1 t_i t^{c_1}\left(t^{b_1^+} + \lambda t^{b_1^-}\right) - \lambda_1 t_i t^{c_1}\mathfrak{f}(b_1) + \lambda_3 t_i t^{a_3} \\ &= (\lambda + \rho(b_1))\lambda_1 t_i t^{c_1 + b_1^-} + \lambda_3 t_i t^{a_3} \\ &= t_i\left((\lambda + \rho(b_1))\lambda_1 t^{c_1 + b_1^-} + \lambda_3 t^{a_3}\right). \end{aligned} \qquad (2.1.1)$$

Equation $c_1 + b_1^- = a_2$ implies Eq. (2.1.1) is a simple component. By $r = 2$, we have $f - \lambda_1 t^{c_1}\mathfrak{f}(b_1) = (\lambda + \rho(b_1))\lambda_1 t^{c_1 + b_1^-} + \lambda_3 t^{a_3}$ is an element of $I(\rho)$. Therefore $f \in I(\rho)$.

Case $r = n$ $(\lambda_1, \ldots, \lambda_n \neq 0)$: $t_i f = \lambda_1 t_i t^{a_1} + \lambda_2 t_i t^{a_2} + \sum_{j=3}^{n} \lambda_j t_i t^{a_j} = \lambda_1 t_i t^{c_1}\left(t^{b_1^+} + \lambda t^{b_1^-}\right) + \sum_{j=3}^{n} \lambda_j t_i t^{a_j} \in I(\rho)$. As $b_1^+ - b_1^- = a_1 - a_2 \in \mathcal{L}$ then $\lambda_1 t_i t^{c_1}\mathfrak{f}(b_1) \in I(\rho)$. Thus

$$\begin{aligned} t_i\left(f - \lambda_1 t^{c_1}\mathfrak{f}(b_1)\right) &= t_i f - \lambda_1 t_i t^{c_1}\mathfrak{f}(b_1) \\ &= \lambda_1 t_i t^{c_1}\left(t^{b_1^+} + \lambda t^{b_1^-}\right) - \lambda_1 t_i t^{c_1}\mathfrak{f}(b_1) + \sum_{j=3}^{n} \lambda_j t_i t^{a_j} \\ &= \left(\lambda + \rho(b_1)\right)\lambda_1 t_i t^{c_1 + b_1^-} + \sum_{j=3}^{n} \lambda_j t_i t^{a_j} \in I(\rho) \\ &= t_i\left(\left(\lambda + \rho(b_1)\right)\lambda_1 t^{c_1 + b_1^-} + \sum_{j=3}^{n} \lambda_j t^{a_j}\right). \end{aligned} \tag{2.1.2}$$

Equation $c_1 + b_1^- = a_2$ implies Eq. (2.1.2) is a simple component. By case $r = n-1$ we get $f - \lambda_1 t^{c_1}\mathfrak{f}(b_1) = \left(\lambda + \rho(b_1)\right)\lambda_1 t^{c_1 + b_1^-} + \sum_{j=3}^{n} \lambda_j t^{a_j}$ is an element of $I(\rho)$. We conclude that f is an element of $I(\rho)$. □

The previous result presents a base to obtain in the following Theorem a characterization of a lattice ideal in terms of zero divisors.

Theorem 2.1.23 *An ideal $I \subset S$ is a lattice ideal if and only if*

(i) *I is binomial,*

(ii) *I contains no monomials and*

(iii) *$t_i \notin \mathcal{Z}(S/I)$ for all i.*

Proof. ($\Rightarrow$) (i) It follows by definition. (ii) It follows by Theorem 2.1.21. (iii) It follows by Theorem 2.1.22.

($\Leftarrow$) Using (i), (ii) and [16, Corollary 2.5] there is a unique partial character ρ on $\mathcal{L}_\rho \subset \mathbb{Z}^n$ such that $I : (t_1 \cdots t_n)^\infty = I(\rho)$. By (iii) we have $I = I(\rho)$. □

The last theorem is a well-known description of pure lattice ideals that follows from [16, Corollary 2.5]. We have extended the result for an arbitrary lattice ideal.

2.2 Relation between a lattice and its lattice ideal

Let K be a field, $S := K[t_1, \ldots, t_n]$ a polynomial ring with n variables over K, $\mathcal{L}_\rho \subset \mathbb{Z}^n$ a lattice and ρ a partial character from $\mathcal{L}_\rho$. In this section we show some relations between the lattice $\mathcal{L}_\rho$ and its lattice ideal $I(\mathcal{L}_\rho)$. One of the most important properties says that the lattice $\mathcal{L}_\rho$ is generated by the elements $a_1, \ldots, a_r$ if and only if its lattice ideal $I(\mathcal{L}_\rho)$ is equal to the saturation of the ideal generated by the binomials $t^{a_1^+} - \rho(a_1)t^{a_1^-}, \ldots, t^{a_r^+} - \rho(a_r)t^{a_r^-}$ with respect to the monomial $t_1 \cdots t_n$. Other relation is that the height of $I(\rho)$ is the rank of $\mathcal{L}_\rho$.

Lemma 2.2.1 *If $z \in \mathbb{Z}$ and $a \in \mathcal{L}_\rho$ then $\mathfrak{f}(za) \in (\mathfrak{f}(a))$.*

Proof. We just need to prove it for $z > 0$ because $\mathfrak{f}(-za) = \frac{-1}{\rho(za)}\mathfrak{f}(za)$ gives us the negative case. Now we use induction over $z > 0$. $z = 1$ is clear. Assume the result is true for z. We have $\mathfrak{f}((z+1)a) = \mathfrak{f}(za)\mathfrak{f}(a) + \rho(za)t^{za^-}\mathfrak{f}(a) + \rho(a)t^{a^-}\mathfrak{f}(za)$ and the Lemma is true. □

Lemma 2.2.2 *If $z_1, \ldots, z_r \in \mathbb{Z}$ and $a_1, \ldots, a_r \in \mathcal{L}_\rho$ then*

$$(\mathfrak{f}(z_1a_1), \ldots, \mathfrak{f}(z_ra_r)) : (t_1 \cdots t_n)^\infty \subset (\mathfrak{f}(a_1), \ldots, \mathfrak{f}(a_r)) : (t_1 \cdots t_n)^\infty.$$

Proof. This is a consequence of Definition 1.1.36 and Lemma 2.2.1.

Lemma 2.2.3 *If $a_1, \ldots, a_r \in \mathcal{L}_\rho$ then $\mathfrak{f}(a_1 + \cdots + a_r) \in (\mathfrak{f}(a_1), \ldots, \mathfrak{f}(a_r)) : (t_1 \cdots t_n)^\infty$.*

Proof. By induction on r.

Case $r = 1$: This is Lemma 2.2.1.

Case $r = 2$: We have $a_1 + a_2 = a_1^+ - a_1^- + a_2^+ - a_2^- = \left(a_1^+ + a_2^+\right) - \left(a_1^- + a_2^-\right)$. Thus there is $b \in \mathbb{N}^n$ such that $(a_1 + a_2)^+ = a_1^+ + a_2^+ - b$ and $(a_1 + a_2)^- = a_1^- + a_2^- - b$. These equations imply $\mathfrak{f}(a_1)\mathfrak{f}(a_2) + \rho(a_1)t^{a_1^-}\mathfrak{f}(a_2) + \rho(a_2)t^{a_2^-}\mathfrak{f}(a_1) = t^{a_1^+ + a_2^+} - \rho(a_1 + a_2)t^{a_1^- + a_o n^-} = t^b\left(t^{(a_1+a_2)^+} - \rho(a_1 + a_2)t^{(a_1+a_2)^-}\right) = t^b\mathfrak{f}(a_1 + a_2)$.

Case $r = n$: By case $r = n - 1$, $\mathfrak{f}(a_1 + \cdots + a_r) \in (\mathfrak{f}(a_1 + a_2), \mathfrak{f}(a_3), \ldots, \mathfrak{f}(a_r) : (t_1 \cdots t_n)^\infty)$, then there is $b_1 \in \mathbb{N}^n$ such that

$$\mathfrak{f}(a_1 + \cdots + a_r)t^{b_1} = g\mathfrak{f}(a_1 + a_2) + g_3\mathfrak{f}(a_3) + \cdots + g_r\mathfrak{f}(a_r). \qquad (*)$$

By case $r = 2$ there is $b_2 \in \mathbb{N}^n$ such that

$$\mathfrak{f}(a_1 + a_2)t^{b_2} = g_1\mathfrak{f}(a_1) + g_2\mathfrak{f}(a_2). \qquad (**)$$

By Eqs. $(*)$ and $(**)$ we have $\mathfrak{f}(a_1 + \cdots + a_r)t^{b_1+b_2} = gg_1\mathfrak{f}(a_1) + gg_2\mathfrak{f}(a_2) + g_3t^{b_2}\mathfrak{f}(a_3) + \cdots + g_rt^{b_2}\mathfrak{f}(a_r)$. □

Proposition 2.2.4 *If $a \in \mathcal{L}_\rho := \mathbb{Z}\{a_1, \ldots, a_r\}$, then*

$$\mathfrak{f}(a) \in \left(t^{a_1^+} - \rho(a_1)t^{a_1^-}, \ldots, t^{a_r^+} - \rho(a_r)t^{a_r^-}\right) : (t_1 \cdots t_n)^\infty.$$

Proof. Assume $a = z_1a_1 + \cdots + z_ra_z$. It suffices to notice that by Lemma 2.2.3 $\mathfrak{f}(a) \in (\mathfrak{f}(z_1a_1), \ldots, \mathfrak{f}(z_ra_r)) : (t_1 \cdots t_n)^\infty$, and that by Lemma 2.2.2
$(\mathfrak{f}(z_1a_1), \ldots, \mathfrak{f}(z_ra_r)) : (t_1 \cdots t_n)^\infty \subset (\mathfrak{f}(a_1), \ldots, \mathfrak{f}(a_r)) : (t_1 \cdots t_n)^\infty$. □

Lemma 2.2.5 *If $a, b \in \mathbb{N}^n$ and $a - b \in \mathcal{L}_\rho := \mathbb{Z}\{a_1, \ldots, a_r\}$, then there is $t^\delta \in S$ such that*

$$t^\delta\left(t^a - \rho(a - b)t^b\right) \in \left(t^{a_1^+} - \rho(a_1)t^{a_1^-}, \ldots, t^{a_r^+} - \rho(a_r)t^{a_r^-}\right).$$

Proof. By Proposition 2.2.4 there is $\delta^* \in \mathbb{N}^n$ such that

$$t^{\delta^*}\mathfrak{f}(a-b) \in I := \left(t^{a_1^+} - \rho(a_1)t^{a_1^-}, \ldots, t^{a_r^+} - \rho(a_r)t^{a_r^-}\right).$$

As $[(a-b)^+]_i = \begin{cases} a_i - b_i & \text{if } \ a_i \geq b_i, \\ 0 & \text{if } \ a_i < b_i, \end{cases}$ then $a - (a-b)^+ = b - (a-b)^- \in \mathbb{N}^n$, and we have $t^{\delta^*}\left(t^a - \rho(a-b)t^b\right) = t^{\delta}\mathfrak{f}(a-b) \in I$, where $\delta = \delta^* + a - (a-b)^+$. $\square$

Proposition 2.2.6 *$t^a - \lambda t^b \in I(\rho)$ if and only if $a - b \in \mathcal{L}_\rho$ and $\lambda = \rho(a-b)$.*

Proof. ($\Rightarrow$) By Theorem 2.1.21 $I(\rho)$ contains no monomials, so $t^a - \lambda t^b$ is simple with respect to $\sim_{\mathcal{L}_\rho}$ and $a - b \in \mathcal{L}_\rho$. We have $t^a - \lambda t^b = t^c\left(t^{\gamma^+} - \lambda t^{\gamma^-}\right) \in I(\rho)$ and $t^c\left(t^{\gamma^+} - \rho\left(\gamma\right)t^{\gamma^-}\right) \in I(\rho)$. So

$$t^c\left(t^{\gamma^+} - \lambda t^{\gamma^-}\right) - t^c\left(t^{\gamma^+} - \rho\left(\gamma\right)t^{\gamma^-}\right) = t^c t^{\gamma^-}\left(\rho\left(\gamma\right) - \lambda\right) \in I(\rho)$$

and $\lambda = \rho\left(\gamma\right) = \rho\left(c + \gamma^+ - c - \gamma^-\right) = \rho\left(a-b\right)$ because $I(\rho)$ contains no monomials by Theorem 2.1.21.

($\Leftarrow$) By Lemma 2.2.5 there is $t^\delta \in S$ such that $t^\delta\left(t^a - \rho\left(a-b\right)t^b\right) \in I(\rho)$. By Theorem 2.1.23 (ii) we can omit t^δ. $\square$

We come to one of the main results of this section.

Theorem 2.2.7 *$\mathcal{L}_\rho = \mathbb{Z}\left\{a_1, \ldots, a_r\right\}$ if and only if*

$$I(\rho) = \left(t^{a_1^+} - \rho(a_1)t^{a_1^-}, \ldots, t^{a_r^+} - \rho(a_r)t^{a_r^-}\right) : (t_1 \cdots t_n)^\infty.$$

Proof. ($\Rightarrow$) ($\supseteq$) It is clear. ($\subseteq$) If $\mathfrak{f}(a) \in I(\rho)$, then $a \in \mathcal{L}_\rho$ because $\mathfrak{f}(a)$ is simple with respect to $\sim_{\mathcal{L}_\rho}$, and by Proposition 2.2.4

$$\mathfrak{f}(a) \in \left(t^{a_1^+} - \rho(a_1)t^{a_1^-}, \ldots, t^{a_r^+} - \rho(a_r)t^{a_r^-}\right) : (t_1 \cdots t_n)^\infty.$$

($\Leftarrow$) ($\supseteq$) For $i = 1, \ldots, r$ we have

$$\mathfrak{f}(a_i) \in \left(t^{a_1^+} - \rho(a_1)t^{a_1^-}, \ldots, t^{a_r^+} - \rho(a_r)t^{a_r^-}\right) : (t_1 \cdots t_n)^\infty = I(\rho).$$

As $I(\rho)$ contains no monomials (Theorem 2.1.21), $\mathfrak{f}(a_i)$ is simple with respect to $\sim_{\mathcal{L}_\rho}$ and $a_i \in \mathcal{L}_\rho$. Thus $\mathbb{Z}\left\{a_1, \ldots, a_r\right\} \subset \mathcal{L}_\rho$. ($\subseteq$) Let $\mathcal{L}' = \mathbb{Z}\left\{a_1, \ldots, a_r\right\} \subset \mathcal{L}_\rho$ and $\rho' = \rho|_{\mathcal{L}'}$. If $a \in \mathcal{L}_\rho$,

$$\mathfrak{f}(a) \in I(\rho) = \left(t^{a_1^+} - \rho(a_1)t^{a_1^-}, \ldots, t^{a_r^+} - \rho(a_r)t^{a_r^-}\right) : (t_1 \cdots t_n)^\infty,$$

then there is $\delta \in \mathbb{N}^n$ such that $t^\delta\mathfrak{f}(a) \in \left(t^{a_1^+} - \rho(a_1)t^{a_1^-}, \ldots, t^{a_r^+} - \rho(a_r)t^{a_r^-}\right) \subset I(\rho')$. As $t_i \notin \mathcal{Z}(S/I(\rho'))$ for all i (Theorem 2.1.23 (iii)), $\mathfrak{f}(a) \in I(\rho')$ and it is simple (with respect to $\sim_{\mathcal{L}'}$). Thus $a \in \mathcal{L}'$ and $\mathcal{L}_\rho \subset \mathbb{Z}\left\{a_1, \ldots, a_r\right\}$. The proof is complete. $\square$

Remark 2.2.8 Let $\succ_{lex}$ be the lex order on $S[t_0]$ (and on $\mathbb{Z}^{n+1}$) with $t_0 \succ_{lex} \cdots \succ_{lex} t_n$, where t_0 is a new indeterminate. Following the notation of Theorem 2.2.7 we know that

$$I(\rho) = \left(t^{a_1^+} - \rho(a_1)t^{a_1^-}, \ldots, t^{a_r^+} - \rho(a_r)t^{a_r^-}\right) : (t_1 \cdots t_n)^\infty ,$$

and by [103, Proposition 3.3.23]

$$I(\rho) = \underbrace{\left(t^{a_1^+} - \rho(a_1)t^{a_1^-}, \ldots, t^{a_r^+} - \rho(a_r)t^{a_r^-}, t_0t_1 \cdots t_n - 1\right)}_{J} \bigcap S.$$

By [75, Theorem 2, pag 116], if $\mathcal{G}_J$ is a Gröbner basis of J with respect to $\succ_{lex}$, then

$$\mathcal{G} := \{f \in G_j \mid t_0 \text{ does not appear in } f\}$$

is a Gröbner basis of $I(\rho)$.

A lattice ideal is defined by a unique lattice and by a unique partial character.

Theorem 2.2.9 *Let ρ be a partial character on a lattice $\mathcal{L}_\rho$and let $I(\rho)$ be its lattice ideal. If $I(\rho) = \left(t^{a_1} - \lambda_1 t^{b_1}, \ldots, t^{a_r} - \lambda_r t^{b_r}\right)$, then $\mathcal{L}_\rho = \mathbb{Z}\{a_1 - b_1, \ldots, a_r - b_r\}$ and $\rho(a_i - b_i) = \lambda_i$, for $i = 1, \ldots, r$. In particular, if L is a lattice ideal, there are a unique lattice $\mathcal{L}_\rho$ and a unique partial character ρ on the lattice $\mathcal{L}_\rho$ such that $L = I(\rho)$.*

Proof. Consider the lattice $\mathcal{G} := \mathbb{Z}\{a_1 - b_1, \ldots, a_r - b_r\}$. First we show the inclusion $\mathcal{L} \subset \mathcal{G}$. Take $0 \neq a \in \mathcal{L}$. We can write $a = a^+ - a^-$. Then $f(a) = t^{a^+} - \rho(a)t^{a^-}$ belongs to $I(\rho) = \left(t^{a_1} - \lambda_1 t^{b_1}, \ldots, t^{a_r} - \lambda_r t^{b_r}\right)$ by Proposition 2.2.6. By Lemma 2.1.12, any simple component of $f(a)$ with respect to $\sim_\mathcal{G}$ is also in $\left(t^{a_1} - \lambda_1 t^{b_1}, \ldots, t^{a_r} - \lambda_r t^{b_r}\right)$. Since t^{a^+} and t^{a^-} are not in $I(\mathcal{L})$ (Theorem 2.1.21), then $f(a)$ is a simple component of $f(a)$ with respect to $\sim_\mathcal{G}$, i.e., $a = a^+ - a^- \in \mathcal{G}$. Thus, $\mathcal{L} \subset \mathcal{G}$. To show the other inclusion notice that a binomial $t^a - \lambda t^b$ is in $I(\rho)$ if and only if $a - b \in \mathcal{L}$ and $\lambda = \rho(a - b)$. This is Proposition 2.2.6. Hence, $a_i - b_i \in \mathcal{L}$ for all i, i.e., $\mathcal{G} \subset \mathcal{L}$ and $\lambda_i = \rho(a_i - b_i)$. □

Proposition 2.2.10 [91, Proposition 7.5] *The height of $I(\rho)$ is the rank of $\mathcal{L}_\rho$.*

Theorem 2.2.11 [46, Theorem 3.2] *Let $I(\mathcal{L})$ be a pure lattice ideal of S over an arbitrary field K of characteristic p, let c be the number of associated primes of $I(\mathcal{L})$, and for $p > 0$, let G be the unique largest subgroup of $T(\mathbb{Z}^n/\mathcal{L})$ whose order is relatively prime to p. Then*

(a) *All associated primes of $I(\mathcal{L})$ have height equal to* $\mathrm{rank}(\mathcal{L})$.

(b) $|T(\mathbb{Z}^n/\mathcal{L})| \geq c$ *if $p = 0$ and $|G| \geq c$ if $p > 0$, with equality if K is algebraically closed.*

(c) $\deg(S/I(\mathcal{L})) \geq |T(\mathbb{Z}^n/\mathcal{L})|$ *if $p = 0$ and* $\deg(S/I(\mathcal{L})) \geq |G|$ *if $p > 0$.*

Proposition 2.2.12 *Let $I = I(\mathcal{L}) \subset S$ be a standard graded pure lattice ideal. If the initial ideal $LT(I)$ is square-free, then I is a prime ideal and S/I is normal and Cohen-Macaulay.*

Proof. By Theorem 2.2.11 and Proposition 1.1.37 all associated prime ideals of I have height $r = \mathrm{rank}(\mathcal{L})$ and I is a radical ideal. Then I has an irredundant primary decomposition $I = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_m$, where $\mathfrak{p}_i$ is a prime ideal of height r for all i. Let $\mathcal{L}_s = \mathrm{Sat}(\mathcal{L})$ be the saturation of $\mathcal{L}$ consisting of all $a \in \mathbb{Z}^n$ such that $pa \in \mathcal{L}$ for some $0 \neq p \in \mathbb{N}$ and let $I(\mathcal{L}_s)$ be its lattice ideal. Since $\mathrm{rank}(\mathcal{L})$ is equal to $\mathrm{rank}(\mathcal{L}_s)$, by Theorem 2.2.10, we get that r is also the height of $I(\mathcal{L}_s)$. As $\mathbb{Z}^n/\mathcal{L}_s$ is torsion-free, by Theorem 2.1.14, $I(\mathcal{L}_s)$ is a prime toric ideal. Then we may assume that $\mathfrak{p}_1 = I(\mathcal{L}_s)$. We claim that $LT(I) = LT(I(\mathcal{L}_s))$. Clearly $LT(I) \subset LT(I(\mathcal{L}_s))$ because $I \subset I(\mathcal{L}_s)$. To show the reverse inclusion take any element f in the reduced Gröbner basis of $I(\mathcal{L}_s)$. It suffices to show that $LT(f) \in LT(I)$. By Lemma 1.1.45, we can write $f = t^{a^+} - t^{a^-}$ for some $a = a^+ - a^-$ in $\mathcal{L}_s$. We may assume that $LT(f) = t^{a^+}$. There is $p \in \mathbb{N}_+$ such that $pa \in \mathcal{L}$. The binomial $g = t^{pa^+} - t^{pa^-}$ is in $I = I(\mathcal{L})$ and $LT(g) = t^{pa^+}$. Thus $t^{pa^+} \in LT(I)$ and since this ideal is square-free we get that $t^{a^+} \in LT(I)$. This proves the claim. Hence $\deg(S/I)$ is $\deg(S/I(\mathcal{L}_s))$ because S/I and $S/I(\mathcal{L}_s)$ have the same Hilbert function. Therefore, by additivity of the degree, we get that $m = 1$. Consequently, by Theorems 1.1.49 and 1.1.49, S/I is normal and Cohen-Macaulay. □

The primary decomposition of a lattice ideal depends from the partial character ρ.

Example 2.2.13 Using Singular [65] with $K := \mathbb{R}$ and $\prec_{dp}$ we have

$$\left(t_1t_3 - 1, t_1t_2^2 - t_3, t_3^2 - t_2\right) = (t_3 - 1, t_2 - 1, t_1 - t_3) \cap (t_3 + 1, t_2 - 1, t_1 - t_3)$$
$$\left(t_1t_3 - 2, t_1t_2^2 - 3t_3, t_3^2 - 4t_2\right) = \left(t_3^2 - 24, t_2 - 6, 12t_1 - t_3\right).$$

2.3 Binomial ideals in terms of lattice ideals

Let K be a field and $S := K[t_1, \ldots, t_n]$ a polynomial ring with n variables over K. By [16, Corollary 2.5] we know that a binomial ideal containing no monomials is characterized by a lattice. In some way we complement this result. If the field has characteristic different that 2, we show that a binomial ideal (without restrictions) can be characterized by a finite number of lattices. If the field has characteristic 2, the binomial ideal depends of a lattice ideal and of a monomial ideal.

Lemma 2.3.1 *Let I be a binomial ideal. I contains no monomials if and only if there are $a_1, b_1, \ldots, a_r, b_r$ in $\mathbb{N}^n$ and a partial character $\rho\colon \mathcal{L}_\rho := \mathbb{Z}\{a_1 - b_1, \ldots, a_r - b_r\} \to K^*$ such that $I = \left(t^{a_1} - \rho(a_1 - b_1)t^{b_1}, \ldots, t^{a_r} - \rho(a_r - b_r)t^{b_r}\right)$.*

Proof. ($\Rightarrow$) Assume $I = \left(t^{a_1} - \lambda_1 t^{b_1}, \ldots, t^{a_s} - \lambda_s t^{b_s}\right)$. By [16, Corollary 2.5] there is a lattice $\mathcal{L}_\rho$ and a partial character $\rho : \mathcal{L}_\rho \to K^*$ such that

$$I : (t_1 \cdots t_n)^\infty = I(\rho).$$

For $i = 1, \ldots, s$ we have $t^{a_i} - \lambda_i t^{b_i} \in I \subset I : (t_1 \cdots t_n)^\infty = I(\rho)$. By Proposition 2.2.6 $a_i - b_i \in \mathcal{L}_\rho$ and $\lambda_i = \rho(a_i - b_i)$, then $I = \left(t^{a_1} - \rho(a_1 - b_1)t^{b_1}, \ldots, t^{a_s} - \rho(a_s - b_s)t^{b_s}\right)$, with $\{a_1 - b_1, \ldots, a_s - b_s\} \subset \mathcal{L}_\rho$. Finally the set $\{a_1 - b_1, \ldots, a_s - b_s\}$ can be extended to a generating set $\{a_1 - b_1, \ldots, a_r - b_r\}$ of $\mathcal{L}_\rho$.

($\Leftarrow$) Observe that there are c_i's and d_i's in $\mathbb{Z}^n$ such that

$$\begin{aligned} I &= \left(t^{a_1} - \rho(a_1 - b_1)t^{b_1}, \ldots, t^{a_r} - \rho(a_r - b_r)t^{b_r}\right) = \\ &= \left(t^{c_1}(t^{d_1^+} - \rho(d_1)t^{d_1^-}), \ldots, t^{c_r}(t^{d_r^+} - \rho(d_r)t^{d_r^-})\right). \end{aligned}$$

By Theorem 2.1.23 (ii) $\left(t^{d_1^+} - \rho(d_1)t^{d_1^-}, \ldots, t^{d_r^+} - \rho(d_r)t^{d_r^-}\right)$ contains no monomials, so, I contains no monomials. □

Lemma 2.3.2 *Let* $I_1 := \left(\left\{t^{a_i} - \rho_1(a_i - b_i)t^{b_i}\right\}_{i=1}^r\right)$ *and* $I_2 := \left(\left\{t^{c_j} - \rho_2(c_j - d_j)t^{d_j}\right\}_{j=1}^s\right)$ *be ideals of* S*, where* ρ_1 *and* ρ_2 *are partial characters from* $\mathcal{L}_{\rho_1} := \mathbb{Z}\{a_1 - b_1, \ldots, a_r - b_r\}$ *and* $\mathcal{L}_{\rho_2} := \mathbb{Z}\{c_1 - d_1, \ldots, c_s - d_s\}$*, respectively. The ideal* $I_1 + I_2$ *contains no monomials if and only if* $\rho_1 |_{\mathcal{L}_{\rho_1} \cap \mathcal{L}_{\rho_2}} = \rho_2 |_{\mathcal{L}_{\rho_1} \cap \mathcal{L}_{\rho_2}}$.

Proof. ($\Rightarrow$) Assume $\rho_1 |_{\mathcal{L}_{\rho_1} \cap \mathcal{L}_{\rho_2}} \neq \rho_2 |_{\mathcal{L}_{\rho_1} \cap \mathcal{L}_{\rho_2}}$. Let a be an element of $\mathcal{L}_{\rho_1} \cap \mathcal{L}_{\rho_2}$ such that $\rho_1(a) \neq \rho_2(a)$. For $i = 1, \ldots, r$, define $\gamma_i := \operatorname{lcm}(a_i, b_i)$, $a_i' := a_i - \gamma_i$ and $b_i' := b_i - \gamma_i$. Thus $I_1 = \left(t^{\gamma_i}\left(t^{a_i'} - \rho_1(a_i' - b_i')t^{b_i'}\right)\right)$ and $a_i - b_i = a_i' - b_i'$ for $i = 1, \ldots, r$. By Lemma 2.2.5, there is δ in $\mathbb{N}^n$ such that $t^\delta\left(t^{a^+} - \rho_1(a)t^{a^-}\right) \in \left(t^{a_i'} - \rho_1(a_i' - b_i')t^{b_i'}\right)$. Therefore

$$t^{\delta + \sum_{i=1}^r \gamma_i}\left(t^{a^+} - \rho_1(a)t^{a^-}\right) \in \left(t^{\gamma_i}\left(t^{a_i'} - \rho_1(a_i' - b_i')t^{b_i'}\right)\right) = I_1.$$

In a similar way, there is γ in $\mathbb{N}^n$ such that $t^\gamma\left(t^{a^+} - \rho_2(a)t^{a^-}\right) \in I_2$. Finally the polynomials $t^{\gamma+\delta+\sum_{i=1}^r \gamma_i}\left(t^{a^+} - \rho_1(a)t^{a^-}\right)$ and $t^{\gamma+\delta+\sum_{i=1}^r \gamma_i}\left(t^{a^+} - \rho_2(a)t^{a^-}\right)$ are in $I_1 + I_2$, and the difference of them, $t^{\gamma+\delta+\sum_{i=1}^r \gamma_i}\left(\rho_1(a) - \rho_2(a)\right)t^{a^-}$, is a monomial also in $I_1 + I_2$.

($\Leftarrow$) Define the lattice $\mathcal{L} := \mathcal{L}_{\rho_1} + \mathcal{L}_{\rho_2}$ and the partial character ρ from $\mathcal{L}$ as

$$\rho(a) := \begin{cases} \rho_1(a) & \text{if } a \in \mathcal{L}_{\rho_1}, \\ \rho_2(a) & \text{if } a \in \mathcal{L}_{\rho_2}. \end{cases}$$

By Theorem 2.1.21 $I(\rho)$ contains no monomials. As $I_1 + I_2$ is contained in $I(\rho)$, then $I_1 + I_2$ contains no monomials. □

Remark 2.3.3 Observe that Lemma 2.3.2 can be seen as $I_1 + I_2$ contains no monomials if and only if there is a lattice $\mathcal{L}_\rho := \mathbb{Z}\{e_1 - f_1, \ldots, e_t - f_t\}$ and a partial character ρ from $\mathcal{L}_\rho$ such that

$$I_1 + I_2 := \left(\left\{t^{e_i} - \rho(e_i - f_i)t^{f_i}\right\}_{i=1}^t\right).$$

We come to one of the main results of this section.

Theorem 2.3.4 *Let K be a field with characteristic different than 2. An ideal I of S is a binomial ideal if and only if there are m lattices $\mathcal{L}_i := \mathbb{Z}\{a_{i1} - b_{i1}, \ldots, a_{1r_i} - b_{1r_i}\}$ and m partial characters $\rho_i \colon \mathcal{L}_i \to K^*$ such that $I = I_1 + \cdots + I_m$, where*

$$I_i := \left(t^{a_{i1}} - \rho_i(a_{i1} - b_{i1})t^{b_{i1}}, \ldots, t^{a_{ir_i}} - \rho_i(a_{ir_i} - b_{ir_i})t^{b_{ir_i}}\right),$$

and for $i \neq j$, the ideal $I_i + I_j$ contains a monomial.

Proof. Observe that if a monomial t^a is a generator of the ideal I, then this monomial can be substituted by the binomials $t^{2a} - t^a$ and $t^{2a} - 2t^a$; thus the ideal I can be written as $I = \left(t^{a_1} - \lambda_1 t^{b_1}, \ldots, t^{a_s} - \lambda_s t^{b_s}\right)$, where $\lambda_1, \ldots, \lambda_s$ are elements of K^*. Define for $i = 1, \ldots, s$, the ideals $I_i := \left(t^{a_i} - \rho_i'(a_i - b_i)t^{b_i}\right)$, where $\rho_i'(a_i - b_i) := \lambda_i$ is a partial character from $\mathcal{L}_i' := \mathbb{Z}\{a_i - b_i\}$. The rest of the proof is just a consequence of Remark 2.3.3. We compare every two ideals. If two ideals I_i and I_j are such that their sum contains no monomials, then we define the ideal $I_{ij} := I_i + I_j$. By Remark 2.3.3 I_{ij} depends of a lattice and a partial character, so we replace I_i and I_j by the ideal I_{ij}. We compare again every two ideals. We do this until we obtain maximal components in the sense that the sum of each two ideals contains a monomial. $\square$

When the characteristic of the field is 2, then a binomial ideal is characterized by a lattice and a set of monomials.

Remark 2.3.5 Let K be a field of characteristic 2. If I is a binomial ideal of S, then there is a partial character

$$\rho \colon \mathcal{L}_\rho := \mathbb{Z}\{a_1 - b_1, \ldots, a_r - b_r\} \to K^*$$

and monomials $t^{c_1}, \ldots, t^{c_s}$ in S such that

$$I = \left(t^{a_1} - \rho(a_1 - b_1)t^{b_1}, \ldots, t^{a_r} - \rho(a_r - b_r)t^{b_r}\right) + \left(t^{c_1}, \ldots, t^{c_s}\right).$$

This is true because the ideal I is of the form $I = \left(t^{a_1} - t^{b_1}, \ldots, t^{a_r} - t^{b_r}, t^{c_1}, \ldots, t^{c_s}\right)$. Thus the associated partial character is the trivial partial character and the lattice is the lattice defined by the powers of the pure binomials of I. The following example shows that this property is not always true when the characteristic is different than 2

Example 2.3.6 Let K be a field with characteristic other than 2 and $S := K[t_1, t_2, t_3, t_4]$. The ideal $I = (t_1t_3 - t_2t_3, t_1t_4 - 2t_2t_4, t_2t_3t_4)$ can not be characterized using only a lattice and a set of monomials as in Remark 2.3.5. Assume that there is a partial character ρ from a lattice $\mathcal{L}_\rho := \{a_1 - b_1, \ldots, a_r - b_r\}$ such that

$$I = \left(t^{a_1} - \rho(a_1 - b_1)t^{b_1}, \ldots, t^{a_r} - \rho(a_r - b_r)t^{b_r}\right) + \left(t^{c_1}, \ldots, t^{c_s}\right).$$

By Lemma 2.3.2, there is δ in $\mathbb{N}^n$ such that $t^\delta * t_3(t_1 - t_2)$ is in the part of I that depends of the lattice. Thus $\rho(e_1 - e_2) = 1$, where e_1 and e_2 are two of the canonical vectors of $\mathbb{N}^n$. But also there is γ in $\mathbb{N}^n$ such that $t^\gamma * t_4(t_1 - 2t_2)$ is also in the part of I that depends of the lattice. In this case we obtain $\rho(e_1 - e_2) = 2$. A contradiction.

2.4 Gröbner basis of lattice ideals

Let K be a field, $S := K[t_1, \dots, t_n]$ a polynomial ring with n variables over K, $\mathcal{L}_\rho \subset \mathbb{Z}^n$ a lattice and ρ a partial character from $\mathcal{L}_\rho$. In this section we prove that there are a finite number of elements $a_1, \dots, a_r$ in the lattice $\mathcal{L}_\rho$ such that the binomials $t^{a_1^+} - \rho(a_1)t^{a_1^-}, \dots, t^{a_r^+} - \rho(a_r)t^{a_r^-}$ form a Gröbner basis of the lattice ideal $I(\rho)$. Then we adapt the Buchberger's algorithm to create a procedure that extends a set of generators of $\mathcal{L}_\rho$, $\{a_1, \dots, a_r\}$, to a subset $\{a_1, \dots, a_s\}$ of $\mathcal{L}_\rho$ such that $\left\{t^{a_1^+} - \rho(a_1)t^{a_1^-}, \dots, t^{a_s^+} - \rho(a_s)t^{a_s^-}\right\}$ is a Gröbner basis of $I(\rho)$.

We come to one of the main results of this section.

Theorem 2.4.1 *Let $\rho\colon \mathcal{L}_\rho \to K^*$ be a partial character and $\prec$ an arbitrary monomial order fixed on S. There are elements $a_1, \dots, a_s$ of $\mathcal{L}_\rho$ such that*

$$\mathcal{G} := \left\{t^{a_1^+} - \rho(a_1)t^{a_1^-}, \dots, t^{a_s^+} - \rho(a_s)t^{a_s^-}\right\}$$

is a Gröbner basis of $I(\rho)$. In particular the reduced Gröbner basis has this form.

Proof. By Proposition 2.1.20 there is a Gröbner basis for $I(\rho)$ of the form

$$\mathcal{G}' := \left\{\mathfrak{f}(a_1), \dots, \mathfrak{f}(a_r), \mathfrak{g}(\gamma_{r+1}, b'_{r+1}, b_{r+1}), \dots, \mathfrak{g}(\gamma_s, b'_s, b_s)\right\}.$$

We can assume that in every $\mathfrak{f}(a_i)$ we have $a_i^+ \succ a_i^-$. As $\mathfrak{g}(\gamma_j, b'_j, b_j) = \rho(b_j)t^{\gamma - b_j} - \rho(b'_j)t^{\gamma - b'_j}$ and

$$\left(\rho(b_j)t^{\gamma-b_j} - \rho(b'_j)t^{\gamma-b'_j}\right) = \left(t^{\gamma-b_j} - \rho(b'_j - b_j)t^{\gamma-b'_j}\right) = \left(t^c\left(t^{a_j^+} - \rho(b'_j - b_j)t^{a_j^-}\right)\right),$$

then every $\mathfrak{g}(\gamma_j, b'_j, b_j)$ can be substituted by $t^{a_j^+} - \rho(a_j)t^{a_j^-}$, because $\rho(a_j) = \rho(b'_j - b_j)$ by Theorem 2.1.21, t^c can be omitted by Theorem 2.1.22 and the leading term of $\mathfrak{f}(a_j)$ divides the leading term of $\mathfrak{g}(\gamma_j, b'_j, b_j)$, for $j = r+1, \dots, s$. Finally by Proposition 2.2.6 if $\mathfrak{f}(a_j)$ is an element of $I(\rho)$, then a_j is an element of $\mathcal{L}_\rho$. $\square$

Now we give an algorithm that extends a generating set of $\{a_1, \dots, a_r\}$ of $\mathcal{L}_\rho$ to a set of vectors $\{a_1, \dots, a_s\}$ of $\mathcal{L}_\rho$ such that $\mathcal{G} := \left\{t^{a_1^+} - \rho(a_1)t^{a_1^-}, \dots, t^{a_s^+} - \rho(a_s)t^{a_s^-}\right\}$ is a Gröbner basis of $I(\rho)$. The idea is very simple, we are going to adapt the Buchberger's algorithm (Proposition 1.1.19) that works with monomials in an algorithm that works with vectors.

Lemma 2.4.2 *Let a, b be elements of $\mathbb{Z}^n$. The following hold:*

(i) $\operatorname{lcm}(a^+, b^+) - b - \gcd(\operatorname{lcm}(a^+, b^+) - b, \operatorname{lcm}(a^+, b^+) - a) = (a-b)^+$.

(ii) $\operatorname{lcm}(a^+, b^+) - a - \gcd(\operatorname{lcm}(a^+, b^+) - b, \operatorname{lcm}(a^+, b^+) - a) = (a-b)^-$.

(iii) $\gcd\left(\operatorname{lcm}\left(a^{+}, b^{+}\right)-b, \operatorname{lcm}\left(a^{+}, b^{+}\right)-a\right)=\gcd\left(a^{-}, b^{-}\right).$

Proof. The idea is to compare the *i-th* element of both sides of each equation. Considering all possible combinations of a_i and b_i : $a_i \geq 0, a_i < 0, b_i \geq 0, b_i < 0, a_i \geq b_i$ and $a_i < b_i$ the proof follows readily. □

Let a, b be elements of $\mathbb{Z}^n$. Observe the following facts on S-polynomials and reductions.

Lemma 2.4.3 *Let a, b be elements of $\mathbb{Z}^n$ and set $\gamma := \gcd\left(a^{-}, b^{-}\right)$. The following hold.*

(i) $S(t^{a^+} - \rho(a)t^{a^-}, t^{b^+} - \rho(b)t^{b^-}) = t^{\gamma}\left(t^{(a-b)^+} - \rho(a-b)t^{(a-b)^-}\right).$

(ii) *If $b^+ \mid a^+$, the remainder after dividing $t^{a^+} - \rho(a)t^{a^-}$ by $t^{b^+} - \rho(b)t^{b^-}$ is* $t^{\gamma}\left(\rho(b)t^{(a-b)^+} - \rho(a)t^{(a-b)^-}\right).$

Proof. Both items are a consequence of Lemma 2.4.2. □

Lemma 2.4.4 *Let a, b be elements of $\mathbb{Z}^n$, c_1, c_2 elements of $\mathbb{N}^n$, set $\gamma := \gcd\left(a^{-}, b^{-}\right)$ and $\delta := \gcd\left(\operatorname{lcm}\left(a^{+}+c_1, b^{+}+c_2\right)-b, \operatorname{lcm}\left(a^{+}+c_1, b^{+}+c_2\right)-a\right)$. The following hold.*

(i) $S(t^{a^+ + c_1} - \rho(a)t^{a^- + c_1}, t^{b^+ + c_2} - \rho(b)t^{b^- + c_2}) = t^{\delta}\left(t^{(a-b)^+} - \rho(a-b)t^{(a-b)^-}\right).$

(ii) *If $b^+ + c_2 \mid a^+ + c_1$, the remainder after dividing $t^{a^+ + c_1} - \rho(a)t^{a^- + c_1}$ by $t^{b^+ + c_2} - \rho(b)t^{b^- + c_2}$ is $t^{c_1 + \gamma}\left(\rho(b)t^{(a-b)^+} - \rho(a)t^{(a-b)^-}\right).$*

Proof. The proof is similar to the proof of Lemma 2.4.2. □

Definition 2.4.5 Let $\mathcal{A} := \{a_1, \ldots, a_r\}$ be an ordered set of $\mathbb{Z}^n$ with $a_i^+ \succ_{lex} a_i^-$ for all i, and b an element of $\mathbb{Z}^n$. We define the element

$$\overline{b}^{\mathcal{A}} := b \ominus a_{b1} \ominus \cdots \ominus a_{bs},$$

where $\ominus$ is a non-associative operation, we perform this operation from left to right, i.e., first $b \ominus a_{b1}$, second $(b \ominus a_{b1}) \ominus a_{b2}$ and so on. It is defined as:

$$x \ominus y := \begin{cases} x - y & \text{if } \;(x-y)^+ \succ_{lex} (x-y)^-, \\ y - x & \text{otherwise;} \end{cases}$$

for all a_{bj} we have

(i) $a_1, \ldots, a_{bj-1}$ are no divisors of $b \ominus a_{b1} \ominus \cdots \ominus a_{b(j-1)}$

(ii) $a_{bj} \mid b \ominus a_{b1} \ominus \cdots \ominus a_{b(j-1)}$, and there is not other a_{bk} such that $a_{bk} \mid b \ominus a_{b1} \ominus \cdots \ominus a_{bs}$.

Using Definition 2.4.5, Lemma 2.4.4 and Buchberger's algorithm we extend a set of generators of $\mathcal{L}_\rho$, $\{a_1, \ldots, a_r\}$, to a subset $\{a_1, \ldots, a_s\}$ of $\mathcal{L}_\rho$ such that

$$\mathcal{G} = \left\{ t^{a_1^+} - \rho(a_1)t^{a_1^-}, \ldots, t^{a_s^+} - \rho(a_s)t^{a_s^-} \right\}$$

is a Gröbner basis of $I(\rho)$.

Theorem 2.4.6 *Let $\rho\colon \mathcal{L}_\rho \to K^*$ be a partial character and $\prec$ an arbitrary monomial order fixed on S. The set $\{a_1 \ldots, a_r\}$ can be extended to a subset of elements $\{a_1, \ldots, a_s\}$ of $\mathcal{L}_\rho$ such that*

$$\mathcal{G} = \left\{ t^{a_1^+} - \rho(a_1)t^{a_1^-}, \ldots, t^{a_s^+} - \rho(a_s)t^{a_s^-} \right\}$$

is a Gröbner basis of $I(\rho)$ in a finite number of steps by the following algorithm.

Data: $\{a_1, \ldots, a_r\}$, *a set of generators of* $\mathcal{L}_\rho$
Result: $\mathcal{L}$, *a finite subset of* $\mathcal{L}_\rho$ *such that* $\mathcal{G} = \left\{ t^{a^+} - \rho(a)t^{a^-} \mid a \in \mathcal{L} \right\}$ *is a Gröbner basis of* $I(\rho)$.
$\mathcal{A} := \{(1, \mathbf{1}), (0, a_1), \ldots, (0, a_r)\} \subset \mathbb{Z}^{n+1}$;
repeat
    $\mathcal{A}' := \mathcal{A}$
    for *each pair* a, b *in* $\mathcal{A}', a \neq b$ **do**
        $S := \overline{a \ominus b}^{\mathcal{A}'}$
        if $S \neq 0$ **then**
            $\mathcal{A} := \mathcal{A} \cup \{S\}$
        end
    end
until $\mathcal{A} = \mathcal{A}'$;
$\mathcal{L} := \{a \in \mathcal{A} \mid (0, a) \in \mathcal{A}\}$.

Proof. It is a consequence of Definition 2.4.5, Lemma 2.4.4 and Buchberger's algorithm (Proposition 1.1.19). □

2.5 Algebraic invariants of lattice ideals

This is one of our favorite sections for its implications. We prove that a Gröbner basis, or more precisely the initial ideal of a lattice ideal, is independent from the partial character, and so are the Hilbert function, the Hilbert series, the Hilbert polynomial, the index of regularity, the a-invariant and the degree of the lattice ideal.

Let K be a field, $S := K[t_1, \ldots, t_n]$ a polynomial ring with n variables over K, $\mathcal{L}_\rho \subset \mathbb{Z}^n$ a lattice and ρ a partial character from $\mathcal{L}_\rho$. We define

$H_\rho(d) := H_{I(\rho)}(d)$ (Hilbert function),

$F_\rho(t) := F_{I(\rho)}(t)$ (Hilbert series), and

$h_\rho(t) := h_{I(\rho)}(t)$ (Hilbert polynomial).

We come to the main result of this section.

Theorem 2.5.1 *Let $\rho\colon \mathcal{L}_\rho \to K^*$ be a partial character and $\prec$ an arbitrary monomial order fixed on S. The set $\mathcal{G} := \left\{t^{a_1^+} - \rho(a_1)t^{a_1^-}, \ldots, t^{a_r^+} - \rho(a_r)t^{a_r^-}\right\}$ is a Gröbner basis of the lattice ideal $I(\rho)$ if and only if the set $\mathcal{G}' := \left\{t^{a_1^+} - t^{a_1^-}, \ldots, t^{a_r^+} - t^{a_r^-}\right\}$ is a Gröbner basis of the pure lattice ideal $I(\mathcal{L}_\rho)$.*

Proof. We denote $t^{a_i^+} - t^{a_i^-}$ by $\mathfrak{f}'(a_i)$ and $\mathfrak{g}'(\gamma, b_1, b_2) := t^{\gamma - b_2} - t^{\gamma - b_1}$. We just need to see that in Lemma 2.1.18

$$\mathrm{S}\left(\mathfrak{f}(a_i), \mathfrak{f}(a_j)\right) = \mathfrak{g}(\gamma, b_1, b_2) \qquad \text{if and only if} \qquad \mathrm{S}\left(\mathfrak{f}'(a_i), \mathfrak{f}'(a_j)\right) = \mathfrak{g}'(\gamma, b_1, b_2),$$

and in Lemma 2.1.19

$$\overline{\mathfrak{g}(\gamma, d_1, d_2)}^{G} = \mathfrak{g}(\gamma', d_1', d_2') \qquad \text{if and only if} \qquad \overline{\mathfrak{g}'(\gamma, d_1, d_2)}^{G'} = \mathfrak{g}'(\gamma', d_1', d_2').$$

Finally the fact that $\mathfrak{g}(\gamma', d_1', d_2') = 0$ if and only if $\mathfrak{g}'(\gamma', d_1', d_2') = 0$ tells us that the result is true. $\square$

Theorem 2.5.2 (Hilbert function of a lattice ideal is independent from the partial character) *If $\mathcal{L}$ is a lattice and ρ, ρ' are two partial characters on $\mathcal{L}$, then*

$$H_\rho(d) = H_{\rho'}(d) \qquad \textit{for all } d \geq 0.$$

Proof. By Theorem 2.5.1 $\mathcal{G} := \left\{t^{a_1^+} - \rho(a_1)t^{a_1^-}, \ldots, t^{a_r^+} - \rho(a_r)t^{a_r^-}\right\}$ is a Gröbner basis of $I(\rho)$ if and only if $\mathcal{G}' := \left\{t^{a_1^+} - \rho'(a_1)t^{a_1^-}, \ldots, t^{a_r^+} - \rho'(a_r)t^{a_r^-}\right\}$ is a Gröbner basis of $I(\rho)$. Thus $\mathrm{LT}(I(\rho)) = \mathrm{LT}(I(\rho'))$. $\square$

Corollary 2.5.3 (Algebraic invariants of a lattice ideal are independent from the partial character) *If $\mathcal{L}$ is a lattice and ρ, ρ' are two partial characters on $\mathcal{L}$, then*

$F_\rho(t) = F_{\rho'}(t)$ *(Hilbert series).*

$h_\rho(t) = h_{\rho'}(t)$ *(Hilbert polynomial).*

$\deg(S/I(\rho)) = \deg(S/I(\rho'))$ *(degree).*

$\operatorname{reg} S/I(\rho) = \operatorname{reg} S/I(\rho')$ *(regularity index).*

$a(\rho) = a(\rho')$ *(a-invariant).*

Proof. They are a direct consequence of Theorem 2.5.2. $\square$

2.6 Graded lattice ideals of dimension 1

Let K be a field, $S := K[t_1, \ldots, t_n]$ a polynomial ring with n variables over K, $\mathcal{L}_\rho \subset \mathbb{Z}^n$ a lattice and ρ a partial character from $\mathcal{L}_\rho$. In this section we prove that if the lattice ideal $I(\rho)$ is standard-graded and has dimension 1, then the degree of this ideal is equal to $|T(\mathbb{Z}^n/\mathcal{L})|$. Let ω be a vector with positive integer entries. If $I(\rho)$ is ω-graded of dimension 1, we establish a complete intersection criterion in algebraic and geometric terms. If $I(\rho)$ is ω-graded of dimension 1, and K has positive characteristic, then we show that $I(\rho)$ is a pure binomial set theoretic complete intersection. If K has characteristic zero, we prove that in the set of pure lattice ideals the property binomial set theoretic complete intersection implies complete intersection. Let $\upsilon_1, \ldots, \upsilon_n$ be a sequence of vectors in $\mathbb{N}^s$ and $\mathcal{Q}$ the projective algebraic toric set parameterized by the vectors $\upsilon_1, \ldots, \upsilon_n$ on $\mathbb{P}^{n-1}$. In the last subsection we apply the results about graded pure lattice ideals of dimension 1 to the vanishing ideal $I(\mathcal{Q})$.

By the dimension of $I(\rho)$ we mean the Krull dimension of the quotient ring $S/I(\rho)$.

Definition 2.6.1 Let $a := (a_1, \ldots, a_n)$ be an element of $\mathbb{Z}^n$. We set $|a| := \sum_{i=1}^n a_i$. A lattice $\mathcal{L}$ is called *homogeneous* if $|a| = 0$ for all $a \in \mathcal{L}$.

Lemma 2.6.2 *Let $\rho : \mathcal{L}_\rho \to K^*$ be a partial character. Then $\mathcal{L}_\rho$ is homogeneous if and only if its lattice ideal $I(\rho)$ is graded with respect to the standard graduation.*

Proof. We can express $a = a^+ - a^-$ with disjoint support $\operatorname{supp}(a^+) \cap \operatorname{supp}(a^-) = \phi$, then $0 = |a| = |a^+| - |a^-|$ if and only if $|a^+| = |a^-|$ if and only if the lattice ideal $I(\rho) = \left(\left\{t^{a^+} - \rho(a)t^{a^-} \mid a \in \mathcal{L}_\rho\right\}\right)$ is graded. □

Definition 2.6.3 Let $\omega := (\omega_1, \ldots, \omega_n)$ be an integral vector with positive entries. A lattice $\mathcal{L}$ is called ω-homogeneous (or *homogeneous with respect to* ω) if $\langle \omega, a \rangle = 0$ for all $a \in \mathcal{L}$.

Remark 2.6.4 Analogous to Lemma 2.6.2, a lattice $\mathcal{L}_\rho$ is ω-homogeneous if and only if its lattice ideal $I(\rho)$ is graded with respect to the grading of S induced by setting $\deg(t_i) = \omega_i$ for $i = 1, \ldots, n$. The standard grading of S is obtained when $\omega = (1, \ldots, 1)$.

Lemma 2.6.5 *Let $\rho : \mathcal{L}_\rho \to K^*$ be a partial character. If $\mathcal{L}_\rho \subset \mathbb{Z}^n$ is homogeneous of rank $n-1$, then $S/I(\rho)$ is a Cohen-Macaulay ring of dimension 1.*

Proof. This follows from Theorem 2.1.23 and using Proposition 2.2.10. □

2.6.1 The degree

Let K be a field, $S := K[t_1, \ldots, t_n]$ a polynomial ring with n variables over K and $\mathcal{L}$ a lattice of $\mathbb{Z}^n$. In this subsection we are going to work with the pure lattice ideal $I(\mathcal{L})$, i.e. we use the trivial partial character to define the lattice ideal. We do not consider an arbitrary partial character because by Corollary 2.5.3 the degree of a lattice ideal is independent from the partial character. We prove that an element of $T(\mathbb{Z}^n/\mathcal{L})$ can be written in a unique way. Then we show that if the ideal $I(\mathcal{L})$ is graded and has dimension 1, then the degree of this ideal is equal to $|T(\mathbb{Z}^n/\mathcal{L})|$.

In what follows of this subsection we shall assume that $\succ$ is the revlex order $\succ_{revlex}$ (reverse lexicographical order, Definition 1.1.10) on the monomials of S. It is also important to remember from Section 1, Definition 1.1.11, that if g is a polynomial of S, we denote the leading term of g by $\mathrm{LT}(g)$ as well as if L is an ideal of S, the initial ideal of L, denoted by $\mathrm{LT}(L)$, is generated by the leading terms of the polynomials of L.

Lemma 2.6.6 [18, Lemma 2.3] *Let $\mathcal{A} := \{a_1, \ldots, a_r\}$ be a subset of $\mathbb{Z}^n$ and define $\mathcal{L} := \mathbb{Z}\mathcal{A}$. Then*

(i) $\mathbb{Q}\mathcal{L} \cap \mathbb{Z}^n/\mathbb{Z}\mathcal{L} = T(\mathbb{Z}^n/\mathbb{Z}\mathcal{L})$.

(ii) *In particular, $\mathbb{Q}\mathcal{L} \cap \mathbb{Z}^n = \mathbb{Z}\mathcal{L}$ if and only if $\mathbb{Z}^n/\mathbb{Z}\mathcal{L}$ is torsion-free.*

Lemma 2.6.7 *Let $\mathcal{L} \subset \mathbb{Z}^n$ be a homogeneous lattice of rank $n-1$ and let $\mathbb{Q}\mathcal{L}$ be the $\mathbb{Q}$-linear space spanned by $\mathcal{L}$. Then*

(a) $\mathbb{Q}\mathcal{L} \cap \mathbb{Z}^n = \mathbb{Z}(e_1 - e_n) \oplus \cdots \oplus \mathbb{Z}(e_{n-1} - e_n)$, *where e_i is the i^{th} unit vector in $\mathbb{Q}^n$.*

(b) $T(\mathbb{Z}^n/\mathcal{L}) = \mathbb{Z}(e_1 - e_n) \oplus \cdots \oplus \mathbb{Z}(e_{n-1} - e_n)/\mathcal{L}$.

Proof. (a) ($\subseteq$) Take $a := (a_1, \ldots, a_n)$ in $\mathbb{Q}\mathcal{L} \cap \mathbb{Z}^n$. Then $a_n = -a_{n-1} - \cdots - a_1$ and we can write

$$a = a_1(e_1 - e_n) + \cdots + a_{n-1}(e_{n-1} - e_n).$$

Thus a is a $\mathbb{Z}$-linear combination of $e_1 - e_n, \ldots, e_{n-1} - e_n$. ($\supseteq$) It suffices to show that $e_k - e_n$ is in $\mathbb{Q}\mathcal{L}$ for all k. The dimension of $\mathbb{Q}\mathcal{L}$ is equal to $\mathrm{rank}(\mathcal{L}) = n-1$. Notice that $e_n \notin \mathbb{Q}\mathcal{L}$ because $\mathcal{L}$ is homogeneous. Hence $\mathbb{Q}e_n + \mathbb{Q}\mathcal{L} = \mathbb{Q}^n$. Therefore we can write

$$e_k = \mu_{kn}e_n + \lambda_{k1}\gamma_1 + \cdots + \lambda_{km}\gamma_m \qquad (\mu_{kn}, \lambda_{ki} \in \mathbb{Q}; \gamma_j \in \mathcal{L} \text{ for all } i, j).$$

Taking inner products with $\mathbf{1} := (1, \ldots, 1) \in \mathbb{Z}^n$ and using that $\langle \mathbf{1}, \gamma_i \rangle = 0$ for all i, we get $1 - \mu_{kn} = \langle \mathbf{1}, e_k - \mu_{kn}e_n \rangle = \langle \mathbf{1}, \lambda_{k1}\gamma_1 + \cdots + \lambda_{km}\gamma_m \rangle = \sum_{i=1}^{m} \lambda_{ki} \langle \gamma_i \rangle = 0$. Thus $\mu_{kn} = 1$. We conclude that $e_k - e_n \in \mathbb{Q}\mathcal{L}$.

(b) By Lemma 2.6.6 (i) the torsion subgroup of $\mathbb{Z}^n/\mathcal{L}$ is $\mathbb{Q}\mathcal{L} \cap \mathbb{Z}^n/\mathcal{L}$. Hence, the expression for the torsion follows from (a). $\Box$

Remark 2.6.8 By Buchberger's algorithm (Proposition 1.1.19) and by Proposition 1.1.21, a graded pure lattice ideal $I(\mathcal{L})$ has a unique reduced Gröbner basis $\mathcal{G}$ consisting of homogeneous pure binomials and, by Theorem 2.1.23 (iii), each pure binomial $t^a - t^b \in \mathcal{G}$ satisfies that $\mathrm{supp}(a) \cap \mathrm{supp}(b) = \emptyset$.

Lemma 2.6.9 *Let $\mathcal{L} \subset \mathbb{Z}^n$ be a homogeneous lattice of rank $n-1$. Then, given $\widetilde{\gamma} := \gamma + \mathcal{L}$ in the torsion subgroup $T(\mathbb{Z}^n/\mathcal{L})$ there exists a unique $a := (a_1, \ldots, a_{n-1}, a_n)$ in $\mathbb{Z}^n$ such that*

(i) $a_i \geq 0$ *for* $i = 1, \ldots, n-1$,

(ii) $t_1^{a_1} \cdots t_{n-1}^{a_{n-1}} \notin \mathrm{LT}(I(\mathcal{L}))$, *and*

(iii) $\widetilde{a} = \widetilde{\gamma}$.

Proof. First we show the existence of a. If $\gamma \in \mathcal{L}$, then $a = 0$ satisfies (i), (ii) and (iii). Assume that $\gamma \notin \mathcal{L}$. By Lemma 2.6.7, $\widetilde{e}_i - \widetilde{e}_n$ is a torsion element of $\mathbb{Z}^n/\mathcal{L}$ for $1 \leq i \leq n-1$, that is, there is a positive integer n_i such that $n_i(e_i - e_n)$ is in $\mathcal{L}$. If γ_i is the i^{th} entry of γ, there are integers q_i and c_i such that $\gamma_i = q_i n_i + c_i$ and $0 \leq c_i \leq n_i - 1$. Hence, since $|\gamma| = 0$, we can write

$$\begin{aligned} \gamma &= \gamma_1(e_1 - e_n) + \cdots + \gamma_{n-1}(e_{n-1} - e_n) \\ &= c_1(e_1 - e_n) + \cdots + c_{n-1}(e_{n-1} - e_n) + q_1 n_1(e_1 - e_n) + \cdots + q_{n-1}n_{n-1}(e_{n-1} - e_n). \end{aligned}$$

If we set $c := (c_1, \ldots, c_n) = c_1(e_1 - e_n) + \cdots + c_{n-1}(e_{n-1} - e_n)$, then $\widetilde{c} = \widetilde{\gamma}$, $c \notin \mathcal{L}$ and $|c| = 0$. Consider the homogeneous binomial

$$f := t_1^{c_1} \cdots t_{n-1}^{c_{n-1}} - t_n^{-c_n}.$$

Let $\mathcal{G} := \{g_1, \ldots, g_r\}$ be the reduced Gröbner basis of $I(\mathcal{L})$, with respect to the revlex order, then $\mathrm{LT}(I(\mathcal{L})) = (\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_r))$. By Remark 2.6.8, t_n does not divide any of the leading terms of $g_1, \ldots, g_r$. Hence, by the division algorithm Proposition 1.1.12, we can write

$$f = h_1 g_1 + \cdots + h_r g_r + g \tag{$*$}$$

for some $h_1, \ldots, h_r$ in S, where $g := t_1^{b_1} \cdots t_n^{b_n} - t_n^{-c_n}$ is homogeneous and $t^b := t_1^{b_1} \cdots t_n^{b_n}$ is not divisible by any of the leading terms of $g_1, \ldots, g_r$, i.e., $t^b \notin \mathrm{LT}(I(\mathcal{L}))$. Thus, $t_1^{b_1} \cdots t_{n-1}^{b_{n-1}} \notin \mathrm{LT}(I(\mathcal{L}))$. Notice that $b_i > 0$ for some $1 \leq i \leq n-1$, otherwise $g = 0$ and c would be in $\mathcal{L}$, a contradiction. By Eq. $(*)$, the binomial $f - g$ is in $I(\mathcal{L})$ and simplifies to

$$f - g = t_1^{c_1} \cdots t_{n-1}^{c_{n-1}} - t_1^{b_1} \cdots t_n^{b_n}.$$

Hence, $(c_1, \ldots, c_{n-1}, 0) - (b_1, \ldots, b_n)$ is in $\mathcal{L}$. Consequently, one has

$$(c_1, \ldots, c_{n-1}, c_n) - (b_1, \ldots, b_{n-1}, b_n + c_n) = (c_1, \ldots, c_{n-1}, 0) - (b_1, \ldots, b_{n-1}, b_n) \in \mathcal{L}. \tag{$**$}$$

Consider the vector $a := (a_1, \ldots, a_n)$, where $a_i := b_i$ for $i = 1, \ldots, n-1$ and $a_n := b_n + c_n$. Then, by Eq. $(**)$, $c - a \in \mathcal{L}$. Thus, $\widetilde{a} = \widetilde{c}$. For all the above, we get that a satisfies (i), (ii) and (iii).

Next, we show the uniqueness of a. Assume that there are vectors $a := (a_1, \ldots, a_n)$ and $a' := (a'_1, \ldots, a'_n)$ in $\mathbb{Z}^n$ that satisfy (i), (ii) and (iii). If $a_i \neq a'_i$ for some $1 \leq i \leq n-1$, then the binomial

$$h := t_1^{a_1} \cdots t_{n-1}^{a_{n-1}} t_n^{-a_n} - t_1^{a'_1} \cdots t_{n-1}^{a'_{n-1}} t_n^{-a'_n}$$

is non-zero and belongs to $I(\mathcal{L})$ because $a-a' \in \mathcal{L}$ by (iii), a contradiction because none of the two terms of h are in the initial ideal of $I(\mathcal{L})$ by (ii). Thus, $a_i = a_i'$ for $i = 1, \ldots, n-1$. Since $|a| = |a'|$, we get $a = a'$. $\Box$

Remark 2.6.10 A graded ideal I is a complete intersection if and only if I is generated by a homogeneous regular sequence with $\mathrm{ht}(I)$ elements (see Proposition 1.1.7 and Lemma 1.1.8).

Proposition 2.6.11 *If $L \subset S$ is a graded pure lattice ideal of dimension 1, then there are positive integers $m_1, \ldots, m_{n-1}$ such that*

(a) $L' := (t_1^{m_1} - t_n^{m_1}, \ldots, t_{n-1}^{m_{n-1}} - t_n^{m_{n-1}}) \subset L$,

(b) $\mathrm{reg}(S/(t_n, L)) \leq \mathrm{reg}(S/(t_n, L')) = \sum_{i=1}^{n-1}(m_i - 1) + 1$, *and*

(c) $H_L(d) = H_L(d-1) = \deg\, S/L$ *for* $d \geq \sum_{i=1}^{n-1}(m_i - 1) + 1$.

Proof. There is a regular sequence in L of length $ht(L) = n-1$, because S/L is C-M of dimension 1 from Lemma 2.6.5. By Lemma 2.6.7 there are positive integers $m_1, \ldots, m_{n-1}$ such that $m_i(e_i - e_n) \in \mathcal{L}$ for all i, thus L' is contained in L. Then $(L', t_n) = \left(t_1^{m_1}, \ldots, t_{n-1}^{m_{n-1}}, t_n\right)$ is a complete intersection and we have the result. $\Box$

We come to one of the main results of this section.

Theorem 2.6.12 *If $I(\mathcal{L}) \subset S$ is a graded pure lattice ideal of dimension 1, then*

$$\deg\, S/I(\mathcal{L}) = |T(\mathbb{Z}^n/\mathcal{L})|.$$

Proof. Let $\succ_{revlex}$ be the revlex order on the monomial of S and let $\mathrm{LT}(I(\mathcal{L}))$ be the initial ideal of $I(\mathcal{L})$. We set $d := \sum_{i=1}^{n-1}(m_i - 1) + 1$. By Proposition 2.6.11, there are positive integers $m_1, \ldots, m_{n-1}$ such that $t_i^{m_i} - t_n^{m_i} \in I(\mathcal{L})$ for all i and $H_{I(\mathcal{L})}(d) = \deg\, S/I(\mathcal{L})$. There is an injective map

$$\mathcal{M}_d := \{t^c |\, t^c \notin \mathrm{LT}(I(\mathcal{L}))\} \cap S_d \longrightarrow (S/I(\mathcal{L}))_d, \qquad t^c \mapsto t^c + I(\mathcal{L}).$$

By a classical result in Gröbner bases theory ([75, Proposition 1, pag 230]), the image of this map is a basis for the K-vector space $(S/I(\mathcal{L}))_d$. Thus, $|\mathcal{M}_d| = H_{I(\mathcal{L})}(d)$. Consider the map

$$\phi\colon \mathcal{M}_d \to T(\mathbb{Z}^n/\mathcal{L}), \quad t^c := t_1^{c_1} \cdots t_n^{c_n} \overset{\phi}{\longmapsto} (c_1, \ldots, c_{n-1}, c_n - d) + \mathcal{L}.$$

The map ϕ is well defined, i.e., $\phi(t^c)$ is in $T(\mathbb{Z}^n/\mathcal{L})$ for all t^c in $\mathcal{M}_d$. This follows directly from Lemma 2.6.7 (b) by noticing the equality

$$(c_1, \ldots, c_{n-1}, c_n - d) = c_1(e_1 - e_n) + \cdots + c_{n-1}(e_{n-1} - e_n).$$

Altogether, we need only show that ϕ is bijective. Notice that t_n^d maps to $\widetilde{0}$ under ϕ. By Lemma 2.6.9, the map ϕ is injective. To show that ϕ is onto, take $\widetilde{a} \in T(\mathbb{Z}^n/\mathcal{L})$. By Lemma 2.6.9, we may assume that $a_i \geq 0$ for $i = 1, \ldots, n-1$ and $t_1^{a_1} \cdots t_{n-1}^{a_{n-1}} \notin \mathrm{LT}(I(\mathcal{L}))$. Notice that $0 \leq a_i \leq m_i - 1$ for $i = 1, \ldots, n-1$ because $t_i^{m_i} - t_n^{m_i} \in I(\mathcal{L})$ for all i. Thus, $\sum_{i=1}^{n-1} a_i \leq \sum_{i=1}^{n-1}(m_i - 1) < d$. Consider the vector $c := (c_1, \ldots, c_n)$ given by $c_i := a_i$ for $i = 1, \ldots, n-1$ and $c_n := d - \sum_{i=1}^{n-1} a_i$. Then, the monomial t^c is in $\mathcal{M}_d$ and maps to $\widetilde{a}$ under the map ϕ. $\square$

Corollary 2.6.13 *If $I(\rho) \subset S$ is a graded lattice ideal of dimension 1, then*

$$\deg\, S/I(\rho) = |T(\mathbb{Z}^n/\mathcal{L}_\rho)|.$$

Proof. It follows by Corollary 2.5.3 and Theorem 2.6.12. $\square$

Corollary 2.6.14 *Let $\mathcal{L} \subset \mathbb{Z}^n$ be a homogeneous lattice of rank $n-1$ generated as a $\mathbb{Z}$-module by the rows of an integral matrix A. Then*

$$\deg S/I(\mathcal{L}) = d_1 \cdots d_{n-1},$$

where $d_1, \ldots, d_{n-1}$ are the invariant factors of A.

Proof. It is well known [92, Theorem II.9, pp. 26-27] that there are invertible integral matrices U and V such that

$$UAV = D := \mathrm{diag}\{d_1, \ldots, d_{n-1}, 0, \ldots, 0\},$$

$d_i > 0$ for $1 \leq i \leq n-1$ and d_i divides d_{i+1} for all i. In matrix theory terminology, this means that $D = \mathrm{diag}\{d_1, \ldots, d_{n-1}, 0, \ldots, 0\}$ is the *Smith normal form* of A and $d_1, \ldots, d_{n-1}$ are the *invariant factors* of A. Hence, by the fundamental structure theorem for finitely generated abelian groups [87, pp. 187-188], we get

$$\mathbb{Z}^n/\mathcal{L} \simeq \mathbb{Z}/(d_1) \oplus \cdots \oplus \mathbb{Z}/(d_{n-1}) \oplus \mathbb{Z} \;\text{ and }\; T(\mathbb{Z}^n/\mathcal{L}) \simeq \mathbb{Z}/(d_1) \oplus \cdots \oplus \mathbb{Z}/(d_{n-1}).$$

Thus, the result follows from Theorem 2.6.12. $\square$

Corollary 2.6.15 *Let $L \subset S$ be a graded pure lattice ideal of dimension 1. If L is generated by the binomials $t^{a_1^+} - t^{a_1^-}, \ldots, t^{a_m^+} - t^{a_m^-}$. Then*

$$\deg S/L = d_1 \cdots d_{n-1},$$

where $d_1, \ldots, d_{n-1}$ are the invariant factors of the matrix A whose rows are $a_1, \ldots, a_m$.

Proof. Let $\mathcal{L}$ be the homogeneous lattice that defines the pure lattice ideal L. By Theorem 2.2.9, one has the equality $\mathcal{L} = \mathbb{Z}a_1 + \cdots + \mathbb{Z}a_m$. Thus, the result follows at once from Corollary 2.6.14. $\square$

Lemma 2.6.16 [96, pp. 32-33] *If $M \subset M'$ are free abelian groups of the same rank d with $\mathbb{Z}$-bases $\delta_1, \ldots, \delta_d$ and $\gamma_1, \ldots, \gamma_d$ related by $\delta_i := \sum_j z_{ij}\gamma_j$, where $z_{ij} \in \mathbb{Z}$ for all i, j, then $|M'/M| = |\det(z_{ij})|$.*

Definition 2.6.17 Let $\mathcal{O}$ be a *lattice d-simplex* in $\mathbb{R}^n$, i.e., $\mathcal{O}$ is the convex hull of a set of $d+1$ affinely independent points in $\mathbb{Z}^n$. The *normalized volume* of $\mathcal{O}$ is defined as $d!\mathrm{vol}(\mathcal{O})$.

The next result shows that the degree is the normalized volume of any $(s-1)$-simplex arising from a $\mathbb{Z}$-basis of $\mathcal{L}$.

Corollary 2.6.18 *If $\mathcal{L} \subset \mathbb{Z}^n$ is a homogeneous lattice and $a_1, \ldots, a_{n-1}$ is a $\mathbb{Z}$-basis of $\mathcal{L}$, then*

$$\deg S/I(\mathcal{L}) = (n-1)!\mathrm{vol}(\mathrm{conv}(0, a_1, \ldots, a_{n-1})),$$

where vol *is the relative volume and* conv *is the convex hull.*

Proof. By hypothesis, $\mathcal{L} = \mathbb{Z}a_1 \oplus \cdots \oplus \mathbb{Z}a_{n-1}$. Hence, using Lemma 2.6.7 (b), we get the equality

$$T(\mathbb{Z}^n/\mathcal{L}) = \mathbb{Z}(e_1 - e_n) \oplus \cdots \oplus \mathbb{Z}(e_{n-1} - e_n)/\mathbb{Z}a_1 \oplus \cdots \oplus \mathbb{Z}a_{n-1}.$$

For $1 \leq i \leq n-1$, we can write $a_i = a_{i,1}(e_1 - e_n) + \cdots + a_{i,n-1}(e_{n-1} - e_n)$, where $a_{i,j}$ is the j^{th} entry of a_i. Applying Theorem 2.6.12 and Lemma 2.6.16 gives

$$\deg S/I(\mathcal{L}) = |T(\mathbb{Z}^n/\mathcal{L})| = \left|\det\begin{pmatrix} a_{1,1} & \cdots & a_{1,n-1} \\ \vdots & \vdots & \vdots \\ a_{n-1,1} & \ldots & a_{n-1,n-1} \end{pmatrix}\right| = (n-1!)\mathrm{vol}(\mathcal{O}),$$

where $\mathcal{O} := \mathrm{conv}(0, (a_{1,1}, \ldots, a_{1,n-1}), \ldots, (a_{n-1,1}, \ldots, a_{n-1,n-1}))$ is a simplex in $\mathbb{R}^{n-1}$. To finish the proof we need only show that $\mathrm{vol}(\mathcal{O}) = \mathrm{vol}(\mathrm{conv}(0, a_1, \ldots, a_{n-1}))$. This follows from the very definition of the notion of a relative volume (see [18, Section 2] and [95, p. 238]). □

Corollary 2.6.19 *Let $I(\mathcal{L}) \subset S$ be a graded pure lattice ideal of dimension 1. If $I(\mathcal{L})$ is a complete intersection generated by $t^{a_1^+} - t^{a_1^-}, \ldots, t^{a_{n-1}^+} - t^{a_{n-1}^-}$, then*

$$\deg S/I(\mathcal{L}) = (n-1)!\mathrm{vol}(\mathrm{conv}(0, a_1, \ldots, a_{n-1})).$$

Proof. By Theorem 2.2.9, one has the equality $\mathcal{L} = \mathbb{Z}a_1 \oplus \cdots \oplus \mathbb{Z}a_{n-1}$. Thus, the formula for the degree follows from Corollary 2.6.18. □

Corollary 2.6.20 *If $I(\mathcal{L}) \subset S$ is a graded lattice ideal of dimension 1, then $\mathbb{Z}^n/\mathcal{L}$ is torsion-free if and only if $I(\mathcal{L}) = (t_1 - t_n, \ldots, t_{n-1} - t_n)$.*

Proof. Assume that $\mathbb{Z}^n/\mathcal{L}$ is torsion-free. Then, by Lemma 2.6.7 b), one has the equality.

$$\mathcal{L} = \mathbb{Z}(e_1 - e_n) \oplus \cdots \oplus \mathbb{Z}(e_{n-1} - e_n).$$

Hence, $I(\mathcal{L}) = (t_1 - t_n, \ldots, t_{n-1} - t_n)$. The converse is clear because the $(n-1) \times n$ matrix with rows $e_1 - e_n, \ldots, e_{n-1} - e_n$ diagonalizes over the integers to an identity matrix. □

Examples

Given a set of generators of a homogeneous lattice $\mathcal{L} \subset \mathbb{Z}^n$, a standard method to compute the degree of the lattice ring $S/I(\mathcal{L})$ consists of two steps.

- First, one computes a generating set for $I(\mathcal{L})$ using Theorem 2.2.7: If $\mathcal{L} \subset \mathbb{Z}^n$ is a lattice generated by $a_1, \ldots, a_r$, then

$$((t^{a_1^+} - t^{a_1^-}, \ldots, t^{a_r^+} - t^{a_r^-})\colon (t_1 \cdots t_n)^\infty) = I(\mathcal{L}).$$

- Second, one uses Hilbert functions and Proposition 1.1.31 to compute the degree of $S/I(\mathcal{L})$. The handy command "degree" of *Macaulay*2 [61] computes the degree.

This standard method works for any homogeneous lattice. For homogeneous lattices of rank $n-1$, our method is far more efficient, especially with large examples.

Example 2.6.21 Let $\mathcal{L} \subset \mathbb{Z}^5$ be the homogeneous lattice of rank 4 generated by the rows of the matrix

$$A = \begin{pmatrix} 1001 & 500 & -501 & 0 & 0 \\ 0 & 3500 & -3500 & 0 & 0 \\ 0 & 0 & 3200 & -200 & -3000 \\ 5000 & -1000 & -1000 & -1001 & -1999 \end{pmatrix}.$$

The following procedure for *Maple* [64]

```
with(linalg);
A:=array([[1001,-500,-501,0,0],[0,3500,-3500,0,0],
[0,0,3200,-200,-3000],[5000,-1000,-1000,-1001,-1999]]);
ismith(A);
```

computes the Smith normal form of A:

$$D = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 100 & 0 & 0 \\ 0 & 0 & 0 & 56000 & 0 \end{pmatrix}.$$

Thus, by Theorem 2.6.12, we obtain $\deg S/I(\mathcal{L}) = (2^8)(5^5)(7)$. The standard procedure for computing the degree of $S/I(\mathcal{L})$ fails for this example. Indeed, *Macaulay*2 does not even computes the saturation $(I\colon h^\infty)$ of the ideal

$$I := (t_1^{1001} - t_2^{500}t_3^{501}, t_2^{3500} - t_3^{3500}, t_3^{3200} - t_4^{200}t_5^{3000}, t_1^{5000} - t_2^{1000}t_3^{1000}t_4^{1001}t_5^{1999})$$

with respect to $h = t_1t_2t_3t_4t_5$. Notice that I is a complete intersection and accordingly

$$\deg(S/I) = (1001)(3500)(3200)(5000) = (2^{12})(5^9)(7^2)(11)(13).$$

Remark 2.6.22 Given an integral matrix A, the *Macaulay2* [61] function "smithNormalFrom" produces a diagonal matrix D, and invertible matrices U and V such that $D = UAV$. Warning: even though this function is called the Smith normal form, it doesn't necessarily satisfy the more stringent condition that the diagonal entries $d_1, d_2, \ldots, d_m$ of D satisfy: $d_1|d_2|\cdots|d_m$. For this reason we prefer to use *Maple* [64] to compute the Smith normal form of A.

Example 2.6.23 Let $\mathcal{L} \subset \mathbb{Z}^3$ be the homogeneous lattice of rank 2 generated by the rows of the matrix

$$A = \begin{pmatrix} 18 & -18 & 0 \\ 45 & 0 & -45 \\ 0 & 10 & -10 \end{pmatrix}.$$

The following procedure for *Maple* [64]

```
with(linalg);
A:=array([[18,-18,0],[45,0,-45],[0,10,-10]]);
ismith(A);
```

computes the Smith normal form of A:

$$D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 90 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Thus, by Theorem 2.6.12, we obtain $\deg S/I(\mathcal{L}) = 90$. The standard procedure for computing the degree of $S/I(\mathcal{L})$ works fine in this "small" example. Indeed, using the following procedure for *Macaulay2*

```
S=QQ[t1,t2,t3]
I=ideal(t1^18-t2^18,t1^45-t3^45,t2^10-t3^10)
saturate(I,t1*t2*t3)
degree saturate(I,t1*t2*t3)
```

we obtain

$$I(\mathcal{L}) = I\colon (t_1t_2t_3)^\infty = (t_1^9 - t_2^4t_3^5, t_2^{10} - t_3^{10}) \text{ and } \deg(S/I(\mathcal{L})) = 90.$$

Remark 2.6.24 The program *Normaliz* [62] computes the *normalized volume* of lattice polytopes. Hence, by Corollary 2.6.18, we can use this program with the handy option `-v` to compute the degree. This of course requires to compute a $\mathbb{Z}$-basis of the lattice first. We computed the degree of Example 2.6.23 without any problem using "`normbig.exe`".

Our main result of Subsection 2.6.1, Theorem 2.6.12, does not extend to graded pure lattice ideals of dimension ≥ 2.

Example 2.6.25 Consider the homogeneous lattice $\mathcal{L} := \mathbb{Z}\{(-1, 2, -1)\} \subset \mathbb{Z}^3$. Then,

$$I(\mathcal{L}) = (t_2^2 - t_1t_3) \text{ and } \deg \mathbb{Q}[t_1, t_2, , t_3]/I(\mathcal{L}) = 2 \neq 1 = |T(\mathbb{Z}^3/\mathcal{L})|.$$

2.6.2 A complete intersection criterion

Let K be a field, $S := K[t_1, \ldots, t_n]$ a polynomial ring with n variables over K and $\mathcal{L}$ a lattice of $\mathbb{Z}^n$. In this section we work with a pure lattice ideal $L := I(\mathcal{L})$, i.e. we use the trivial partial character to define a lattice ideal. We do not consider arbitrary partial characters because in [44] it is proved that the complete intersection property of a lattice ideal is independent from the partial character. If L is ω-graded of dimension 1, we establish a complete intersection criterion in algebraic and geometric terms. If L is ω-graded of dimension 1, and K has positive characteristic, then we show that L is a pure binomial set theoretic complete intersection. If K has characteristic zero, we prove that in the set of pure lattice ideals the property binomial set theoretic complete intersection implies complete intersection.

Lemma 2.6.26 *Let I be a pure binomial ideal of S such that $V(I, t_i) = \{0\}$ for all i. If $\mathfrak{p}$ is a prime ideal containing (I, t_m) for some $1 \leq m \leq n$, then $\mathfrak{p} = (t_1, \ldots, t_n)$.*

Proof. Let $h_1, \ldots, h_r$ be a generating set for I consisting of pure binomials. For simplicity of notation assume that $m = 1$. We may assume that $t_1, \ldots, t_k$ are in $\mathfrak{p}$ and $t_i \notin \mathfrak{p}$ for $i > k$. If $t_i \in \operatorname{supp}(h_j)$ for some $1 \leq i \leq k$, say $h_j = t^{a_j} - t^{b_j}$ and $t_i \in \operatorname{supp}(t^{a_j})$, then $t^{b_j} \in \mathfrak{p}$ and there is $1 \leq \ell \leq k$ such that t_ℓ is in the support of t^{b_j}. Thus, $h_j \subset (t_1, \ldots, t_k)$. Hence, for each $1 \leq j \leq r$, either

(i) $\operatorname{supp}(h_j) \cap \{t_1, \ldots, t_k\} = \emptyset$ or

(ii) $h_j \in (t_1, \ldots, t_k)$.

Consider the point $c := (c_i) \in \mathbb{A}^n_K$, with $c_i := 0$ for $i \leq k$ and $c_i := 1$ for $i > k$. If (i) occurs, then $h_j(c) = (t^{a_j} - t^{b_j})(c) = 1 - 1 = 0$. If (ii) occurs, then $h_j(c) = (t^{a_j} - t^{b_j})(c) = 0 - 0 = 0$. Clearly the polynomial t_1 vanishes at c. Hence, $c \in V(I, t_1) = \{0\}$. Therefore, $k = n$. Thus, $\mathfrak{p}$ contains all the variables of S, i.e., $\mathfrak{p} = (t_1, \ldots, t_n)$. $\square$

Proposition 2.6.27 *Let $I \subset S$ be a ω-graded pure binomial ideal.*

(a) *If $V(I, t_i) = \{0\}$ for all i, then $\operatorname{ht}(I) = n - 1$.*

(b) *If I is a pure lattice ideal and $\operatorname{ht}(I) = n - 1$, then $V(I, t_i) = \{0\}$ for all i.*

Proof. (a) As I is ω-graded, all associated prime ideal of S/I are ω-graded. Thus, all associated prime ideals of S/I are contained in $\mathfrak{m} := (t_1, \ldots, t_n)$. If $\operatorname{ht}(I) = n$, then $\mathfrak{m}$ would be the only associated prime of S/I, that is, $\mathfrak{m}$ is the radical of I, a contradiction because I cannot contain a power of t_i for any i. Thus, $\operatorname{ht}(I) \leq n - 1$. On the other hand, by Lemma 2.6.26, the ideal (I, t_n) has height n. Hence, $n = \operatorname{ht}(I, t_n) \leq \operatorname{ht}(I) + 1$ (here we use the fact that I is ω-graded). Altogether, we get $\operatorname{ht}(I) = n - 1$.

(b) Let $\mathcal{L}$ be the lattice that defines I and let $g_1, \ldots, g_r$ be a generating set for I consisting of homogeneous pure binomials. By Theorem 2.2.9, one has the equality $\mathcal{L} =$

$\mathbb{Z}\{\widehat{g}_1,\ldots,\widehat{g}_r\}$. Notice that $n-1=\mathrm{ht}(I)=\mathrm{rank}(\mathcal{L})$. Given two distinct integers $1\le i,k\le n$, the vector space $\mathbb{Q}^n$ is generated by $e_k,\widehat{g}_1,\ldots,\widehat{g}_r$. Hence, as $\mathcal{L}$ is homogeneous with respect to $\omega:=(\omega_1,\ldots,\omega_n)$, there are positive integers r_i and r_k such that $r_ie_i-r_ke_k\in\mathcal{L}$ and $r_i\omega_i-r_k\omega_k=0$. By Lemma 2.2.5, there is t^δ such that $t^\delta(t_i^{r_i}-t_k^{r_k})$ is in I. Hence, by Theorem 2.1.23 (iii), $t_i^{r_i}-t_k^{r_k}$ is in I. Therefore, $V(I,t_i)=\{0\}$ for $i=1,\ldots,n$. $\Box$

Example 2.6.28 Let $S:=\mathbb{Q}[t_1,t_2,t_3]$. The ideal $I:=(t_1^2-t_2t_3,t_1^2-t_1t_2)$ has height 2 is not a pure lattice ideal and $V(I,t_1)\neq\{0\}$, that is, Proposition 2.6.27 (b) only holds for pure lattice ideals.

Recall that a ω-graded ideal I is a complete intersection if and only if I is generated by a homogeneous regular sequence with $\mathrm{ht}(I)$ elements (see [102, Proposition 1.3.17, Lemma 1.3.18]).

Lemma 2.6.29 *Let $I\subset S$ be a ω-graded pure binomial ideal. If $V(I,t_i)=\{0\}$ for all i and I is a complete intersection, then I is a pure lattice ideal.*

Proof. By Proposition 2.6.27 (a), the height of I is $n-1$. It suffices to prove that t_i is a non-zero divisor of S/I for all i (see Theorem 2.1.23 (iii)). If t_i is a zero divisor of S/I for some i, there is an associated prime ideal $\mathfrak{p}$ of S/I containing (I,t_i). Hence, using Lemma 2.6.26, we get that $\mathfrak{p}=\mathfrak{m}$, a contradiction because I is a complete intersection of height $n-1$ and all associated prime ideals of I have height equal to $n-1$ (see [102, Proposition 1.3.22]). $\Box$

Example 2.6.30 Let $S:=\mathbb{Q}[t_1,t_2,t_3]$. The ideal $I:=(t_1^2-t_2t_3,t_2^2-t_3^2)$ has height 2 and $V(I,t_i)=\{0\}$ for all i. Thus, by Lemma 2.6.29, I is a pure lattice ideal.

We come to one of the main results of this subsection.

Theorem 2.6.31 *Let L be the pure lattice ideal of an ω-homogeneous lattice $\mathcal{L}$ in $\mathbb{Z}^n$. If $V(L,t_i)=\{0\}$ for all i, then L is a complete intersection if and only if there are homogeneous pure binomials $h_1,\ldots,h_{n-1}$ in L satisfying the following conditions*:

(i) $\mathcal{L}=\mathbb{Z}\left\{\widehat{h}_1,\ldots,\widehat{h}_{n-1}\right\}$.

(ii) $V(h_1,\ldots,h_{n-1},t_i)=\{0\}$ *for all* i.

(iii) $h_i=t^{a_i^+}-t^{a_i^-}$ *for* $i=1,\ldots,n-1$.

Proof. As $\mathcal{L}$ is ω-homogeneous, its pure lattice ideal L is graded with respect to the grading of S induced by setting $\deg(t_i):=\omega_i$ for $i=1,\ldots,n$ (Remark 2.6.4). By Proposition 2.6.27, the height of L is $n-1$.

($\Rightarrow$) Since L is a ω-graded pure binomial ideal which is a complete intersection, it is well known that L is an ideal generated by homogeneous pure binomials $h_1,\ldots,h_{n-1}$ (see for instance [102, Lemma 2.2.16]). Then, by Theorem 2.1.23 and Theorem 2.2.9 (iii), we have (i) and (iii) hold. From the equality $(L, t_i) = (h_1, \ldots, h_{n-1}, t_i)$, we get

$$\{0\} = V(L, t_i) = V(h_1, \ldots, h_{n-1}, t_i).$$

Thus, $V(h_1, \ldots, h_{n-1}, t_i) = \{0\}$ for all i, i.e., (ii) holds.

($\Leftarrow$) We set $I := (h_1, \ldots, h_{n-1})$. By hypothesis $I \subset L$. Thus, we need only to show the inclusion $L \subset I$. Let $g_1, \ldots, g_m$ be a generating set of L consisting of pure binomials, then $\widehat{g}_i \in \mathcal{L}$ for all i. Using condition (i) and Lemma 2.2.5, for each i there is a monomial t^{γ_i} such that $t^{\gamma_i} g_i \in I$. Hence, $t^{\gamma} L \subset I$, where t^{γ} is equal to $t^{\gamma_1} \cdots t^{\gamma_m}$. By (ii) and Proposition 2.6.27, the height of I is $n-1$. This means that I is a complete intersection. As $t^{\gamma} L \subset I$, to show the inclusion $L \subset I$, it suffices to notice that by (ii), Lemma 2.6.29 and Theorem 2.1.23 (iii) t_i is a non-zero divisor of S/I for all i. □

Remark 2.6.32 The result remains valid if we remove condition (iii), i.e., condition (iii) is redundant. In both implications of the theorem the set $h_1, \ldots, h_{n-1}$ is shown to generate L.

Definition 2.6.33 An ideal I is called a *(pure) binomial set theoretic complete intersection* if there are (pure) binomials $g_1, \ldots, g_r$ such that $\mathrm{rad}(I) = \mathrm{rad}(g_1, \ldots, g_r)$, where r is the height of I.

The next result gives a family of binomial set theoretic complete intersections. We show this result using a theorem of Katsabekis, Morales and Thoma [34, Theorem 4.4(2)].

Proposition 2.6.34 *If K is a field of positive characteristic and $L \subset S$ is a ω-graded pure lattice ideal of dimension 1, then L is a pure binomial set theoretic complete intersection.*

Proof. Let $\mathcal{L}$ be the ω-homogeneous lattice of $\mathbb{Z}^n$ such that $L = I(\mathcal{L})$. Notice that $\mathcal{L}$ is a lattice of rank $n-1$ because $\mathrm{ht}(L) = \mathrm{rank}(\mathcal{L})$. Thus, there is an isomorphism of groups $\psi\colon \mathbb{Z}^n/\mathrm{Sat}(\mathcal{L}) \to \mathbb{Z}$, where $\mathrm{Sat}(\mathcal{L})$ is the saturation of $\mathcal{L}$ consisting of all $a \in \mathbb{Z}^n$ such that $da \in \mathcal{L}$ for some $0 \neq d \in \mathbb{Z}$. For each $1 \leq i \leq n$, we set $a_i := \psi(e_i + \mathrm{Sat}(\mathcal{L}))$, where e_i is the ith unit vector in $\mathbb{Z}^n$. Following [34], the multiset $A := \{a_1, \ldots, a_n\}$ is called the configuration of vectors associated to $\mathcal{L}$. Recall that $s - 1 = \mathrm{rank}(\mathcal{L})$. Hence, as $\mathcal{L}$ is homogeneous with respect to $\omega := (\omega_1, \ldots, \omega_n)$, there are positive integers r_i and r_k such that $r_i e_i - r_k e_k \in \mathcal{L}$ and $r_i \omega_i - r_k \omega_k = 0$. Thus, $r_i a_i = r_k a_k$ and a_i has the same sign as a_k. This means that $a_1, \ldots, a_n$ are all positive or all negative. It follows that A is a full configuration in the sense of [34, Definition 4.3]. Thus, $I(\mathcal{L})$ is a binomial set theoretic complete intersection by [34, Theorem 4.4(2)] and its proof. □

Corollary 2.6.35 [6] *If $P \subset S$ is the toric ideal of a monomial curve, then P is a complete intersection if and only if there are homogeneous pure binomials $g_1, \ldots, g_{n-1}$ in P, with $g_i = t^{a_i^+} - t^{a_i^-}$ for all i, such that the following conditions hold:*

(a) $\mathcal{L}_1 = \mathbb{Z}\{\widehat{g}_1, \ldots, \widehat{g}_{n-1}\}$, *where* $\mathcal{L}_1$ *is the lattice that defines* P.

(b) $V(g_1, \ldots, g_{n-1}, t_i) = \{0\}$ *for* $i = 1, \ldots, n$.

Proof. There are positive integers $\omega_1, \ldots, \omega_n$ such that P is the kernel of the epimorphism of K-algebras:

$$\varphi\colon K[t_1, \ldots, t_n] \longrightarrow K[y_1^{\omega_1}, \ldots, y_1^{\omega_n}], \qquad f \overset{\varphi}{\longmapsto} f(y_1^{\omega_1}, \ldots, y_1^{\omega_n}),$$

where y_1 is a new variable. Consider the homomorphism of $\mathbb{Z}$-modules $\psi\colon \mathbb{Z}^n \to \mathbb{Z}$, $e_i \mapsto \omega_i$. According to [102, Corollary 7.1.4], the toric ideal P is the pure lattice ideal of the homogeneous lattice $\mathcal{L}_1 := \ker(\psi)$ with respect to the vector $\omega := (\omega_1, \ldots, \omega_n)$, that is $P = I(\mathcal{L}_1)$. In particular the height of P is $n-1$. The binomial $t_i^{\omega_j} - t_j^{\omega_i}$ is in P for all i, j. Thus, $V(I(\mathcal{L}_1), t_i) = \{0\}$ for all i. Then, the result follows from Theorem 2.6.31. $\Box$

Corollary 2.6.36 [43] *Let* $P \subset S$ *be the toric ideal of a monomial curve. If* $\operatorname{char}(K) > 0$*, then* P *is a binomial set theoretic complete intersection.*

Proof. As seen in the proof of Corollary 2.6.35, P is a 1-dimensional ω-graded pure lattice ideal. Thus, the result follows at once from Proposition 2.6.34. $\Box$

We come to another of our main results of this subsection.

Theorem 2.6.37 *Let* $L \subset S$ *be an arbitrary pure lattice ideal of height* r. *If* $\operatorname{char}(K) = 0$ *and* $\operatorname{rad}(L) = \operatorname{rad}(g_1, \ldots, g_r)$ *for some pure binomials* $g_1, \ldots, g_r$, *then* $L = (g_1, \ldots, g_r)$.

Proof. Consider the pure binomial ideal $I := (g_1, \ldots, g_r)$, where $g_i := t^{a_i} - t^{b_i}$ for $i = 1, \ldots, r$. Since $\operatorname{rad}(I)$ is again a pure binomial ideal (see [84, Theorem 9.4 and Corollary 9.12]), we may assume that $\operatorname{rad}(I)$ is generated by a set of pure binomials $\{h_1, \ldots, h_m\}$. From [84, Corollary 9.12, p. 106], it is seen that any lattice ideal over a field K of characteristic zero is radical, i.e., $\operatorname{rad}(L) = L$. Let

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_p \tag{2.6.1}$$

be a primary decomposition of I. Since I is an ideal of height r generated by r elements and S is Cohen-Macaulay, by the unmixedness theorem [73, Theorem 2.1.6], I has no embedded primes. Hence, $\operatorname{rad}(\mathfrak{q}_i) = \mathfrak{p}_i$ is a minimal prime of both I and L for $i = 1, \ldots, p$. Since $\operatorname{char}(K) = 0$, by [6, Lemma 2.2], we have the equality

$$\mathbb{Z}\{\widehat{g}_1, \ldots, \widehat{g}_r\} = \mathbb{Z}\left\{\widehat{h}_1, \ldots, \widehat{h}_m\right\}. \tag{2.6.2}$$

The inclusion $I \subset L$ is clear. We now show the reverse inclusion. Take a pure binomial h in L. Since L is generated by $h_1, \ldots, h_m$, by Theorem 2.2.9, the lattice that defines L is $\mathbb{Z}\left\{\widehat{h}_1, \ldots, \widehat{h}_m\right\}$. Therefore, using Eq. (2.6.2) and Lemma 2.2.5, we get that there is a monomial t^δ so that $t^\delta h \in I$. Thus, by Eq. (2.6.1), $t^\delta h \in \mathfrak{q}_i$ for all i. If $t^\delta = 1$, then $h \in I$

and there is nothing to prove. Assume that $t^\delta \neq 1$. It suffices to prove that h belongs to $\mathfrak{q}_i$ for all i. If $h \notin \mathfrak{q}_i$ for some i, then $(t^\delta)^\ell \in \mathfrak{q}_i$ and consequently $\mathfrak{p}_i$ must contain at least one variable t_k. Since $\mathfrak{p}_i$ is a minimal prime of L, all its elements are zero divisors of S/L. In particular t_k must be a zero divisor of S/L, a contradiction because L is a pure lattice ideal and none of the variables of S can be a zero divisor of S/L (see Theorem 2.1.23 (iii)). $\square$

As a consequence, we recover the following result.

Corollary 2.6.38 [2] *Let $P \subset S$ be an arbitrary toric ideal of height r. If* $\mathrm{char}(K) = 0$ *and $P = \mathrm{rad}(g_1, \ldots, g_r)$ for some pure binomials $g_1, \ldots, g_r$, then $P = (g_1, \ldots, g_r)$.*

2.6.3 Vanishing ideals over finite fields

Let $K := \mathbb{F}_q$ be a finite field with q elements, $S := K[t_1, \ldots, t_n] = \oplus_{d=0}^{\infty} S_d$ a polynomial ring over the field K with the standard grading, $v_1, \ldots, v_n$ a sequence of vectors in $\mathbb{N}^s$ and

$$\mathcal{Q} := \{[(x_1^{v_{11}} \cdots x_s^{v_{1s}}, \ldots, x_1^{v_{n1}} \cdots x_s^{v_{ns}})] \,|\, x_i \in K^* \text{ for all } i\} \subset \mathbb{P}^{n-1},$$

the projective algebraic toric set parameterized by the vectors $v_1, \ldots, v_n$ on $\mathbb{P}^{n-1}$. In this subsection we study the degree and a pair of complete intersection criterions of the vanishing ideal of $\mathcal{Q}$, $I(\mathcal{Q})$. This ideal has very important consequences in mathematics, for instance in coding theory, as we will see in Chapters 3 and 4. The following lemma and theorem show that the results about graded pure lattice ideals of dimension 1 proved in Subsections 2.6.1 and 2.6.2 can be applied to the ideal $I(\mathcal{Q})$.

Lemma 2.6.39 *If K is a finite field, then there is a unique homogeneous lattice such that $I(\mathcal{Q}) = I(\mathcal{L})$.*

Proof. By [49, Theorem 2.1], $I(\mathcal{Q})$ is a pure lattice ideal generated by homogeneous binomials. Let $\mathcal{L}$ be a homogeneous lattice that defines $I(\mathcal{Q})$. The uniqueness of $\mathcal{L}$ follows from Theorem 2.2.9. $\square$

Theorem 2.6.40 *If K is a finite field, then*

(a) [21] *$I(\mathcal{Q})$ is a radical 1-dimensional Cohen-Macaulay ideal.*

(b) [86, Lecture 13] *$H_{I(\mathcal{Q})}(d) = |\mathcal{Q}|$ for $d \geq |\mathcal{Q}| - 1$.*

Hence, by (b), the degree of $S/I(\mathcal{Q})$ is equal to $|\mathcal{Q}|$. Thus, our results can be used to compute $|\mathcal{Q}|$, especially in cases where the homogeneous lattice that defines the ideal $I(\mathcal{Q})$ is known (see for instance [49, Theorem 2.5] for such cases).

Let $\mathcal{L}$ be the homogeneous lattice that defines $I(\mathcal{Q})$. The next result shows how the algebraic structure of $\mathbb{Z}^n/\mathcal{L}$ is reflected in the algebraic structure of $I(\mathcal{Q})$.

Corollary 2.6.41 *If $q-1$ is a prime number such that $v_i \not\equiv v_j \mod (q-1)$ for $i \neq j$ and $T(\mathbb{Z}^n/\mathcal{L}) \simeq (\mathbb{Z}_{q-1})^{n-1}$, then $I(\mathcal{Q})$ is a complete intersection if and only if*

$$I(\mathcal{Q}) = (t_1^{q-1} - t_n^{q-1}, \ldots, t_{n-1}^{q-1} - t_n^{q-1}).$$

Proof. Assume that $I(\mathcal{Q})$ is a complete intersection, i.e., the ideal $I(\mathcal{Q})$ is generated by homogeneous pure binomials $f_1, \ldots, f_{n-1}$ of degrees $\delta_1, \ldots, \delta_{n-1}$. The linear binomial $t_i - t_j$ is not in $I(\mathcal{Q})$ for any $i \neq j$, this follows using that $v_i \not\equiv v_j \mod (q-1)$. Thus, $\deg(f_i) = \delta_i \geq 2$ for all i. By Theorem 2.6.12, we have

$$\deg S/I(\mathcal{Q}) = (q-1)^{n-1} = \delta_1 \cdots \delta_{s-1}.$$

As $q-1$ is prime, we get that $\delta_i = q-1$ for all i. Consider the K-vector spaces

$$V = K(t_1^{q-1} - t_n^{q-1}) + \cdots + K(t_{n-1}^{q-1} - t_n^{q-1}) \ \text{ and } \ I(\mathcal{Q})_{q-1} = Kf_1 + \cdots + Kf_{n-1}.$$

It suffices to show the equality $V = I(\mathcal{Q})_{q-1}$. Since $t_i^{q-1} - t_n^{q-1}$ vanishes at all point of $\mathcal{Q}$ for all i, we get that $t_i^{q-1} - t_n^{q-1} \in I(\mathcal{Q})_{q-1}$ for all i. Consequently $V = I(\mathcal{Q})_{q-1}$ because V and $I(\mathcal{Q})_{q-1}$ have the same dimension. The converse is clear because $t_1^{q-1} - t_n^{q-1}, \ldots, t_{n-1}^{q-1} - t_n^{q-1}$ form a regular sequence and the height of $I(\mathcal{Q})$ is $n-1$. $\square$

The complete intersection property of $I(\mathcal{Q})$ is partial characterized in the next results (see also [55]). If $\mathcal{Q}$ is parameterized by the edges of a clutter, then $I(\mathcal{Q})$ is a complete intersection if and only if $\mathcal{Q}$ is a projective torus [54].

Corollary 2.6.42 *If K is a finite field, then $I(\mathcal{Q})$ is a complete intersection if and only if there are homogeneous pure binomials $h_1, \ldots, h_{n-1}$ in $I(\mathcal{Q})$ such that the following conditions hold*:

(i) $\mathcal{L} = \mathbb{Z}\left\{\widehat{h}_1, \ldots, \widehat{h}_{n-1}\right\}$, *where $\mathcal{L}$ is the lattice that defines $I(\mathcal{Q})$.*

(ii) $V(h_1, \ldots, h_{n-1}, t_i) = \{0\}$ *for $i = 1, \ldots, n$.*

(iii) $h_i = t^{a_i^+} - t^{a_i^-}$ *for $i = 1, \ldots, n-1$.*

Proof. By Lemma 2.6.39 or Theorem 2.6.40, there is a unique homogeneous lattice $\mathcal{L}$ with respect to the vector $\omega := \mathbf{1}$ such that $I(\mathcal{Q}) = I(\mathcal{L})$. The binomial $t_i^{q-1} - t_j^{q-1}$ is in $I(\mathcal{Q})$ for all i, j. Thus, $V(I(\mathcal{L}), t_i) = \{0\}$ for all i. Therefore the result follows from Theorem 2.6.31. $\square$

Corollary 2.6.43 *If K is a finite field, then $I(\mathcal{Q})$ is a pure binomial set theoretic complete intersection.*

Proof. $I(\mathcal{Q})$ is a 1-dimensional ω-graded pure lattice ideal [21, 49]. Thus, the result follows at once from Proposition 2.6.34. $\square$

2.7 Vanishing ideals on projective degenerate tori over finite fields

Let $K := \mathbb{F}_q$ be a finite field with q elements, $S := K[t_1, \ldots, t_n]$ a polynomial ring over the field $K, v := \{v_1, \ldots, v_n\}$ a sequence of positive integers and

$$\mathcal{T} := \{[(x_1^{v_1}, \ldots, x_n^{v_n})] \,|\, x_i \in K^* \text{ for all } i\} \subset \mathbb{P}^{n-1},$$

the projective degenerate torus of type v on $\mathbb{P}^{n-1}$. In this section we study a complete intersection property, the index of regularity and the degree of the vanishing ideal of $\mathcal{T}$, $I(\mathcal{T})$. This ideal has very important consequences in mathematics, for instance in coding theory, as we will see in Chapters 3 and 4. In what follows β denotes a generator of the cyclic group $(K^*, \cdot)$, d_i denotes $o(\beta^{v_i})$, the order of β^{v_i} for $i = 1, \ldots, n$, and $\mathcal{S}$ denotes the semigroup $\mathbb{N}d_1 + \cdots + \mathbb{N}d_n$. If $d_1, \ldots, d_n$ are relatively prime, $\mathcal{S}$ is called a *numerical semigroup*. We will see below that the algebra of $I(\mathcal{T})$ is closely related to the algebra of the toric ideal of the semigroup ring

$$K[\mathcal{S}] := K[y_1^{d_1}, \ldots, y_1^{d_n}] \subset K[y_1],$$

where $K[y_1]$ is a polynomial ring. Recall that the toric ideal of $K[\mathcal{S}]$, denoted by P, is the kernel of the following epimorphism of K-algebras

$$\varphi\colon S := K[t_1, \ldots, t_n] \longrightarrow K[\mathcal{S}], \qquad f \overset{\varphi}{\longmapsto} f(y_1^{d_1}, \ldots, y_1^{d_n}).$$

Thus, $S/P \simeq K[\mathcal{S}]$. Since $K[y_1]$ is integral over $K[\mathcal{S}]$ we have $\mathrm{ht}(P) = n - 1$. The ideal P is graded if one gives degree d_i to variable t_i. The most well-known properties that P and $I(\mathcal{T})$ have in common is that both are Cohen-Macaulay graded pure lattice ideals of dimension 1 [30, 49]. At the end of the section we also give a way to compute the ideal $I(\mathcal{T})$ in terms of the d_i's and a saturation with respect to the monomial $t_1 \cdots t_n$.

Remark 2.7.1 By Definition 1.1.1 an ideal $I \subset S$ is called a *complete intersection* if there exist $f_1, \ldots, f_r$ in S such that $I = (f_1, \ldots, f_r)$, where r is the height of I. If I is a graded binomial ideal, then I is a complete intersection if and only if I is generated by a set of homogeneous binomials $g_1, \ldots, g_r$, and any such set of homogeneous generators is already a regular sequence (see [102, Proposition 1.3.17, Lemma 1.3.18]).

Lemma 2.7.2 *Let $S := K[t_1, \ldots, t_n]$ be a polynomial ring with the standard grading. If I is a graded ideal of S generated by a homogeneous regular sequence $f_1, \ldots, f_{n-1}$, then*

$$\mathrm{reg}(S/I) = \sum_{i=1}^{n-1} (\deg(f_i) - 1) \quad \textit{and} \quad \deg(S/I) = \deg(f_1) \cdots \deg(f_{n-1}).$$

Proof. We set $\delta_i := \deg(f_i)$. By [102, p. 104], the Hilbert series of S/I is given by

$$F_I(t) = \frac{\prod_{i=1}^{n-1}\left(1-t^{\delta_i}\right)}{(1-t)^n} = \frac{\prod_{i=1}^{n-1}(1+t+\cdots+t^{\delta_i-1})}{(1-t)}. \qquad (2.7.1)$$

Thus, by Proposition 1.1.31, $\operatorname{reg}(S/I) = \sum_{i=1}^{n-1}(\delta_i - 1)$ and $\deg(S/I) = \delta_1 \cdots \delta_{n-1}$. $\square$

Let D be the non-singular matrix $D := \operatorname{diag}(d_1, \ldots, d_n)$. Consider the homomorphisms of $\mathbb{Z}$-modules:

$$\psi\colon \mathbb{Z}^n \to \mathbb{Z}, \qquad e_i \mapsto d_i,$$
$$D\colon \mathbb{Z}^n \to \mathbb{Z}^n, \qquad e_i \mapsto d_i e_i.$$

If $c := (c_i) \in \mathbb{R}^n$, we set $|c| := \sum_{i=1}^n c_i$. Notice that $|D(c)| = \psi(c)$ for any $c \in \mathbb{Z}^n$. There are two homogeneous lattices that will play a role here:

$$\mathcal{L}_1 := \ker(\psi) \ \text{ and } \mathcal{L} := D(\ker(\psi)).$$

The map D induces a $\mathbb{Z}$-isomorphism between $\mathcal{L}_1$ and $\mathcal{L}$. It is well known [102] that the toric ideal P is the pure lattice ideal of $\mathcal{L}_1$. Below, we show that $I(\mathcal{T})$ is the pure lattice ideal of $\mathcal{L}$.

Lemma 2.7.3 *The map $t^a - t^b \mapsto t^{D(a)} - t^{D(b)}$ induces a bijection between the binomials $t^a - t^b$ of P whose terms t^a, t^b have disjoint support and the binomials $t^{a'} - t^{b'}$ of $I(\mathcal{T})$ whose terms $t^{a'}$, $t^{b'}$ have disjoint support.*

Proof. If $f := t^a - t^b$ is a binomial of P whose terms have disjoint support, then $a - b \in \mathcal{L}_1$ and the terms of $g := t^{D(a)} - t^{D(b)}$ have disjoint support because

$$\operatorname{supp}(t^a) = \operatorname{supp}(t^{D(a)}) \ \text{ and } \ \operatorname{supp}(t^b) = \operatorname{supp}(t^{D(b)}).$$

Thus, $|D(a)| = \psi(a) = \psi(b) = |D(b)|$. This means that $g = t^{D(a)} - t^{D(b)}$ is homogeneous in the standard grading of S. As $(\beta^{v_i})^{d_i} = 1$ for all i, it is seen that g vanishes at all points of $\mathcal{T}$. Hence, $g \in I(\mathcal{T})$ and the map is well defined.

The map is clearly injective. To show that the map is onto, take a binomial $f' := t^{a'} - t^{b'}$ in $I(\mathcal{T})$ with $a' := (a_i')$, $b' := (b_i')$ and such that $t^{a'}$ and $t^{b'}$ have disjoint support. Then, $(\beta^{v_i})^{a_i' - b_i'} = 1$ for all i because f' vanishes at all points of $\mathcal{T}$. Hence, since the order of β^{v_i} is d_i, there are integers $c_1, \ldots, c_n$ such that $a_i' - b_i' = c_i d_i$ for all i. Since f' is homogeneous, one has $|a'| = |b'|$. It follows readily that $c \in \mathcal{L}_1$ and $a' - b' = D(c)$. We can write $c = c^+ - c^-$. As a' and b' have disjoint support, we get $a' = D(c^+)$ and $b' = D(c^-)$. Thus, the binomial $t^{c^+} - t^{c^-}$ is in P and maps to $t^{a'} - t^{b'}$. $\square$

Proposition 2.7.4 $P = I(\mathcal{L}_1)$ *and* $I(\mathcal{T}) = I(\mathcal{L})$.

Proof. As mentioned above, the first equality is well known [102]. Since $I(\mathcal{T})$ is a pure lattice ideal [49], it is generated by binomials of the form $t^{a^+}-t^{a^-}$ (this follows using that t_i is a non-zero divisor of $S/I(\mathcal{T})$ for all i). To show the second equality, take $t^{a^+}-t^{a^-}$ in $I(\mathcal{T})$. Then, by Lemma 2.7.3, $a^+-a^-\in\mathcal{L}$ and $t^{a^+}-t^{a^-}$ is in $I(\mathcal{L})$. Thus, $I(\mathcal{T})\subset I(\mathcal{L})$. Conversely, take $f:=t^{a^+}-t^{a^-}$ in $I(\mathcal{L})$ with a^+-a^- in $\mathcal{L}$. Then, there is $c\in\mathcal{L}_1$ such that $a^+-a^-=D(c^+-c^-)$. Then, $t^{c^+}-t^{c^-}$ is in P and maps, under the map of Lemma 2.7.3, to f. Thus, $f\in I(\mathcal{T})$. This proves that $I(\mathcal{L})\subset I(\mathcal{T})$. $\square$

Proposition 2.7.5 *If $P=(\{t^{a_i}-t^{b_i}\}_{i=1}^m)$, then $I(\mathcal{T})=(\{t^{D(a_i)}-t^{D(b_i)}\}_{i=1}^m)$.*

Proof. We set $g_i:=t^{a_i}-t^{b_i}$ and $h_i:=t^{D(a_i)}-t^{D(b_i)}$ for $i=1,\ldots,n$. Notice that h_i is equal to $g_i(t^{d_1},\ldots,t^{d_n})$, the evaluation of g_i at $(t_1^{d_1},\ldots,t_n^{d_n})$. By Lemma 2.7.3, one has the inclusion $(h_1,\ldots,h_m)\subset I(\mathcal{T})$. To show the reverse inclusion take a binomial $0\neq f\in I(\mathcal{T})$. We may assume that $f=t^{a^+}-t^{a^-}$. Then, by Lemma 2.7.3, there is $g:=t^{c^+}-t^{c^-}$ in P such that $f=t^{D(c^+)}-t^{D(c^-)}$. By hypothesis we can write $g=\sum_{i=1}^m f_ig_i$ for some $f_1,\ldots,f_m$ in S. Then, evaluating both sides of this equality at $(t_1^{d_1},\ldots,t_n^{d_n})$, we get

$$f=t^{D(c^+)}-t^{D(c^-)}=g(t_1^{d_1},\ldots,t_n^{d_n})=\sum_{i=1}^m f_i(t_1^{d_1},\ldots,t_n^{d_n})g_i(t_1^{d_1},\ldots,t_n^{d_n})=\sum_{i=1}^m f_i'h_i,$$

where $f_i':=f_i(t_1^{d_1},\ldots,t_n^{d_n})$ for all i. Then, $f\in(h_1,\ldots,h_m)$. $\square$

Corollary 2.7.6 *If $n=3$, then $I(\mathcal{T})$ is minimally generated by at most 3 binomials.*

Proof. By a classical theorem of Herzog [30], P is generated by at most 3 binomials. Hence, by Proposition 2.7.5, $I(\mathcal{T})$ is generated by at most 3 binomials. $\square$

Given a subset $I\subset S$, recall that its variety, denoted by $V(I)$, is the set of all $a\in\mathbb{A}_K^n$ such that $f(a)=0$ for all $f\in I$, where $\mathbb{A}_K^n$ is the affine space over K. Given a binomial $g:=t^a-t^b$, we set $\widehat{g}:=a-b$. If $\mathcal{A}$ is a subset of $\mathbb{Z}^n$, $\mathbb{Z}\mathcal{A}$ denotes the subgroup of $\mathbb{Z}^n$ generated by $\mathcal{A}$.

Proposition 2.7.7 [6, Proposition 2.5] *Let $\mathcal{B}:=\{g_1,\ldots,g_{n-1}\}$ be a set of binomials in P. Then, $P=(\mathcal{B})$ if and only if the following two conditions hold*:

(i′) $\mathcal{L}_1=\mathbb{Z}\{\widehat{g}_1,\ldots,\widehat{g}_{n-1}\}$, *where* $\mathcal{L}_1:=\ker(\psi)$.

(ii′) $V(g_1,\ldots,g_{n-1},t_i)=\{0\}$ *for* $i=1,\ldots,n$.

We come to one of the main results of this section.

Theorem 2.7.8 (a) *If $I(\mathcal{T})$ is a complete intersection generated by binomials $h_1,\ldots,h_{n-1}$, then P is a complete intersection generated by binomials $g_1,\ldots,g_{n-1}$ such that h_i is equal to $g_i(t_1^{d_1},\ldots,t_n^{d_n})$ for all i.* (b) *If P is a complete intersection generated by binomials $g_1,\ldots,g_{n-1}$, then $I(\mathcal{T})$ is a complete intersection generated by binomials $h_1,\ldots,h_{n-1}$, where h_i is equal to $g_i(t_1^{d_1},\ldots,t_n^{d_n})$ for all i.*

Proof. (a) Since t_k is a non-zero divisor of $S/I(\mathcal{T})$ for all k, it is not hard to see that the monomials of h_i have disjoint support for all i, i.e., we can write $h_i = t^{a_i^+} - t^{a_i^-}$ for $i = 1, \ldots, n-1$. We claim that the following two conditions hold.

(i) $\mathcal{L} = \mathbb{Z}\{a_1, \ldots, a_{n-1}\}$, where $a_i := a_i^+ - a_i^-$ and $\mathcal{L}$ is the lattice that defines $I(\mathcal{T})$.

(ii) $V(h_1, \ldots, h_{n-1}, t_i) = \{0\}$ for $i = 1, \ldots, n$.

As $I(\mathcal{T})$ is generated by $h_1, \ldots, h_{n-1}$, by [39, Lemma 2.5], condition (i) holds. The binomial $t_i^{q-1} - t_n^{q-1}$ is in $I(\mathcal{T})$ for all i because $\mathbb{F}_q^*$ is a group of order $q-1$. Thus, $V(I(\mathcal{T}), t_i) = \{0\}$ for all i. From the equality $(h_1, \ldots, h_{n-1}, t_i) = (I(\mathcal{T}), t_i)$, we get

$$V(h_1, \ldots, h_{n-1}, t_i) = V(I(\mathcal{T}), t_i) = \{0\}.$$

Thus, (ii) holds. This completes the proof of the claim.

By (i) and Proposition 2.7.4, there are $b_1, \ldots, b_{n-1}$ in $\mathcal{L}_1 := \ker(\psi)$ such that $a_i := D(b_i)$ for all i. Accordingly $a_i^+ = D(b_i^+)$ and $a_i^- = D(b_i^-)$ for all i. We set $g_i := t^{b_i^+} - t^{b_i^-}$ for all i. Clearly, all the g_i's are in P and h_i is equal to $g_i(t_1^{d_1}, \ldots, t_n^{d_n})$ for all i. Next, we prove that P is generated by $g_1, \ldots, g_{n-1}$. By Proposition 2.7.7 it suffices to show that the following two conditions hold:

(i′) $\mathcal{L}_1 = \mathbb{Z}\{b_1, \ldots, b_{n-1}\}$, where $\mathcal{L}_1 := \ker(\psi)$.

(ii′) $V(g_1, \ldots, g_{n-1}, t_i) = \{0\}$ for $i = 1, \ldots, n$.

First we show (i′). Since $b_1, \ldots, b_{n-1}$ are in $\mathcal{L}_1$, we need only show the inclusion ($\subseteq$). Take $\gamma \in \ker(\psi)$, then $D(\gamma) \in \mathcal{L}$, and by (i) it follows that $\gamma \in \mathbb{Z}\{b_1, \ldots, b_{n-1}\}$.

Next we show (ii′). For simplicity of notation, we may assume that $i = n$. Take c in the variety $V(g_1, \ldots, g_{n-1}, t_n)$ and write $c := (c_1, \ldots, c_n)$. Then, $c_n = 0$ and $g_i(c) = c^{b_i^+} - c^{b_i^-} = 0$ for all i, were $c^{b_i^+}$ means to evaluate the monomial $t^{b_i^+}$ at the point c. Let i be a fixed but arbitrary integer in $\{1, \ldots, n-1\}$. We can write

$$b_i = b_i^+ - b_i^- = (b_{i1}^+, \ldots, b_{in}^+) - (b_{i1}^-, \ldots, b_{in}^-)$$

and $a_i = a_i^+ - a_i^- = (a_{i1}^+, \ldots, a_{in}^+) - (a_{i1}^-, \ldots, a_{in}^-)$. Then

$$\begin{aligned} h_i(c_1^{v_1}, \ldots, c_n^{v_n}) &= (c_1^{v_1})^{a_{i1}^+} \cdots (c_n^{v_n})^{a_{in}^+} - (c_1^{v_1})^{a_{i1}^-} \cdots (c_n^{v_n})^{a_{in}^-} \\ &= c_1^{v_1 d_1 b_{i1}^+} \cdots c_n^{v_n d_n b_{in}^+} - c_1^{v_1 d_1 b_{i1}^-} \cdots c_n^{v_n d_n b_{in}^-}. \end{aligned} \tag{2.7.2}$$

We claim that $h_i(c_1^{v_1}, \ldots, c_n^{v_n}) = 0$. To show this we consider two cases.

Case (I): $b_{in}^+ > 0$. Then, as $g_i(c) = c^{b_i^+} - c^{b_i^-} = 0$ and $c^{b_i^+}$=0, one has $c^{b_i^-} = 0$. Hence, there is j such that $b_{ij}^- > 0$ and $c_j = 0$. Thus, by Eq. (2.7.2), $h_i(c_1^{v_1}, \ldots, c_n^{v_n}) = 0$.

Case (II): $b_{in}^+ = 0$. If $c_j = 0$ for some $b_{ij}^+ > 0$, then $c^{b_i^-} = 0$ because $g_i(c) = 0$. Hence, there is k such that $c_k = 0$ and $b_{ik}^- > 0$. Thus, by Eq. (2.7.2), $h_i(c_1^{v_1}, \ldots, c_n^{v_n}) = 0$.

Similarly, if $c_j = 0$ for some $b_{ij}^- > 0$, then $c^{b_i^+} = 0$ because $g_i(c) = 0$. Hence, there is k such that $c_k = 0$ and $b_{ik}^+ > 0$. Thus, by Eq. (2.7.2), $h_i(c_1^{v_1}, \ldots, c_n^{v_n}) = 0$. We may now assume that $c_j \neq 0$ if $b_{ij}^+ > 0$, and $c_m \neq 0$ if $b_{im}^- > 0$. Let β be a generator of the cyclic group $(\mathbb{F}_q^*, \cdot)$. Any $c_j \neq 0$ has the form $c_j = \beta^{j_\ell}$. Thus, using that $(\beta^{v_j})^{d_j} = 1$, we get that $(c_j^{v_j})^{d_j b_{ij}^+} = 1$ if $b_{ij}^+ > 0$ and $(c_j^{v_j})^{d_j b_{ij}^-} = 1$ if $b_{ij}^- > 0$. Hence, by Eq. (2.7.2), $h_i(c_1^{v_1}, \ldots, c_n^{v_n}) = 0$, as required. This completes the proof of the claim.

As $h_i(c_1^{v_1}, \ldots, c_n^{v_n}) = 0$ for all i, the point $c' := (c_1^{v_1}, \ldots, c_n^{v_n})$ is in $V(h_1, \ldots, h_{n-1}, t_n)$. By (ii), the point c' is zero. Hence, $c = 0$ as required. This completes the proof of (ii′). Hence, P is a complete intersection generated by $g_1, \ldots, g_{n-1}$.

(b) It follows from Proposition 2.7.5. □

Using the notion of a binary tree, a criterion for complete intersection toric ideals of affine monomial curves is given in [6]. In [4] an effective algorithm is given to determine whether P is a complete intersection. If P is a complete intersection, this algorithm returns the generators of P and the Frobenius number.

In our situation, the next result allows us to: (A) use the results of [6, 12, 30] to give criteria for complete intersection vanishing ideals over a finite field, (B) use the effective algorithms of [4] to recognize complete intersection vanishing ideals over finite fields and to compute its invariants (see Example 2.7.15).

Corollary 2.7.9 *$I(\mathcal{T})$ is a complete intersection if and only if P is a complete intersection.*

Proof. Assume that $I(\mathcal{T})$ is a complete intersection. By Remark 2.7.1 there are binomials $h_1, \ldots, h_{n-1}$ that generate $I(\mathcal{T})$. Hence, P is a complete intersection by Theorem 2.7.8. The converse follows by similar reasons. □

Lemma 2.7.10 *If $r := \gcd(d_1, \ldots, d_n)$ and $d_i' := o(\beta^{rv_i})$, then $d_i = rd_i'$ and $\gcd(d_1', \ldots, d_n') = 1$.*

Proof. It follows readily by recalling that $o(\beta^{rv_i}) = o(\beta^{v_i})/\gcd(r, o(\beta^{v_i}))$. □

In what follows $\mathcal{T}'$ will denote the degenerate torus in $\mathbb{P}^{n-1}$ parameterized by $x_1^{v_1'}, \ldots, x_n^{v_n'}$, where $v_i' := rv_i$ and $r := \gcd(d_1, \ldots, d_n)$. Below, we relate $I(\mathcal{T})$ and $I(\mathcal{T}')$.

Proposition 2.7.11 *The vanishing ideal $I(\mathcal{T})$ is a complete intersection if and only if $I(\mathcal{T}')$ is a complete intersection.*

Proof. Let P and P' be the toric ideals of $K[y_1^{d_1}, \ldots, y_1^{d_n}]$ and $K[y_1^{d_1'}, \ldots, y_1^{d_n'}]$, respectively, where $d_i' := o(\beta^{rv_i})$ for all i. It is not hard to see that $P = P'$. Then, by Theorem 2.7.8, P is a complete intersection if and only if $I(\mathcal{T})$ is a complete intersection and P' is a complete intersection if and only if $I(\mathcal{T}')$ is a complete intersection. Thus, $I(\mathcal{T})$ is a complete intersection if and only if $I(\mathcal{T}')$ is a complete intersection. □

Lemma 2.7.12 *Let $\mathcal{T}^*$ be the affine degenerate torus of type v on $\mathbb{A}$. Then*

$$|\mathcal{T}^*| = d_1 \cdots d_n \text{ and } \deg(S/I(\mathcal{T})) = |\mathcal{T}| = d_1 \cdots d_n / \gcd(d_1, \ldots, d_n).$$

Proof. Let $S_i := \langle \beta^{v_i} \rangle$ be the cyclic group generated by β^{v_i}. The set $\mathcal{T}^*$ is equal to the cartesian product $S_1 \times \cdots \times S_n$. Hence, to show the first equality, it suffices to recall that $|S_i|$ is $o(\beta^{v_i})$, the order of β^{v_i}. Notice that any element of $\mathcal{T}^*$ can be written as $((\beta^{i_1})^{v_1}, \ldots, (\beta^{i_n})^{v_n})$ for some integers $i_1, \ldots, i_n$. The kernel of the epimorphism of groups $\mathcal{T}^* \mapsto \mathcal{T}$, $x \mapsto [x]$, is equal to

$$\{(\gamma, \ldots, \gamma) \in (K^*)^n : \gamma \in \langle \beta^{v_1} \rangle \cap \cdots \cap \langle \beta^{v_n} \rangle\}.$$

Hence, $|\mathcal{T}^*|/|\cap_{i=1}^n \langle \beta^{v_i} \rangle| = |\mathcal{T}|$. Since $\langle \beta^{v_i} \rangle$ is a subgroup of K^* for all i and K^* is a cyclic group, one has $|\cap_{i=1}^n \langle \beta^{v_i} \rangle| = \gcd(d_1, \ldots, d_n)$ (see for instance [67, Theorem 4, p. 4]). Thus, the second equality follows. $\Box$

Definition 2.7.13 If $\mathcal{S}$ is a numerical semigroup of $\mathbb{N}$, the *Frobenius number* of $\mathcal{S}$, denoted by $g(\mathcal{S})$, is the largest integer not in $\mathcal{S}$.

Consider the semigroup $\mathcal{S}' := \mathbb{N}d_1' + \cdots + \mathbb{N}d_n'$, where $d_i' := o(\beta^{rv_i})$ for $i = 1, \ldots, n$. By Lemma 2.7.10, one has $\gcd(d_1', \ldots, d_n') = 1$, i.e., $\mathcal{S}'$ is a numerical semigroup. Thus, $g(\mathcal{S}')$ is finite. If the toric ideal of $K[\mathcal{S}']$ is a complete intersection, then $g(\mathcal{S}')$ can be expressed entirely in terms of $d_1', \ldots, d_n'$ [6, Remark 4.5].

We come to one of the main results of this section.

Corollary 2.7.14 (i) $\deg(S/I(\mathcal{T})) = d_1 \cdots d_n / \gcd(d_1, \ldots, d_n)$.

(ii) *If $I(\mathcal{T})$ is a complete intersection, then*

$$\operatorname{reg} S/I(\mathcal{T}) = \gcd(d_1, \ldots, d_n)\, g(\mathcal{S}') + \textstyle\sum_{i=1}^n d_i - (n-1),$$

where $g(\mathcal{S}')$ denotes the Frobenius number of the numerical semigroup $\mathcal{S}'$ generated by $o(\beta^{rv_1}), \ldots, o(\beta^{rv_n})$; and r is the greatest common divisor of $d_1, \ldots, d_n$.

Proof. Part (i) follows at once from Lemma 2.7.12. Next, we prove (ii). Let P and P' be as in the proof of Proposition 2.7.11. With the notation above, by Lemma 2.7.10, we get that $d_i = rd_i'$ for all i. The toric ideals P and P' are equal but they are graded differently. Recall that P and P' are graded with respect to the gradings induced by assigning $\deg(t_i) := d_i$ and $\deg(t_i) := d_i'$ for all i, respectively. Let $g_1, \ldots, g_{n-1}$ be a generating set of $P = P'$ consisting of binomials. Then, by Theorem 2.7.8, $I(\mathcal{T})$ is generated by $h_1, \ldots, h_{n-1}$, where h_i is $g_i(t_1^{d_1}, \ldots, t_n^{d_n})$ for all i. Accordingly, $I(\mathcal{T}')$ is generated by $h_1', \ldots, h_{n-1}'$, where h_i' is $g_i(t_1^{d_1'}, \ldots, t_n^{d_n'})$ for all i. If $D_i := \deg(h_i)$ and $D_i' := \deg(h_i')$, then $D_i = rD_i'$ for all i. As P' is a complete intersection generated by $g_1, \ldots, g_{n-1}$ and $\deg_{P'}(g_i) = D_i'$ for all i, using [6, Remark 4.5], we get

$$g(\mathcal{S}') = \sum_{i=1}^{n-1} D_i' - \sum_{i=1}^{n} d_i' = \sum_{i=1}^{n-1} (D_i/r) - \sum_{i=1}^{n} (d_i/r).$$

Therefore, using the equality $\operatorname{reg} S/I(\mathcal{T}) = \sum_{i=1}^{n-1}(D_i - 1)$ (see Lemma 2.7.2), the formula for the regularity follows. $\square$

Example 2.7.15 To illustrate how to use the algorithm of [4] we consider the degenerate torus $\mathcal{T}$, over the field $\mathbb{F}_q$, parameterized by $x_1^{v_1}, \ldots, x_5^{v_5}$, where $v_1 := 1500$, $v_2 := 1000$, $v_3 := 432$, $v_4 := 360$, $v_5 := 240$, and $q := 54001$. In this case, one has

$$d_1 = 36,\ d_2 = 54,\ d_3 = 125,\ d_4 = 150,\ d_5 = 225.$$

Using [4, Algorithm CI, p. 981], we get that P is a complete intersection generated by the binomials

$$g_1 := t_1^3 - t_2^2,\ g_2 := t_4^3 - t_5^2,\ g_3 := t_3^3 - t_4t_5,\ g_4 := t_1^8t_2^3 - t_4^3,$$

and we also get that the Frobenius number of $\mathcal{S}$ is 793. Hence, by our results, the vanishing ideal $I(\mathcal{T})$ is a complete intersection generated by the binomials

$$h_1 := t_1^{108} - t_2^{108},\ h_2 := t_4^{450} - t_5^{450},\ h_3 := t_3^{375} - t_4^{150}t_5^{225},\ h_4 := t_1^{288}t_2^{162} - t_4^{450},$$

the index of regularity and degree of $S/I(\mathcal{T})$ are 1379 and 8201250000, respectively.

The next example is interesting because if one chooses $v_1, \ldots, v_n$ at random, it is likely that $I(\mathcal{T})$ will be generated by binomials of the form $t_i^m - t_j^m$.

Example 2.7.16 Let $\mathbb{F}_q$ be the field with $q := 211$ elements. Consider the sequence $v_1 := 42$, $v_2 := 35$, $v_3 := 30$. In this case, one has $d_1 = 5$, $d_2 = 6$, $d_3 = 7$. By a well known result of Herzog [30], one has

$$P = (t_2^2 - t_1t_3,\ t_1^4 - t_2t_3^2,\ t_1^3t_2 - t_3^3).$$

Hence, by our results, $I(\mathcal{T}) = (t_2^{12} - t_1^5t_3^7,\ t_1^{20} - t_2^6t_3^{14},\ t_1^{15}t_2^6 - t_3^{21})$ and this ideal is not a complete intersection. The index of regularity and the degree of $S/I(\mathcal{T})$ are 25 and 210, respectively. The Frobenius number of $\mathcal{S}$ is equal to 9. Notice that the toric relations $t_1^{30} - t_2^{30}$, $t_1^{35} - t_3^{35}$, $t_2^{42} - t_3^{42}$ do not generate $I(\mathcal{T})$.

The next example was found using Theorem 2.7.8. Without using this theorem it is very difficult to construct examples of complete intersection vanishing ideals not generated by binomials of the form $t_i^m - t_j^m$.

Example 2.7.17 Let $\mathbb{F}_q$ be the field with $q := 271$ elements. Consider the sequence $v_1 := 30$, $v_2 := 135$, $v_3 := 54$. In this case, one has $d_1 = 9$, $d_2 = 2$, $d_3 = 5$. The ideals P and $I(\mathcal{T})$ are complete intersections given by

$$P = (t_1 - t_2^2t_3,\ t_2^5 - t_3^2) \text{ and } I(\mathcal{T}) = (t_1^9 - t_2^4t_3^5,\ t_2^{10} - t_3^{10}).$$

By Lemma 2.7.2, the index of regularity of $S/I(\mathcal{T})$ is 17 and by Corollary 2.7.14 the Frobenius number of $\mathcal{S}$ is 3.

Thesis [36] contains more information about this sort of vanishing ideals. Some results at this thesis are:

Theorem 2.7.18 [36, pp. 32–35] *Let $B := K[t_1,\ldots,t_n,y_1,\ldots,y_s,z]$ be a polynomial ring over the finite field $K := \mathbb{F}_q$. If $v_i \in \mathbb{N}^s$ for all i, then the following holds:*

(a) $I(\mathcal{T}) = (\{t_i - y^{v_i}z\}_{i=1}^n \cup \{y_i^{q-1}-1\}_{i=1}^s) \cap S$ *and $I(\mathcal{T})$ is a pure binomial ideal.*

(b) $t_i \notin \mathcal{Z}_S(S/I(\mathcal{T}))$ *for all i and $I(\mathcal{T})$ is a radical pure lattice ideal.*

(c) $S/I(\mathcal{T})$ *is a Cohen-Macaulay ring of dimension 1.*

Finally we show how to compute the vanishing ideal $I(\mathcal{T})$ using the notion of saturation of an ideal with respect to the monomial $t_1\cdots t_n$.

The next lemma is easy to show.

Lemma 2.7.19 *If $c_{ij} := \mathrm{lcm}\{d_i,d_j\} = \mathrm{lcm}\{o(\beta^{v_i}), o(\beta^{v_j})\}$, then $t_i^{c_{ij}} - t_j^{c_{ij}} \in I(\mathcal{T})$.*

The set of *toric relations* $\mathcal{F} := \{t_i^{c_{ij}} - t_j^{c_{ij}} : 1 \le i,j \le n\}$ do not generate $I(\mathcal{T})$, as is seen in Example 2.7.16. If $v_i := 1$ for all i, then $c_{ij} = q-1$ for all i,j and $I(\mathcal{T})$ is generated by $\mathcal{F}$.

For an ideal $I \subset S$ and a polynomial $h \in S$, recall that the saturation of I with respect to h is the ideal

$$I\colon h^\infty := \{f \in S \mid fh^k \in I \text{ for some } k \ge 1\}.$$

Proposition 2.7.20 *Let I' be the ideal $(t_i^{c_{ij}} - t_j^{c_{ij}} | 1 < i < j \le n)$, where $c_{ij} := \mathrm{lcm}\{d_i,d_j\}$. If $\gcd(d_1,\ldots,d_n) = 1$, then $I(\mathcal{T}) = I'\colon (t_1\cdots t_n)^\infty$.*

Proof. We claim that $\mathcal{L} = \mathbb{Z}\{c_{ij}e_i - c_{ij}e_j | 1 \le i < j \le n\}$. By [102, Proposition 10.1.8], we get

$$\mathcal{L}_1 = \mathbb{Z}\{(d_j/\gcd(d_i,d_j))e_i - (d_i/\gcd(d_i,d_j))e_j | 1 \le i < j \le n\}.$$

Thus, the claim follows from the equality $\mathcal{L} = D(\mathcal{L}_1)$. ($\supseteq$) This follows readily using that t_i is a non-zero divisor of $S/I(\mathcal{T})$ for all i because $I(\mathcal{T})$ is a lattice ideal containing I' (see Lemma 2.7.19). ($\subseteq$) Take a binomial $f := t^a - t^b \in I(\mathcal{T})$. By Proposition 2.7.4, $I(\mathcal{T}) = I(\mathcal{L})$. Thus, $a - b \in \mathcal{L}$. Using the previous claim and [39, Lemma 2.3], there is $\delta \in \mathbb{N}^n$ such that $t^\delta f \in I'$. Hence, $f \in I'\colon (t_1\cdots t_n)^\infty$. $\square$

Chapter 3

Affine Codes

Let $K := \mathbb{F}_q$ be a finite field with q elements, $\mathbb{A}^n := K^n$ an affine space over the field K and $\mathcal{X}^*$ an affine subset of $\mathbb{A}^n$. In this chapter we define an affine evaluation code, a code that depends of $\mathcal{X}^*$. We show that the dimension of this code is an increasing function and the minimum distance is a decreasing function. Let $\overline{\mathcal{X}^*}$ be the projective closure of $\mathcal{X}^*$ In analogous way to $\mathcal{X}^*$ we can construct a code that depends of $\overline{\mathcal{X}^*}$. We prove codes depending of $\mathcal{X}$ or $\overline{\mathcal{X}^*}$ are equivalents.

Let $v_1, \ldots, v_n$ be a sequence of non-negative vectors with $v_i := (v_{i1}, \ldots, v_{is})$ for $1 \leq i \leq n$. The set $\mathcal{Q}^* := \{(x_1^{v_{11}} \cdots x_s^{v_{1s}}, \ldots, x_1^{v_{n1}} \cdots x_s^{v_{ns}}) \in \mathbb{A}^n | \, x_i \in K^* \text{ for all } i\}$, is called an *affine algebraic toric set* parameterized by the vectors $v_1, \ldots, v_n$ on $\mathbb{A}^n$. The code associated with $\mathcal{Q}^*$, denoted by $C_{\mathcal{Q}^*}(d)$, is called a *parameterized affine code* of degree d. In this chapter we show that the length of the code $C_{\mathcal{Q}^*}(d)$ is equal to the degree of the quotient ring $S[u]/I(\overline{\mathcal{Q}^*})$, where $\overline{\mathcal{Q}^*}$ is the projective closure of $\mathcal{Q}^*$ and $u := t_{n+1}$ is a new indeterminate. We prove that the length and the dimension of the code $C_{\mathcal{Q}^*}(d)$ can be computed using Gröbner bases. Then we give an explicit procedure written in *Macaulay*2.

We compute an explicit formula for the dimension of $C_{\mathcal{Q}^*}(d)$ when $n = s$ and the vectors $v_1, \ldots, v_n$ that parameterize $\mathcal{Q}^*$ are the canonical vectors $e_1, \ldots, e_n$ in $\mathbb{Q}^n$. When the vectors $v_1, \ldots, v_n$ come from a graph, the set is called a set associated to a graph. We show a formula for the length of a code that comes from a graph.

Let $\Lambda_1, \ldots, \Lambda_n$ be a collection of non-empty subsets of K with a finite number of elements. Consider the *affine cartesian product* $\mathcal{C}^* := \Lambda_1 \times \cdots \times \Lambda_n \subset \mathbb{A}^n$, and $\overline{\mathcal{C}^*}$, the projective closure of $\mathcal{C}^*$. We show $I\left(\overline{\mathcal{C}^*}\right)$ is a complete intersection. Then we give explicit formulas, in terms of the cardinalities of the Λ_i's, for a set of generators, for the Hilbert series, for the index of regularity and for the degree of the ideal $I\left(\overline{\mathcal{C}^*}\right)$.

The code defined by $\mathcal{C}^*$, denoted by $C_{\mathcal{C}^*}(d)$, is called an *affine cartesian code*. In this chapter we give explicit formulas for the length, dimension and minimum distance for this family of codes in terms of the cardinalities of the Λ_i's.

At the end of this section, given a non decreasing sequence of positive integers $d_1, \ldots, d_n$, we construct an affine cartesian code, over an affine degenerate torus, with prescribed parameters in terms of $d_1, \ldots, d_n$.

3.1 Elementary concepts about affine codes

Let $K := \mathbb{F}_q$ be a finite field with q elements, $\mathbb{A}^n := K^n$ an affine space over the field K and $\mathcal{X}^*$ an affine subset of $\mathbb{A}^n$. In this section we define an affine evaluation code, a code that depends of $\mathcal{X}^*$. We show that the dimension of this code is an increasing function and the minimum distance is a decreasing function. Let $\overline{\mathcal{X}^*} := \{[(\lambda, 1)] \mid \lambda \in \mathcal{X}^*\} \subset \mathbb{P}^n$ be the projective closure of $\mathcal{X}^*$ and $\mathcal{X}$ the image of $\mathcal{X}^* \setminus \{0\}$ under the map $\mathbb{A}^n \setminus \{0\} \mapsto \mathbb{P}^{n-1}$, $\gamma \mapsto [\gamma]$. In analogous way to $\mathcal{X}^*$ we can construct a code that depends of $\overline{\mathcal{X}^*}$ or $\mathcal{X}$. We prove codes depending of $\mathcal{X}$ or $\overline{\mathcal{X}^*}$ are equivalents.

Consider $S := K[t_1, \ldots, t_n]$ with the standard grading and let $\mathbf{a}_1, \ldots, \mathbf{a}_m$ be the points of $\mathcal{X}^*$. Let $S_{\leq d}$ be the K-vector space of all polynomials of S of degree at most d. The *evaluation map*

$$\mathrm{ev}_d \colon S_{\leq d} \longrightarrow K^{|\mathcal{X}^*|}, \qquad f \mapsto (f(\mathbf{a}_1), \ldots, f(\mathbf{a}_m)),$$

defines a linear map of K-vector spaces.

Definition 3.1.1 The image of ev_d in $K^{|\mathcal{X}^*|}$, denoted by $C_{\mathcal{X}^*}(d)$, defines a K-vector subspace. Permitting an abuse of language, we are referring to $C_{\mathcal{X}^*}(d)$ as a *linear code*, even though in some cases we use a field K that might not be finite (Section 3.3). We call $C_{\mathcal{X}^*}(d)$ the *affine evaluation code* (*affine code* for short) of degree d on the set $\mathcal{X}^*$.

The vanishing ideal of $\overline{\mathcal{X}^*}$, denoted by $I(\overline{\mathcal{X}^*})$, is the ideal of $S[u]$ generated by the homogeneous polynomials that vanish on $\overline{\mathcal{X}^*}$, where $u := t_{n+1}$ is a new variable and $S[u] := \oplus_{d \geq 0} S[u]_d$ is a polynomial ring, with the standard grading, over the field K. Let $\mathbf{p}_1, \ldots, \mathbf{p}_m$ (it is the same m that we use for the points of $\mathcal{X}^*$, this is because by Theorem 3.1.3 (b) $|\mathcal{X}^*| = |\overline{\mathcal{X}^*}|$) be a set of representatives for the points of $\overline{\mathcal{X}^*}$ and let $f_0(t_1, \ldots, t_{n+1}) := t_1^d$. The evaluation map

$$\mathrm{ev}'_d \colon S[u]_d \longrightarrow K^{|\overline{\mathcal{X}^*}|}, \qquad f \mapsto \left(\frac{f(\mathbf{p}_1)}{f_0(\mathbf{p}_1)}, \ldots, \frac{f(\mathbf{p}_m)}{f_0(\mathbf{p}_m)}\right),$$

defines a linear map of K-vector spaces. If $\mathbf{p}'_1, \ldots, \mathbf{p}'_m$ is another set of representatives, then there are $\lambda_1, \ldots, \lambda_m$ in K^* such that $\mathbf{p}'_i = \lambda_i \mathbf{p}_i$ for all i. Thus, $f(\mathbf{p}'_i)/f_0(\mathbf{p}'_i) = f(\mathbf{p}_i)/f_0(\mathbf{p}_i)$ for $f \in S[u]_d$ and $1 \leq i \leq m$. This means that the map ev'_d is independent of the set of representatives that we choose for the points of $\overline{\mathcal{X}^*}$. In what follows we choose $(\mathbf{a}_1, 1), \ldots, (\mathbf{a}_m, 1)$ as a set of representatives for the points of $\overline{\mathcal{X}^*}$.

Definition 3.1.2 The image of ev'_d, denoted by $C_{\overline{\mathcal{X}^*}}(d)$, defines a linear code that we call the *projective evaluation code* (*projective code* for short) of degree d on the set $\overline{\mathcal{X}^*}$.

Theorem 3.1.3 (a) *There is an isomorphism of K-vector spaces $\varphi \colon C_{\mathcal{X}^*}(d) \to C_{\overline{\mathcal{X}^*}}(d)$,*

$$(f(\mathbf{a}_1), \ldots, f(\mathbf{a}_m)) \xmapsto{\varphi} \left(\frac{f^{\natural}(\mathbf{a}_1, 1)}{f_0(\mathbf{a}_1, 1)}, \ldots, \frac{f^{\natural}(\mathbf{a}_m, 1)}{f_0(\mathbf{a}_m, 1)}\right) = \left(\frac{f(\mathbf{a}_1)}{f_0(\mathbf{a}_1)}, \ldots, \frac{f(\mathbf{a}_m)}{f_0(\mathbf{a}_m)}\right).$$

(b) *The codes $C_{\mathcal{X}^*}(d)$ and $C_{\overline{\mathcal{X}^*}}(d)$ have the same basic parameters.*

Proof. (a) We set $I(\mathcal{X}^*)_{\leq d} := I(\mathcal{X}^*) \cap S_{\leq d}$. The kernel of ev_d is precisely $I(\mathcal{X}^*)_{\leq d}$. Hence, there is an isomorphism of K-vector spaces

$$S_{\leq d}/I(\mathcal{X}^*)_{\leq d} \simeq C_{\mathcal{X}^*}(d) = \{(f(\mathbf{a}_1), \ldots, f(\mathbf{a}_m)) \mid f \in S_{\leq d}\}. \tag{3.1.1}$$

The kernel of ev'_d is the homogeneous part $I(\overline{\mathcal{X}^*})_d$ of degree d of $I(\overline{\mathcal{X}^*})$. Notice that $I(\overline{\mathcal{X}^*})_d$ is equal to $I(\overline{\mathcal{X}^*}) \cap S[u]_d$. Therefore, there is an isomorphism of K-vector spaces

$$S[u]_d/I(\overline{\mathcal{X}^*})_d \simeq C_{\overline{\mathcal{X}^*}}(d). \tag{3.1.2}$$

The homogenization map $\psi\colon S_{\leq d} \to S[u]_d$, $f \mapsto f^{\mathfrak{h}}$, is an isomorphism of K-vector spaces (see [65, p. 330]) such that $\psi(I(\mathcal{X}^*)_{\leq d}) = I(\overline{\mathcal{X}^*})_d$. Hence, the induced map

$$\Phi\colon S_{\leq d} \to S[u]_d/I(\overline{\mathcal{X}^*})_d, \qquad f \longmapsto f^{\mathfrak{h}} + I(\overline{\mathcal{X}^*})_d, \tag{3.1.3}$$

is a surjection. Thus, by Eqs. (3.1.1) and (3.1.2), it suffices to observe that $\ker(\Phi) = I(\mathcal{X}^*)_{\leq d}$.

(b) From part (a) it is clear that $C_{\mathcal{X}^*}(d)$ and $C_{\overline{\mathcal{X}^*}}(d)$ have the same dimension and length. To show that they have the same minimum distance it suffices to notice that the isomorphism φ between $C_{\mathcal{X}^*}(d)$ and $C_{\overline{\mathcal{X}^*}}(d)$ preserves the norm, i.e., $\|\mathbf{c}\| = \|\varphi(\mathbf{c})\|$ for $\mathbf{c} \in C_{\mathcal{X}^*}(d)$. $\square$

Remark 3.1.4 If $H_{\mathcal{X}^*}(d)$ is the *affine Hilbert function* of the affine K-algebra $S/I(\mathcal{X}^*)$, given by

$$H_{\mathcal{X}^*}(d) := \dim_K \, S_{\leq d}/I(\mathcal{X}^*)_{\leq d},$$

then, by Eq. (3.1.3), $H_{\overline{\mathcal{X}^*}}(d) = H_{\mathcal{X}^*}(d)$ for $d \geq 1$ (see [65, Remark 5.3.16]).

From this result it follows at once that the codes $C_{\mathcal{X}^*}(d)$ and $C_{\overline{\mathcal{X}^*}}(d)$ are equivalent in the sense of [98, p. 48].

Corollary 3.1.5 (a) *The dimension of $C_{\mathcal{X}^*}(d)$ is increasing, as a function of d, until it reaches a constant value equal to $|\mathcal{X}^*|$.* (b) *The minimum distance of $C_{\mathcal{X}^*}(d)$ is decreasing, as a function of d, until it reaches a constant value equal to* 1.

Proof. The dimension of $C_{\overline{\mathcal{X}^*}}(d)$ is increasing, as a function of d, until it reaches a constant value equal to $|\overline{\mathcal{X}^*}|$ (see [21, Remark 1.1, p. 166] or [14, p. 456]). The minimum distance of $C_{\overline{\mathcal{X}^*}}(d)$ is decreasing, as a function of d, until it reaches a constant value equal to 1. This was shown in [49, Proposition 5.1, p. 99] and [59, Proposition 2.1] for some cases. For the general case one simply should observe that for every point $\mathbf{a}$ of $\mathcal{X}^*$ there is a polynomial f in S_1 such that $f(\mathbf{a}) = 0$. The result follows from Theorem 3.1.3. $\square$

3.2 Parameterized affine codes

Let $K := \mathbb{F}_q$ be a finite field with q elements, $\mathbb{A}^n := K^n$ an affine space over the field K, $S := K[t_1, \ldots, t_n]$ a polynomial ring over K with n indeterminates and $v_1, \ldots, v_n$ a sequence of vectors in $\mathbb{N}^s$ with $v_i := (v_{i1}, \ldots, v_{is})$ for $1 \leq i \leq n$. Consider the affine algebraic toric set

$$\mathcal{Q}^* := \{(x_1^{v_{11}} \cdots x_s^{v_{1s}}, \ldots, x_1^{v_{n1}} \cdots x_s^{v_{ns}}) \in \mathbb{A}^n |\, x_i \in K^* \text{ for all } i\},$$

parameterized by the vectors $v_1, \ldots, v_n$ on $\mathbb{A}^n$. The set $\mathcal{Q}^*$ is a multiplicative group under componentwise multiplication. We call $C_{\mathcal{Q}^*}(d)$, the code defined by $\mathcal{Q}^*$ using Definition 3.1.1, a *parameterized affine code* of degree d.

In this section we show that the length of the code $C_{\mathcal{Q}^*}(d)$ is equal to the degree of the quotient ring $S[u]/I(\overline{\mathcal{Q}^*})$, where $\overline{\mathcal{Q}^*}$ is the projective closure of $\mathcal{Q}^*$ and $u := t_{n+1}$ is a new indeterminate. We prove that the length and the dimension of the code $C_{\mathcal{Q}^*}(d)$ can be computed using Gröbner bases. We give an explicit procedure written in *Macaulay*2.

We compute an explicit formula for the dimension of $C_{\mathcal{Q}^*}(d)$ when $n = s$ and the vectors $v_1, \ldots, v_n$ that parameterize $\mathcal{Q}^*$ are the canonical vectors $e_1, \ldots, e_n$ in $\mathbb{Q}^n$. When the vectors $v_1, \ldots, v_n$ come from a graph, the set is called a set associated to a graph. We show a formula for the length of a code that comes from a graph.

Parameterized affine codes are interesting because they generalize others important family of codes. For instance they generalize sets parameterized by graphs (Section 3.2.3). Also parameterized affine codes are special types of affine Reed-Muller codes in the sense of [99, p. 37]. If $s := n := 1$ and $v_1 := 1$, then $\mathcal{Q}^* = K^*$ and we obtain the classical Reed-Solomon code of degree d [98, p. 42].

3.2.1 Length and dimension (Theoretically)

Let $K := \mathbb{F}_q$ be a finite field with q elements, $S := K[t_1, \ldots, t_n]$ a polynomial ring over K with n indeterminates and $\mathcal{Q}^*$ the affine algebraic toric set parameterized by the non-negative vectors $v_1, \ldots, v_n$. Most of the cases length of a code is the "easiest" parameter to compute. But sometimes, as in the case of parameterized affine codes, this is a non-trivial parameter. We show in this subsection that the length of the code $C_{\mathcal{Q}^*}(d)$ is equal to the degree of the quotient ring $S[u]/I(\overline{\mathcal{Q}^*})$, where $\overline{\mathcal{Q}^*}$ is the projective closure of $\mathcal{Q}^*$ and $u := t_{n+1}$ is a new indeterminate. We compute the dimension of $C_{\mathcal{Q}^*}(d)$ when $n = s$ and the non-negative vectors $v_1, \ldots, v_n$ that parameterize $\mathcal{Q}^*$ are the canonical vectors $e_1, \ldots, e_n$ in $\mathbb{Q}^n$.

The projective closure of $\mathcal{Q}^*$ can be seen as

$$\overline{\mathcal{Q}^*} = \{[(x_1^{v_{11}} \cdots x_s^{v_{1s}}, \ldots, x_1^{v_{n1}} \cdots x_s^{v_{ns}}, 1)] \,|\, x_i \in K^* \text{ for all } i\} \subset \mathbb{P}^n.$$

Notice that $\overline{\mathcal{Q}^*}$ is parameterized by the vectors $v_1, \ldots, v_n, v_{n+1}$, where $v_{n+1} := \mathbf{0}$.

Recall that the *vanishing ideal* of $\mathcal{Q}^*$, denoted by $I(\mathcal{Q}^*)$, consists of all polynomials f of S that vanish on the set $\mathcal{Q}^*$.

Theorem 3.2.1 *The length of* $C_{\mathcal{Q}^*}(d)$ *is* $\deg(S[u]/I(\overline{\mathcal{Q}^*}))$.

Proof. The ring $S[u]/I(\overline{\mathcal{Q}^*})$ has Krull-dimension 1 (see [49, Theorem 2.1(c), p. 85]), thus its Hilbert polynomial $h_{\overline{\mathcal{Q}^*}}(t) = c_0$ is a non-zero constant and its degree is equal to c_0. Then, according to [86, Lecture 13], or [21], we get that

$$|\overline{\mathcal{Q}^*}| = h_{\overline{\mathcal{Q}^*}}(d) = c_0 = \deg(S[u]/I(\overline{\mathcal{Q}^*}))$$

for $d \geq |\overline{\mathcal{Q}^*}| - 1$. Thus, $|\overline{\mathcal{Q}^*}|$ is the degree of $S[u]/I(\overline{\mathcal{Q}^*})$. Hence, from part (b) of Theorem 3.1.3, we get that the length of $C_{\mathcal{Q}^*}(d)$ is equal to the degree of $S[u]/I(\overline{\mathcal{Q}^*})$. $\Box$

Next, we give an application by computing the basic parameters of a certain family of parameterized affine codes. Let $\mathcal{Q}^*$ be an affine algebraic toric set parameterized by the canonical vectors in $\mathbb{Q}^s : e_1, \ldots, e_s$. In this case $\mathcal{Q}^*$ becomes in T^*, the affine torus, and $\overline{\mathcal{Q}^*}$ becomes in T, the projective torus. Recall that T^* and T are given by

$$T^* := \{(x_1, \ldots, x_n) \in \mathbb{A}^n \mid x_i \in K^*\} \quad \text{and} \quad T := \{[(x_1, \ldots, x_n, 1)] \mid x_i \in K^*\} \subset \mathbb{P}^n.$$

Corollary 3.2.2 *The minimum distance of* $C_{T^*}(d)$ *is given by*

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

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

Proof. It was shown in [54] that the minimum distance of $C_T(d)$ is given by the formula above. Thus, by Theorem 3.1.3, the result follows. $\Box$

As a consequence of this result we obtain the well-known formula for the minimum distance of a Reed-Solomon code [98, p. 42].

Corollary 3.2.3 (Reed-Solomon codes) *Let* T^* *be an affine torus in* $\mathbb{A}^1$. *Then the minimum distance* $\delta_{T^*}(d)$ *of* $C_{T^*}(d)$ *is given by*

$$\delta_{T^*}(d) := \begin{cases} q-1-d & \text{if} \quad 1 \leq d \leq q-3, \\ 1 & \text{if} \quad d \geq q-2, \end{cases}$$

and $C_{T^*}(d)$ *is an MDS code.*

Proof. In this situation $s = 1$. If $d \leq q-3$, we can write $d = k(q-2) + \ell$, where $k := 0$ and $\ell := d$. Then, by Corollary 3.2.2, we get $\delta_{T^*}(d) = q-1-d$ for $d \leq q-3$ and $\delta_{T^*}(d) = 1$ for $d \geq q-2$. $\Box$

Corollary 3.2.4 *The length of* $C_{T^*}(d)$ *is* $(q-1)^n$ *and its dimension is*

$$\dim_K C_{T^*}(d) = \sum_{j=0}^{\left\lfloor \frac{d}{q-1} \right\rfloor} (-1)^j \binom{n}{j} \binom{n+d-j(q-1)}{n}.$$

Proof. The length of $C_{T^*}(d)$ is clearly equal to $(q-1)^n$ because $T^* = (K^*)^n$. It was shown in [14] that the dimension of $C_T(d)$ is given by the formula above. Thus, by Theorem 3.1.3, the result follows. □

Example 3.2.5 Let T^* be an affine torus in $\mathbb{A}^2$ and let $C_{T^*}(d)$ be its parameterized affine code of degree d over the field $K := \mathbb{F}_{11}$. Using Corollaries 3.2.2 and 3.2.4, we obtain:

d	1	2	3	4	5	6	7	8	9	10	11	12	13
$\|T^*\|$	100	100	100	100	100	100	100	100	100	100	100	100	100
$\dim C_{T^*}(d)$	3	6	10	15	21	28	36	45	55	64	72	79	85
$\delta_{T^*}(d)$	90	80	70	60	50	40	30	20	10	9	8	7	6

3.2.2 Length and dimension (Computation)

Let $K := \mathbb{F}_q$ be a finite field with q elements, $S := K[t_1, \ldots, t_n]$ a polynomial ring over K with n indeterminates and $\mathcal{Q}^*$ the affine algebraic toric set parameterized by the non-negative vectors $\upsilon_1, \ldots, \upsilon_n$. We show in this subsection that the length and the dimension of the code $C_{\mathcal{Q}^*}(d)$ can be computed using Gröbner bases. We give an explicit procedure written in *Macaulay*2.

Theorem 3.2.6 (Combinatorial Nullstellensatz [1, Theorem 1.2]) *Let $R := K[y_1, \ldots, y_s]$ be a polynomial ring over a field K, let $f \in R$, and let $a := (a_i) \in \mathbb{N}^s$. Suppose that the coefficient of y^a in f is non-zero and* $\deg(f) = a_1 + \cdots + a_s$. *If $S_1, \ldots, S_s$ are subsets of K, with $|S_i| > a_i$ for all i, then there are $p_1 \in S_1, \ldots, p_s \in S_s$ such that $f(p_1, \ldots, p_s) \neq 0$.*

Lemma 3.2.7 *Let $K := \mathbb{F}_q$ and let G be a polynomial in $K[y_1, \ldots, y_s]$. If G vanishes on $(K^*)^s$ and* $\deg_{y_i}(G) < q-1$ *for $i = 1, \ldots, s$, 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 $\deg(G) = a_1 + \cdots + a_s$, where $a := (a_1, \ldots, a_s)$ 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 Theorem 3.2.6, there are $x_1, \ldots, x_s \in K^*$ so that $G(x_1, \ldots, x_s) \neq 0$, a contradiction to the fact that G vanishes on $(K^*)^s$. □

Lemma 3.2.8 *Let $B := K[t_1, \ldots, t_n, y_1, \ldots, y_s]$ be a polynomial ring over an arbitrary field K. If I' is a pure binomial ideal of B, then $I' \cap K[t_1, \ldots, t_n]$ is a pure binomial ideal.*

Proof. Let $S := K[t_1, \ldots, t_n]$ and let $\mathcal{G}$ be a Gröbner basis of I' with respect to the lexicographic order $y_1 \succ \cdots \succ y_s \succ t_1 \succ \cdots \succ t_n$. By Buchberger algorithm [75, Theorem 2, p. 89] the set $\mathcal{G}$ consists of binomials and by elimination theory [75, Theorem 2, p. 114] the set $\mathcal{G} \cap S$ is a Gröbner basis of $I' \cap S$. Hence $I' \cap S$ is a pure binomial ideal. See the proof of [97, Corollary 4.4, p. 32] for additional details. □

Theorem 3.2.9 *Let $B := K[t_1, \ldots, t_n, y_1, \ldots, y_s]$ be a polynomial ring over a finite field K with q elements. Then*

$$I\left(\mathcal{Q}^*\right) = \left(t_1 - y^{v_1}, \ldots, t_n - y^{v_n}, y_1^{q-1} - 1, \ldots, y_s^{q-1} - 1\right) \cap S$$

and $I(\mathcal{Q}^*)$ is a binomial ideal.

Proof. We set $I' := \left(t_1 - y^{v_1}, \ldots, t_n - y^{v_n}, y_1^{q-1} - 1, \ldots, y_s^{q-1} - 1\right) \subset B$. First we show the inclusion $I(\mathcal{Q}^*) \subset I' \cap S$. Take a polynomial $F := F\left(t_1, \ldots, t_n\right)$ that vanishes on $\mathcal{Q}^*$. We can write

$$F = \lambda_1 t^{m_1} + \cdots + \lambda_r t^{m_r} \quad (\lambda_i \in K^*;\ m_i \in \mathbb{N}^n)\,. \tag{3.2.1}$$

Write $m_i = (m_{i1}, \ldots, m_{is})$ for $1 \leq i \leq r$. Applying the binomial theorem to expand the right hand side of the equality

$$t_j^{m_{ij}} = [(t_j - y^{v_j}) + y^{v_j}]^{m_{ij}}\,, \quad 1 \leq i \leq r,\ 1 \leq j \leq n,$$

we get the equality

$$t_j^{m_{ij}} = \left(\sum_{k=0}^{m_{ij}-1} \binom{m_{ij}}{k} \left(t_j - y^{v_j}\right)^{m_{ij}-k} (y^{v_j})^k)\right) + (y^{v_j})^{m_{ij}}.$$

As a result, we obtain that t^{m_i} can be written as:

$$t^{m_i} = t_1^{m_{i1}} \cdots t_n^{m_{in}} = p_i + (y^{v_1})^{m_{i1}} \cdots (y^{v_n})^{m_{in}},$$

where p_i is a polynomial in the ideal $(t_1 - y^{v_1}, \ldots, t_n - y^{v_n})$. Thus, substituting $t^{m_1}, \ldots, t^{m_r}$ in Eq. (3.2.1), we obtain that F can be written as:

$$F = \sum_{i=1}^{n} g_i(t_i - y^{v_i}) + F(y^{v_1}, \ldots, y^{v_n}) \tag{3.2.2}$$

for some $g_1, \ldots, g_n$ in B. By the division algorithm in $K[y_1, \ldots, y_s]$ (see [75, Theorem 3, p. 63]) we can write

$$F(y^{v_1}, \ldots, y^{v_n}) = \sum_{i=1}^{s} h_i(y_i^{q-1} - 1) + G(y_1, \ldots, y_s) \tag{3.2.3}$$

for some $h_1, \ldots, h_s$ in $K[y_1, \ldots, y_s]$, where the monomials that occur in $G := G(y_1, \ldots, y_s)$ are not divisible by any of the monomials $y_1^{q-1}, \ldots, y_s^{q-1}$, i.e., $\deg_{y_i}(G) < q-1$ for $i = 1, \ldots, s$. Therefore, using Eqs. (3.2.2) and (3.2.3), we obtain the equality

$$F = \sum_{i=1}^{n} g_i(t_i - y^{v_i}) + \sum_{i=1}^{s} h_i(y_i^{q-1} - 1) + G(y_1, \ldots, y_s). \tag{3.2.4}$$

Thus to show that $F \in I' \cap S$ we need only show that $G = 0$. We claim that G vanishes on $(K^*)^s$. Take an arbitrary sequence $x_1, \ldots, x_s$ of elements of K^*. Making $t_i := x^{v_i}$ for all i in Eq. (3.2.4) and using that F vanishes on $\mathcal{Q}^*$, we obtain

$$0 = F(x^{v_1}, \ldots, x^{v_n}) = \sum_{i=1}^{s} g_i'(x^{v_i} - y^{v_i}) + \sum_{i=1}^{s} h_i(y_i^{q-1} - 1) + G(y_1, \ldots, y_s), \tag{3.2.5}$$

where $g_i' := g_i(x^{v_1}, \ldots, x^{v_n}, y_1, \ldots, y_s)$. Since $(K^*, \cdot)$ is a group of order $q - 1$, we can then make $y_i := x_i$ for all i in Eq. (3.2.5) to get that G vanishes on $(x_1, \ldots, x_s)$. This completes the proof of the claim. Therefore G vanishes on $(K^*)^s$ and $\deg_{y_i}(G) < q - 1$ for all i. Hence $G = 0$ by Lemma 3.2.7.

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

$$f = \sum_{i=1}^{n} g_i(t_i - y^{v_i}) + \sum_{i=1}^{s} h_i(y_i^{q-1} - 1) \tag{3.2.6}$$

for some polynomials $g_1, \ldots, g_n, h_1, \ldots, h_s$ in B. Take a point $P := (x^{v_1}, \ldots, x^{v_n})$ in $\mathcal{Q}^*$. Making $t_i := x^{v_i}$ in Eq. (3.2.6), we get

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

where $g_i' := g_i(x^{v_1}, \ldots, x^{v_n}, y_1, \ldots, y_s)$ and $h_i' := h_i(x^{v_1}, \ldots, x^{v_n}, y_1, \ldots, y_s)$. Hence making $y_i := x_i$ for all i, we get that $f(P) = 0$. Thus f vanishes on $\mathcal{Q}^*$. $\Box$

In this section we are always working over a finite field K. For infinite fields the situation is as follows. If $K := \mathbb{C}$ is the field of complex numbers and $\mathcal{Q}$ is an affine toric variety, i.e.,

$$\mathcal{Q} := V(P) := \{\mathbf{a} \in K^n \,|\, f(\mathbf{a}) = 0 \text{ for all } f \in P\}$$

is the *zero set* of a toric ideal P, then by the Nullstellensatz [78, Theorem 1.6] we have that $I(\mathcal{Q}) = P$. This means that $I(\mathcal{Q})$ is a binomial ideal. For infinite fields, we can use the Combinatorial Nullstellensatz (see Theorem 3.2.6) to show the following description of $I(\mathcal{Q}^*)$. We refer to [97] for the theory of toric ideals.

Proposition 3.2.10 *Let $B := K[t_1, \ldots, t_n, y_1, \ldots, y_s]$ be a polynomial ring over an infinite field K. Then*

$$I(\mathcal{Q}^*) = (t_1 - y^{v_1}, \ldots, t_n - y^{v_n}) \cap S$$

and $I(\mathcal{Q}^*)$ is the toric ideal of $K[y^{v_1}, \ldots, y^{v_n}]$.

Our next aim is to show how to compute $I(\overline{\mathcal{Q}^*})$. For $f \in S$ of degree l define

$$f^h = u^l f\left(t_1/u, \ldots, t_n/u\right),$$

that is, f^h is the *homogenization* of the polynomial f with respect to u and l. The *homogenization* of $I(\mathcal{Q}^*) \subset S$ is the ideal $I(\mathcal{Q}^*)^h$ of $S[u]$ given by

$$I(\mathcal{Q}^*)^h := (\{f^h | \, f \in I(\mathcal{Q}^*)\}).$$

Let $\succ$ be the *elimination order* on the monomials of $S[u]$ with respect to $t_1, \ldots, t_n, t_{n+1}$, where $u := t_{n+1}$. Recall that this order is defined as $t^b \succ t^a$ if and only if the total degree of t^b in the variables $t_1, \ldots, t_{n+1}$ is greater than that of t^a, or both degrees are equal, and the last nonzero component of $b - a$ is negative.

Lemma 3.2.11 *If $f_1, \ldots, f_r$ is a Gröbner basis of $I(\mathcal{Q}^*)$, then $f_1^h, \ldots, f_r^h$ form a Gröbner basis and the following equalities hold*:

$$I(\overline{\mathcal{Q}^*}) = I(\mathcal{Q}^*)^h = (f_1^h, \ldots, f_r^h).$$

Proof. The result follows readily from [102, Propositions 2.4.26 and 2.4.30]. □

We come to one of the main results of this section.

Corollary 3.2.12 *The dimension and the length of $C_{\mathcal{Q}^*}(d)$ can be computed using Gröbner basis.*

Proof. By Lemma 3.2.11 we can find a generating set of $I(\overline{\mathcal{Q}^*})$ using Gröbner basis. Thus, using the computer algebra system *Macaulay*2 [79, 61], we can compute the Hilbert function and the degree of $S[u]/I(\overline{\mathcal{Q}^*})$, i.e., we can compute the dimension and the length of $C_{\overline{\mathcal{Q}^*}}(d)$. Consequently, Theorem 3.1.3 allows to compute the dimension and the length of $C_{\mathcal{Q}^*}(d)$ using Gröbner basis. □

Putting the results of this section together we obtain the following process.

Process 3.2.13 The following simple procedure for *Macaulay*2 computes the dimension and the length of a parameterized affine code $C_{\mathcal{Q}^*}(d)$ of degree d.

```
R=GF(q)[y1,...,ys,t1,...,tn,u,MonomialOrder=>Eliminate s]
I'=ideal(t1-y^{\upsilon_1},...,t_n-y^{\upsilon_n},
y1^{q-1}-1,...,ys^{q-1}-1)
I(\mathcal{Q}^*)=ideal selectInSubring(1,gens gb I')
I({\overline{\mathcal{Q}^*}})'=homogenize(I(\mathcal{Q}^*),u)
S=GF(q)[t1,...,tn,u]
I({\overline{\mathcal{Q}^*}})=substitute(I({\overline{\mathcal{Q}^*}})',S)
degree I({\overline{\mathcal{Q}^*}})
hilbertFunction(d,I({\overline{\mathcal{Q}^*}}))
```

Example 3.2.14 Let $\mathcal{Q}^*$ be the affine algebraic toric set parameterized by the vectors $(1,1,0),(0,1,1),(1,0,1)$ and let $C_{\mathcal{Q}^*}(d)$ be its parameterized affine code of order d over the field $K := \mathbb{F}_5$. Using *Macaulay2*, together with Process 3.2.13, we obtain:

$$\begin{aligned} I(\mathcal{Q}^*) &= (t_3^4-1, t_2^2t_3^2-t_1^2, t_1^2t_3^2-t_2^2, t_2^4-1, t_1^2t_2^2-t_3^2, t_1^4-1), \\ I(\overline{\mathcal{Q}^*}) &= (t_3^4-t_4^4, t_2^2t_3^2-t_1^2t_4^2, t_1^2t_3^2-t_2^2t_4^2, t_2^4-t_4^4, t_1^2t_2^2-t_3^2t_4^2, t_1^4-t_4^4), \end{aligned}$$

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

The minimum distance was also computed with *Macaulay2*. An algorithm to compute the minimum distance can be found in Thesis [36].

3.2.3 The parameterized code associated to a graph

Let $K := \mathbb{F}_q$ be a finite field with q elements. When the non-negative vectors $\upsilon_1,\ldots,\upsilon_n$ that parameterize an affine algebraic toric set come from a graph, the set is called a set associated to a graph. Here we have a more precise definition.

Definition 3.2.15 Let $\mathbf{G}$ be a simple graph with vertex set $V(\mathbf{G}) := \{\mathbf{x}_1,\ldots,\mathbf{x}_s\}$ and edge set $E(\mathbf{G}) := \{\mathbf{e}_1,\ldots,\mathbf{e}_n\}$. For an edge $\mathbf{e}_i := \{\mathbf{x}_j,\mathbf{x}_k\}$, where $\mathbf{x}_j,\mathbf{x}_k \in V(\mathbf{G})$, let $\mathcal{V}_i := e_j + e_k \in \mathbb{N}^s$, where, for $1 \le j \le s, e_j$ is the j-th element of the canonical basis of $\mathbb{Q}^s$.

The *set associated to* $\mathbf{G}$ is the set $\mathcal{Q}^*_{\mathbf{G}}$ parameterized by the s-tuples $\mathcal{V}_1,\ldots,\mathcal{V}_n \in \mathbb{N}^s$, obtained from the edges of $\mathbf{G}$. If $\mathcal{Q}^*_{\mathbf{G}}$ is the set associated to $\mathbf{G}$ we call its associated linear code $C_{\mathcal{Q}^*_{\mathbf{G}}}(d)$ the *parameterized code associated* to $\mathbf{G}$ and we refer to the vanishing ideal of $\mathcal{Q}^*_{\mathbf{G}}$ as the vanishing ideal over $\mathbf{G}$.

Theorem 3.2.16 [45, Theorem 3.2] Suppose $\mathbf{G}$ has r connected components, of which λ are non-bipartite. Then,

$$|\mathcal{Q}^*_{\mathbf{G}}| = \begin{cases} \left(\frac{1}{2}\right)^{\lambda-1}(q-1)^{n-r+\lambda-1}, & \text{if } \lambda \ge 1 \text{ and } q \text{ is odd}, \\ (q-1)^{n-r+\lambda-1}, & \text{if } \lambda \ge 1 \text{ and } q \text{ is even}, \\ (q-1)^{n-r-1}, & \text{if } \lambda = 0. \end{cases}$$

3.3 Affine cartesian codes

Let K be an arbitrary field, $\mathbb{A}^n := K^n$ an affine space over the field K, $S := K[t_1,\ldots,t_n]$ a polynomial ring over K with n indeterminates and $\Lambda_1,\ldots,\Lambda_n$ a collection of non-empty subsets of K with a finite number of elements. Consider the following finite sets: (a) an *affine cartesian product*

$$\mathcal{C}^* := \Lambda_1 \times \cdots \times \Lambda_n \subset \mathbb{A}^n,$$

and (b) the projective closure of $\mathcal{C}^*$

$$\overline{\mathcal{C}^*} := \{[(\lambda_1, \ldots, \lambda_n, 1)] \mid \lambda_i \in \Lambda_i \text{ for all } i\} \subset \mathbb{P}^n,$$

where $\mathbb{P}^n$ is a projective space over the field K. For $i = 1, \ldots, n$, we define $d_i := |\Lambda_i|$, the cardinality of Λ_i. We may always assume that $2 \leq d_i \leq d_{i+1}$ for all i (see Proposition 3.3.6). The vanishing ideal of $\overline{\mathcal{C}^*}$, denoted by $I\left(\overline{\mathcal{C}^*}\right)$, consists of all homogeneous polynomials f of S that vanish on the set $\overline{\mathcal{C}^*}$.

We show in this section that $I\left(\overline{\mathcal{C}^*}\right)$ is a complete intersection. Then we give explicit formulas, in terms of the d_i's, for a set of generators, for the Hilbert series, for the index of regularity and for the degree of the ideal $I\left(\overline{\mathcal{C}^*}\right)$.

The code defined by $\mathcal{C}^*$ using Definition 3.1.1, denoted by $C_{\mathcal{C}^*}(d)$, is called an *affine cartesian code* of degree d on the set $\mathcal{C}^*$. In this section we give explicit formulas for the length, dimension and minimum distance of $C_{\mathcal{C}^*}(d)$ in terms of the d_i's.

At the end of this section, given a non decreasing sequence of positive integers $d_1, \ldots, d_n$, we construct an affine cartesian code, over an affine degenerate torus, with prescribed parameters in terms of $d_1, \ldots, d_n$.

3.3.1 Complete intersections and algebraic invariants

Let K be an arbitrary field, $\mathbb{A}^n := K^n$ an affine space over the field K, $S := K[t_1, \ldots, t_n]$ a polynomial ring over K with n variables, $\mathcal{C}^* := \Lambda_1 \times \cdots \times \Lambda_n \subset \mathbb{A}^n$ an affine cartesian product and $\overline{\mathcal{C}^*}$, the projective closure of $\mathcal{C}^*$. Recall that the vanishing ideal of $\overline{\mathcal{C}^*}$, denoted by $I\left(\overline{\mathcal{C}^*}\right)$, consists of all homogeneous polynomials f of S that vanish on the set $\overline{\mathcal{C}^*}$. We show in this section that $I\left(\overline{\mathcal{C}^*}\right)$ is a complete intersection. Then we give explicit formulas, in terms of the cardinalities of the Λ_i's, for a set of generators, for the Hilbert series, for the index of regularity and for the degree of the ideal $I\left(\overline{\mathcal{C}^*}\right)$.

Lemma 3.3.1 (a) $|\overline{\mathcal{C}^*}| = |\mathcal{C}^*| = d_1 \cdots d_n$.

(b) *If Λ_i is a subgroup of $(K^*, \cdot)$ for all i, then $|\mathcal{C}^*|/|\Lambda_1 \cap \cdots \cap \Lambda_n| = |\mathcal{C}|$.*

(c) *If $G \in I(\mathcal{C}^*)$ and $\deg_{t_i}(G) < d_i$ for $i = 1, \ldots, n$, then $G = 0$.*

Proof. (a) The map $\mathcal{C}^* \mapsto \overline{\mathcal{C}^*}$, $x \mapsto [(x, 1)]$, is bijective. Thus, $|\overline{\mathcal{C}^*}| = |\mathcal{C}^*|$. (b) Since Λ_i is a group for all i, the sets $\mathcal{C}^*$ and $\mathcal{C}$ are also groups under componentwise multiplication. Thus, there is an epimorphism of groups $\mathcal{C}^* \mapsto \mathcal{C}$, $x \mapsto [x]$, whose kernel is equal to

$$\{(\lambda, \ldots, \lambda) \in \mathcal{C}^* \colon \lambda \in \Lambda_1 \cap \cdots \cap \Lambda_n\}.$$

Thus, $|\mathcal{C}^*|/|\Lambda_1 \cap \cdots \cap \Lambda_n| = |\mathcal{C}|$. To show (c) we proceed by contradiction. Assume that G is non-zero. Then, there is a monomial $t^a = t_1^{a_1} \cdots t_n^{a_n}$ of G with $\deg(G) = a_1 + \cdots + a_n$, where $a := (a_1, \ldots, a_n)$ and $a_i > 0$ for some i. As $\deg_{t_i}(G) < d_i$ for all i, then $a_i < |\Lambda_i| = d_i$ for all i. Thus, by Theorem 3.2.6, there are $x_1, \ldots, x_n$ with $x_i \in \Lambda_i$ for all i such that $G(x_1, \ldots, x_n) \neq 0$, a contradiction to the assumption that G vanishes on $\mathcal{C}^*$. $\square$

Lemma 3.3.2 *Let f_i be the polynomial $\prod_{\lambda\in\Lambda_i}(t_i - \lambda)$ for $1 \leq i \leq n$. Then*

$$I(\mathcal{C}^*) = (f_1, \ldots, f_n).$$

Proof. ($\supseteq$) This inclusion is clear because f_i vanishes on $\mathcal{C}^*$ by construction. ($\subseteq$) Take f in $I(\mathcal{C}^*)$. Let $\succ$ be the reverse lexicographical order on the monomials of S. By the division algorithm (Proposition 1.1.12 or [66, Theorem 1.5.9, p. 30]), 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 $t_1^{d_1}, \ldots, t_n^{d_n}$, i.e., $\deg_{t_i}(G) < d_i$ for all i. As G belongs to $I(\mathcal{C}^*)$, by Lemma 3.3.1, we get that $G = 0$. Thus, $f \in (f_1, \ldots, f_n)$. $\square$

The degree and the regularity of $S[u]/I(\overline{\mathcal{C}^*})$ can be computed from its Hilbert series. Indeed, the Hilbert series can be written as

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

where $h_0, \ldots, h_r$ are positive integers. This follows from the fact that $I(\overline{\mathcal{C}^*})$ is a Cohen-Macaulay ideal of height n [21]. The number r is the regularity of $S[u]/I(\overline{\mathcal{C}^*})$ and $h_0 + \cdots + h_r$ is the degree of $S[u]/I(\overline{\mathcal{C}^*})$ (see [102, Corollary 4.1.12]).

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

Proposition 3.3.3 (a) $I(\overline{\mathcal{C}^*}) = (\prod_{\lambda\in\Lambda_1}(t_1 - u\lambda), \ldots, \prod_{\lambda\in\Lambda_n}(t_n - u\lambda))$.

(b) $I(\overline{\mathcal{C}^*})$ *is a complete intersection.*

(c) $F_{\overline{\mathcal{C}^*}}(t) = \prod_{i=1}^n (1 + t + \cdots + t^{d_i - 1})/(1-t)$.

(d) $\operatorname{reg} S[u]/I(\overline{\mathcal{C}^*}) = \sum_{i=1}^n (d_i - 1)$ *and* $\deg(S[u]/I(\overline{\mathcal{C}^*})) = |\mathcal{C}^*| = d_1 \cdots d_n$.

Proof. (a) For $i = 1, \ldots, n$, we set $f_i := \prod_{\lambda\in\Lambda_i}(t_i - \lambda)$. Let $\succ$ be the reverse lexicographical order on the monomials of $S[u]$. Since $f_1, \ldots, f_n$ form a Gröbner basis with respect to this order, by Lemma 3.3.2 and [38, Lemma 3.7], the vanishing ideal $I(\overline{\mathcal{C}^*})$ is equal to $(f_1^h, \ldots, f_n^h)$, where $f_i^h := \prod_{\lambda\in\Lambda_i}(t_i - u\lambda)$ is the homogenization of f_i with respect to a new variable u. Part (b) follows from (a) because $I(\overline{\mathcal{C}^*})$ is an ideal of height n [21]. (c) This part follows using (a) and a well known formula for the Hilbert series of a complete intersection (see [102, p. 104]). (d) This part follows directly from [14, Corollary 2.6]. $\square$

Lemma 3.3.4 *From Remark 3.1.4 $H_{\mathcal{C}^*}(d) = H_{\overline{\mathcal{C}^*}}(d)$ for $d \geq 0$.*

In particular, from this Lemma, the dimension and the length of the cartesian code $C_{\mathcal{C}^*}(d)$ are $H_{\overline{\mathcal{C}^*}}(d)$ and $\deg(S[u]/I(\overline{\mathcal{C}^*}))$, respectively.

3.3.2 Cartesian evaluation codes

Let K be an arbitrary field, $\mathbb{A}^n := K^n$ an affine space over the field K, $S := K[t_1, \ldots, t_n]$ a polynomial ring over K with n variables, $\mathcal{C}^* := \Lambda_1 \times \cdots \times \Lambda_n \subset \mathbb{A}^n$ an affine cartesian product and $C_{\mathcal{C}^*}(d)$, the affine evaluation code associated with $\mathcal{C}^*$. In this subsection we give explicit formulas for the length, dimension and minimum distance of $C_{\mathcal{C}^*}(d)$ in terms of the cardinalities of Λ_i's.

We come to one of the main results of this section.

Theorem 3.3.5 *The length of $C_{\mathcal{C}^*}(d)$ 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*

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

Proof. The length of $C_{\mathcal{C}^*}(d)$ is $|\mathcal{C}^*| = d_1 \cdots d_n$. We set $r := \sum_{i=1}^{n}(d_i - 1)$. By Proposition 3.3.3, the regularity of $S[u]/I(\overline{\mathcal{C}^*})$ is equal to r, i.e., $H_{\overline{\mathcal{C}^*}}(d) = |\overline{\mathcal{C}^*}|$ for $d \geq r$. Thus, by Lemmas 3.3.1 and 3.3.4, $H_{\mathcal{C}^*}(d) = |\mathcal{C}^*|$ for $d \geq r$, i.e., $C_{\mathcal{C}^*}(d) = K^{|\mathcal{C}^*|}$ for $d \geq r$. Hence $\delta_{\mathcal{C}^*}(d) = 1$ for $d \geq r$. By Proposition 3.3.3, the ideal $I(\overline{\mathcal{C}^*})$ is a complete intersection generated by n homogeneous polynomials $f_1, \ldots, f_n$ of degrees $d_1, \ldots, d_n$. Thus, applying [14, Corollary 2.6] and using the equality $H_{\mathcal{C}^*}(d) = H_{\overline{\mathcal{C}^*}}(d)$, we obtain the required formula for the dimension. □

Proposition 3.3.6 *If $d_1 = 1$ and $\mathcal{C}' = \Lambda_2 \times \cdots \times \Lambda_n$, then $C_{\mathcal{C}^*}(d) = C_{\mathcal{C}'}(d)$ for $d \geq 1$.*

Proof. Let λ_1 be the only element of Λ_1 and let $\overline{\mathcal{C}'}$ be the projective closure of $\mathcal{C}'$. Then, by Proposition 3.3.3, we get

$$I(\overline{\mathcal{C}^*}) = (t_1 - u\lambda_1, f_2^h, \ldots, f_n^h) \ \text{ and } \ I(\overline{\mathcal{C}'}) = (f_2^h, \ldots, f_n^h),$$

where $f_i^h := \prod_{\lambda\in\Lambda_i}(t_i - u\lambda)$ for $i = 2, \ldots, n$. Since $S[u]/I(\overline{\mathcal{C}^*})$ and $K[t_2, \ldots, t_n, u]/I(\overline{\mathcal{C}'})$ have the same Hilbert function, we get that the dimension and the length of $C_{\mathcal{C}^*}(d)$ and $C_{\mathcal{C}'}(d)$ are the same. Thus, to show the equality $C_{\mathcal{C}^*}(d) = C_{\mathcal{C}'}(d)$, it suffices to show the inclusion ($\subseteq$). Any element of $C_{\mathcal{C}^*}(d)$ has the form

$$\mathbf{c} = (f(\lambda_1, \mathbf{a}_1), \ldots, f(\lambda_1, \mathbf{a}_m)),$$

where $\mathbf{a}_1, \ldots, \mathbf{a}_m$ are the points of $\mathcal{C}'$ and $f \in S_{\leq d}$. If $\widetilde{f}$ is the polynomial $f(\lambda_1, t_2, \ldots, t_n)$, then $\widetilde{f}$ is in $K[t_2, \ldots, t_n]_{\leq d}$ and $f(\lambda_1, \mathbf{a}_i) = \widetilde{f}(\mathbf{a}_i)$ for all i. Thus, $\mathbf{c}$ is an element of $C_{\mathcal{C}'}(d)$, as required. □

Since permuting the sets $\Lambda_1, \ldots, \Lambda_n$ does not affect neither the parameters of the corresponding cartesian evaluation codes, nor the invariants of the corresponding vanishing ideal, by Proposition 3.3.6 we may always assume that $2 \leq d_i \leq d_{i+1}$ for all i, where $d_i := |\Lambda_i|$.

For $G \in S$, we denote the zero set of G in $\mathcal{C}^*$ by $Z_{\mathcal{C}^*}(G)$. We begin with a general bound that will be refined later in this section. The proof of [93, Lemma 3A, p. 147] can be easily adapted to obtain the following auxiliary result.

Lemma 3.3.7 *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*

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

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 Λ_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

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

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

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

where $Z(H_k) := \{a \in \Lambda_2 \times \cdots \times \Lambda_n \,|\, H_k(a) = 0\}$. As $\deg(H_k) + n - 1 < d + n$ and $d_i \leq d_{i+1}$ for all i, then by induction

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

as required. $\square$

Lemma 3.3.8 *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. $\square$

Lemma 3.3.9 *If $0 \neq G \in S$. Then, there are $r \geq 0$ distinct elements $\beta_1, \ldots, \beta_r$ in Λ_n and $G' \in S$ such that*

$$G = (t_n - \beta_1)^{l_1} \cdots (t_n - \beta_r)^{l_r} G', \qquad l_i \geq 1 \text{ for all } i,$$

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

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

Proposition 3.3.10 *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*

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

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

Proof. We proceed by induction on n. By Lemma 3.3.9, there are $r \geq 0$ distinct elements $\beta_1, \ldots, \beta_r$ in Λ_n and $G' \in S$ such that

$$G = (t_n - \beta_1)^{l_1} \cdots (t_n - \beta_r)^{l_r} G', \qquad l_i \geq 1 \text{ for all } i,$$

and $G'(t_1, \ldots, t_{n-1}, \lambda) \neq 0$ for any $\lambda \in \Lambda_n$. 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 $\Lambda_n = \{\beta_1, \ldots, \beta_{d_n}\}$. Let d_i' be the degree of $G'(t_1, \ldots, t_{n-1}, \beta_i)$ and define $d' := \max\{d_i' | \ r+1 \leq i \leq d_n\}$.

Case (I): Assume $n = 1$. Then, $k = 0$ and $d = \ell$. Then $|Z_{\mathcal{C}^*}(G)| \leq \ell$ 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 3.3.7, we get

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

as required.

Case (III): Assume $n \geq 2$, $k \geq 1$ and $d' = 0$. Then, $|Z_{\mathcal{C}^*}(G)| = r d_1 \cdots d_{n-1}$. 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 $\mathcal{C}^*$. Hence, counting the roots of G' that are not in $Z_{\mathcal{C}^*}(H)$, we obtain:

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

where $Z(G_i')$ is the set of zeros of G_i' in $\Lambda_1 \times \cdots \times \Lambda_{n-1}$. 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 3.3.1, the non-zero polynomial G_i' cannot be the zero-function on $\Lambda_1 \times \cdots \times \Lambda_{n-1}$. 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

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

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 3.3.8 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 3.3.8, we obtain:

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

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 3.3.8 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 3.3.8, we obtain:

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

Thus, we need only show the inequality

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

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

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

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. $\Box$

Corollary 3.3.11 *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*

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

Proof. Let $F:=F(t_1,\ldots,t_n)\in S$ be an arbitrary polynomial of total degree $d'\leq d$ such that $F(\mathbf{a})\neq 0$ for some $\mathbf{a}\in\mathcal{C}^*$. 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 $\prec$ be the graded reverse lexicographical order on the monomials of S. In this order $t_1\succ\cdots\succ t_n$. For $1\leq i\leq n$, let f_i be the polynomial $\prod_{\lambda\in\Lambda_i}(t_i-\lambda)$. Recall that $d_i=|\Lambda_i|$, i.e., f_i has degree d_i. By the division algorithm [66, Theorem 1.5.9, p. 30], we can write

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

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. ($\dagger\dagger$) and using that $0\neq F(\mathbf{a})=G'(\mathbf{a})$, we get $Z_{\mathcal{C}^*}(F)=\emptyset$. 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 $Z_{\mathcal{C}^*}(F)=Z_{\mathcal{C}^*}(G')$. By Proposition 3.3.10, and applying Lemma 3.3.8 to the sequences $d_1,\ldots,d_n,d'',d'$ and $d_1,\ldots,d_n,d',d$, we obtain

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

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

We come to one of the main results of this section.

Theorem 3.3.12 *Let K be a field and let $C_{\mathcal{C}^*}(d)$ be the cartesian evaluation code of degree d on the finite set $\mathcal{C}^* := \Lambda_1 \times \cdots \times \Lambda_n \subset K^n$. If $2 \leq d_i \leq d_{i+1}$ for all i, with $d_i := |\Lambda_i|$, and $d \geq 1$, then the minimum distance of $C_{\mathcal{C}^*}(d)$ is given by*

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

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 $C_{\mathcal{C}^*}(d)$ is equal to 1 by Theorem 3.3.5. Assume that $1 \leq d \leq \sum_{i=1}^{n} (d_i - 1) - 1$. We can write

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

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

$$\begin{aligned} Z_{\mathcal{C}^*}(G) \;=\;& [(\Lambda_1 \setminus \{\beta_{1,d_1}\}) \times \Lambda_2 \times \cdots \times \Lambda_n] \cup \\ & [\{\beta_{1,d_1}\} \times (\Lambda_2 \setminus \{\beta_{2,d_2}\}) \times \Lambda_3 \times \cdots \times \Lambda_n] \cup \\ & \qquad\qquad\vdots \\ & [\{\beta_{1,d_1}\} \times \cdots \times \{\beta_{k-1,d_{k-1}}\} \times (\Lambda_k \setminus \{\beta_{k,d_k}\}) \times \Lambda_{k+1} \times \cdots \times \Lambda_n] \cup \\ & [\{\beta_{1,d_1}\} \times \cdots \times \{\beta_{k,d_k}\} \times \{\beta_{k+1,1}, \ldots, \beta_{k+1,\ell}\} \times \Lambda_{k+2} \times \cdots \times \Lambda_n], \end{aligned}$$

we get that the number of zeros of G in $\mathcal{C}^*$ is given by:

$$|Z_{\mathcal{C}^*}(G)| = \sum_{i=1}^{k} (d_i - 1)(d_{i+1} \cdots d_n) + \ell d_{k+2} \cdots d_n = d_1 \cdots d_n - d_{k+1} \cdots d_n + \ell d_{k+2} \cdots d_n.$$

By Lemma 3.3.1, one has $|\mathcal{C}^*| = d_1 \cdots d_n$. Therefore

$$\begin{aligned} \delta_{\mathcal{C}^*}(d) &= \min\{\|\mathrm{ev}_d(F)\| \colon \mathrm{ev}_d(F) \neq 0; F \in S_{\leq d}\} = |\mathcal{C}| - \max\{|Z_{\mathcal{C}^*}(F)| \colon F \in S_{\leq d};\ F \not\equiv 0\} \\ &\leq d_1 \cdots d_n - |Z_{\mathcal{C}^*}(G)| = (d_{k+1} - \ell)\, d_{k+2} \cdots d_n, \end{aligned}$$

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 $\mathcal{C}^*$. Thus

$$\delta_{\mathcal{C}^*}(d) \leq (d_{k+1} - \ell) d_{k+2} \cdots d_n.$$

The reverse inequality follows at once from Corollary 3.3.11. $\Box$

Remember that if K is a finite field, the set $T := \{[(x_1, \ldots, x_{n+1})] \in \mathbb{P}^n | \, x_i \in K^* \text{ for all } i\}$ is called a projective torus in $\mathbb{P}^n$, where $K^* = K \setminus \{0\}$.

As a consequence of our main result, we recover the following formula for the minimum distance of a parameterized code over a projective torus.

Corollary 3.3.13 [54, Theorem 3.5] *Let $K = \mathbb{F}_q$ be a finite field with $q \neq 2$ elements. If T is a projective torus in $\mathbb{P}^n$ and $d \geq 1$, then the minimum distance of $C_T(d)$ is given by*

$$\delta_T(d) := \begin{cases} (q-1)^{n-k-1}(q-1-\ell) & \text{if } \; d \leq (q-2)n-1, \\ 1 & \text{if } \; d \geq (q-2)n, \end{cases}$$

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 $\Lambda_i := K^*$ for $i = 1, \ldots, n$, then $\mathcal{C}^* = (K^*)^n$, $\overline{\mathcal{C}^*} = T$, and $d_i = q-1$ for all i. Since $\delta_{\mathcal{C}^*}(d) = \delta_{\overline{\mathcal{C}^*}}(d)$, the result follows at once from Theorem 3.3.12. $\Box$

As another consequence of our main result, we recover a formula for the minimum distance of an evaluation code over an affine space.

Corollary 3.3.14 [13, Theorem 2.6.2] *Let $K := \mathbb{F}_q$ be a finite field and let $\overline{\mathcal{C}^*}$ 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 $C_{\overline{\mathcal{C}^*}}(d)$ is given by:*

$$\delta_{\overline{\mathcal{C}^*}}(d) := \begin{cases} (q-\ell)q^{n-k-1} & \text{if } \; d \leq n(q-1)-1, \\ 1 & \text{if } \; d \geq n(q-1), \end{cases}$$

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 $\Lambda_i := K$ for $i = 1, \ldots, n$, then $\mathcal{C}^* = K^n = \mathbb{A}^n$ and $d_i = q$ for all i. Since $\delta_{\mathcal{C}^*}(d) = \delta_{\overline{\mathcal{C}^*}}(d)$, the result follows at once from Theorem 3.3.12. $\Box$

Example 3.3.15 If $\mathcal{C}^* := \mathbb{F}_2^n$, then the basic parameters of $C_{\mathcal{C}^*}(d)$ are given by

$$|\mathcal{C}^*| = 2^n, \quad \dim C_{\mathcal{C}^*}(d) = \textstyle\sum_{i=0}^{d} \binom{n}{i}, \quad \delta_{\mathcal{C}^*}(d) = 2^{n-d}, \quad 1 \leq d \leq n.$$

Example 3.3.16 Let $K := \mathbb{F}_9$ be a field with 9 elements. Assume that $\Lambda_i := K$ for $i = 1, \ldots, 4$. For certain values of d, the basic parameters of $C_{\mathcal{C}^*}(d)$ are given in the following table:

d	1	2	3	4	5	10	16	20	28	31	32
$\lvert\mathcal{C}^*\rvert$	6561	6561	6561	6561	6561	6561	6561	6561	6561	6561	6561
$\dim C_{\mathcal{C}^*}(d)$	5	15	35	70	126	981	3525	5256	6526	6560	6561
$\delta_{\mathcal{C}^*}(d)$	5832	5103	4374	3645	2916	567	81	45	5	2	1

3.3.3 Cartesian codes over affine degenerate tori

Let K be an arbitrary field, $\mathbb{A}^n := K^n$ an affine space over the field K and $S := K[t_1,\ldots,t_n]$ a polynomial ring over K with n variables. Given a non decreasing sequence of positive integers $d_1,\ldots,d_n$, in this section we construct a cartesian code, over an affine degenerate torus, with prescribed parameters in terms of $d_1,\ldots,d_n$.

Let $v := \{v_1,\ldots,v_n\}$ be a sequence of positive integers. The set

$$\mathcal{T}^* := \{(x_1^{v_1},\ldots,x_n^{v_n}) \in \mathbb{A}^n \,|\, x_i \in \mathbb{F}_q{}^* \text{ for all } i\}$$

is called an *affine degenerate torus* of type v on $\mathbb{F}_q$.

We come to the main result of this section.

Theorem 3.3.17 *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 an affine degenerate torus $\mathcal{T}^*$ such that the length of $C_{\mathcal{T}^*}(d)$ is $d_1\cdots d_n$, its dimension is*

$$\dim_K C_{\mathcal{T}^*}(d) = \binom{n+d}{d} - \sum_{1\leq i\leq n}\binom{n+d-d_i}{d-d_i} + \sum_{i<j}\binom{n+d-(d_i+d_j)}{d-(d_i+d_j)} -$$
$$\sum_{i<j<k}\binom{n+d-(d_i+d_j+d_k)}{d-(d_i+d_j+d_k)} + \cdots + (-1)^n\binom{n+d-(d_1+\cdots+d_n)}{d-(d_1+\cdots+d_n)},$$

its minimum distance is 1 if $d \geq \sum_{i=1}^n(d_i-1)$, and

$$\delta_{\mathcal{T}^*}(d) = (d_{k+1}-\ell)d_{k+2}\cdots d_n \quad \textit{if} \quad d \leq \textstyle\sum_{i=1}^n(d_i-1)-1,$$

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 $q-1 = v_id_i$ 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 $\Lambda_i := \langle\beta^{v_i}\rangle$, where $\langle\beta^{v_i}\rangle$ is the subgroup of K^* generated by β^{v_i}. If $\mathcal{T}^*$ is the cartesian product of $\Lambda_1,\ldots,\Lambda_n$, it not hard to see that $\mathcal{T}^*$ is given by

$$\mathcal{T}^* = \{(x_1^{v_1},\ldots,x_n^{v_n}) \,|\, x_i \in K^* \text{ for all } i\} \subset \mathbb{A}^n,$$

i.e., $\mathcal{T}^*$ is an affine degenerate torus of type $v = \{v_1,\ldots,v_n\}$. The length of $|\mathcal{T}^*|$ is $d_1\cdots d_n$ because $|\Lambda_i| = d_i$ for all i. The formulae for the dimension and the minimum distance of $C_{\mathcal{T}^*}(d)$ follow from Theorems 3.3.5 and 3.3.12. □

Remark 3.3.18 Let $K := \mathbb{F}_q$ be a finite field and let β be a generator of the cyclic group $(K^*,\cdot)$. If $\mathcal{T}^*$ is an affine degenerate torus of type $v := \{v_1,\ldots,v_n\}$, then $\mathcal{T}^*$ is the cartesian product of $\Lambda_1, \ldots, \Lambda_n$, where Λ_i is the cyclic group generated by β^{v_i}. Thus, if $d_i := |\Lambda_i|$ for $i = 1, \ldots, n$, the affine evaluation code over $\mathcal{T}^*$ is a cartesian code. Hence, according to Theorem 3.3.5 and 3.3.12, the basic parameters of $C_{\mathcal{T}^*}(d)$ can be computed in terms of $d_1, \ldots, d_n$ as in Theorem 3.3.17:

- The length of $C_{\mathcal{T}^*}(d)$ is $d_1 \cdots d_n$.
- The dimension of $C_{\mathcal{T}^*}(d)$ is

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

- The minimum distance of $C_{\mathcal{T}^*}(d)$ is

$$\delta_{\mathcal{T}^*}(d) := \begin{cases} (d_{k+1}-\ell)\, d_{k+2} \cdots d_n & \text{if } d \le \sum_{i=1}^{n} (d_i - 1) - 1, \\ 1 & \text{if } d \ge \sum_{i=1}^{n} (d_i-1)\,, \end{cases}$$

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

Therefore, we are recovering the main results of [25, 26].

As an illustration of Theorem 3.3.17 consider the following example.

Example 3.3.19 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 $C_{\mathcal{T}^*}(d)$, over the affine degenerate torus

$$\mathcal{T}^* := \{(x_1^{90}, x_2^{36}, x_3^{20}) |\, x_i \in \mathbb{F}_{181}^* \ \text{ for } i = 1, 2, 3\},$$

are shown in the following table. Notice that the regularity of $S[u]/I(\overline{\mathcal{C}^*})$ is 13.

d	1	2	3	4	5	6	7	8	9	10	11	12	13
$\lvert\mathcal{T}^*\rvert$	90	90	90	90	90	90	90	90	90	90	90	90	90
$\dim C_{\mathcal{T}^*}(d)$	4	9	16	25	35	45	55	65	74	81	86	89	90
$\delta_{\mathcal{T}^*}(d)$	45	36	27	18	9	8	7	6	5	4	3	2	1

Notice that if $K' := \mathbb{F}_9$, and we pick subsets $\Lambda_1, \Lambda_2, \Lambda_3$ of K' with $|\Lambda_1| = 2$, $|\Lambda_2| = 5$, $|\Lambda_3| = 9$, the cartesian evaluation code $C_{\mathcal{T}'}(d)$, over the set $\mathcal{T}' := \Lambda_1 \times \Lambda_2 \times \Lambda_3$, has the same parameters that $C_{\mathcal{T}^*}(d)$ for any $d \ge 1$.

Chapter 4

Projective Codes

Let $K := \mathbb{F}_q$ be a finite field with q elements, $\mathbb{P}^n$ a projective pace over the field $K, S := K[t_0, \ldots, t_n]$ a polynomial ring over the field K with $n+1$ variables and S_d the K-vector space of all homogeneous polynomials of S of degree d union the zero polynomial. Let $\mathcal{X}$ be a subset of $\mathbb{P}^n$ and $\mathbf{p}_1, \ldots, \mathbf{p}_m$ the points of $\mathcal{X}$ written with standard representation for projective points, that is, zeros to the left and the first nonzero entry equal 1.

The *evaluation map*

$$\varphi_d \colon S_d \longrightarrow K^{|\mathcal{X}|}, \qquad f \mapsto (f(\mathbf{p}_1), \ldots, f(\mathbf{p}_m)),$$

defines a linear map of K-vector spaces. The image, denoted by $C_{\mathcal{X}}(d)$, defines a linear code, i.e., a K-vector subspace. We call $C_{\mathcal{X}}(d)$ the *projective evaluation code* (*projective code* for short) of degree d on the set $\mathcal{X}$.

Let $v := \{v_1, \ldots, v_n\}$ be a sequence of positive integers and $\mathcal{T} := \{[(x_1^{v_1}, \ldots, x_n^{v_n})] \mid x_i \in K^* \text{ for all } i\} \subseteq \mathbb{P}^{n-1}$ a projective degenerate torus of type v. In this chapter we compute the length of $C_{\mathcal{T}}(d)$. We give an explicit formula of the index of regularity of $S/I(\mathcal{T})$ in terms of a Frobenius number. Thus we can give a condition over d in order to good codes can appear.

Let $\Lambda_0, \ldots, \Lambda_n$ be a collection of non-empty subsets of K and $\mathcal{C} := [\Lambda_0 \times \Lambda_1 \times \cdots \times \Lambda_n]$ a projective nested cartesian product. In this chapter we compute the length and the dimension of $C_{\mathcal{C}}(d)$. We also compute the minimum distance when every Λ_i is a field. We give a relation between projective cartesian codes and affine cartesian codes. In particular, we show that there exists a relation between the basic parameters of generalized Reed-Muller codes and the basic parameters of projective Reed-Muller codes.

4.1 Parameterized projective codes

Let $K := \mathbb{F}_q$ be a finite field with q elements, $\mathbb{P}^n$ a projective pace over the field K and $S := K[t_0, \ldots, t_n]$ a polynomial ring over the field K with $n+1$ variables. Let $v := \{v_1, \ldots, v_n\}$ be a sequence of positive integers and $\mathcal{T} := \{[(x_1^{v_1}, \ldots, x_n^{v_n})] \mid x_i \in K^* \text{ for all } i\} \subseteq \mathbb{P}^{n-1}$ a projective degenerate torus of type v. The projective code associated with $\mathcal{T}$, denoted by $C_{\mathcal{T}}(d)$, is called a *parameterized projective code* of degree d. In this section we compute the length of $C_{\mathcal{T}}(d)$ and we give a condition over d in order to good codes can appear.

The linear code $C_{\mathcal{T}}(d)$ has length $|\mathcal{T}|$. The index of regularity of $S/I(\mathcal{T})$ is important because good codes $C_{\mathcal{T}}(d)$ can occur only if $1 \leq d < \operatorname{reg}(S/I(\mathcal{T}))$. Therefore we apply the results of Section 2.7 about $S/I(\mathcal{T})$.

Let β be a generator of the cyclic group $(\mathbb{F}_q^*, \cdot)$ and d_i denotes $o(\beta^{v_i})$, the order of β^{v_i} for $i = 1, \dots, n$.

Theorem 4.1.1 (i) *The length of $C_{\mathcal{T}}(d)$ is $d_1 \cdots d_n / \gcd(d_1, \dots, d_n)$.*

(ii) *If $I(\mathcal{T})$ is a complete intersection, then good codes $C_{\mathcal{T}}(d)$ can occur only if*

$$d \leq \gcd(d_1, \dots, d_n)\, g(\mathcal{S}') + \textstyle\sum_{i=1}^{n} d_i - (n-1),$$

where $g(\mathcal{S}')$ denotes the Frobenius number of the numerical semigroup $\mathcal{S}'$ generated by $o(\beta^{rv_1}), \dots, o(\beta^{rv_n})$; and r is the greatest common divisor of $d_1, \dots, d_n$.

Proof. This is a consequence of Corollary 2.7.14. □

4.2 Projective nested cartesian codes

Let $K := \mathbb{F}_q$ be a finite field with q elements, $\mathbb{P}^n$ a projective pace over the field $K, S := K[t_0, \dots, t_n]$ a polynomial ring over K with $n+1$ indeterminates, $\Lambda_0, \dots, \Lambda_n$ a collection of non-empty subsets of K. Consider the *projective cartesian product*:

$$\mathcal{C} := [\Lambda_0 \times \Lambda_1 \times \cdots \times \Lambda_n] = \{[(\lambda_0, \lambda_1, \dots, \lambda_n)] |\, \lambda_i \in \Lambda_i \text{ for all } i\} \subseteq \mathbb{P}^n.$$

Let Λ and Λ' be subsets of $\mathbb{F}_q$. We define the set $\frac{\Lambda}{\Lambda'} := \left\{ \frac{\lambda}{\lambda'} \mid \lambda \in \Lambda, 0 \neq \lambda' \in \Lambda' \right\}$.

Definition 4.2.1 Let $\Lambda_0, \Lambda_1, \dots, \Lambda_n$ be a collection of non-empty subsets of K such that

(i) for all $i = 0, \dots, n$ we have $0 \in \Lambda_i$, and

(ii) for every $i = 1, \dots, n$ we have $\frac{\Lambda_j}{\Lambda_{i-1}} \subseteq \Lambda_j$, for $j = i, \dots, n$.

Under these conditions, the projective cartesian set $\mathcal{C} = [\Lambda_0 \times \Lambda_1 \times \cdots \times \Lambda_n]$ is called a *projective nested cartesian set,* and the projective code $C_{\mathcal{C}}(d)$ is called a *projective nested cartesian code*. In this section we compute the length and the dimension of $C_{\mathcal{C}}(d)$. We also compute the minimum distance when every Λ_i is a field. We give a relation between projective cartesian codes and affine cartesian codes. In particular, we show that there exists a relation between the basic parameters of generalized Reed-Muller codes and the basic parameters of projective Reed-Muller codes.

For $i = 0, \dots, n$, define $d_i := |\Lambda_i|$, the cardinality of Λ_i. We shall always assume that $2 \leq d_i \leq d_{i+1}$ for all i. The case $d_1 = \cdots = d_j = 1$ will be treated separately (Lemma 4.2.5).

Remark 4.2.2 If for $i=0,\ldots,n$ we take $\Lambda_i := K$, then the Λ_i's satisfies the conditions of Definition 4.2.1. This means that the projective space $\mathbb{P}^n$ is a projective nested cartesian set. As a consequence the Projective Reed-Muller code $PC_d(n,q)$ is a projective nested cartesian code.

4.2.1 Length

Let $K := \mathbb{F}_q$ be a finite field with q elements, $\mathcal{C} := [\Lambda_0 \times \Lambda_1 \times \cdots \times \Lambda_n]$ a projective nested cartesian set and $C_{\mathcal{C}}(d)$, the evaluation code associated with $\mathcal{C}$. For $i = 0,\ldots,n$, define $d_i := |\Lambda_i|$, the cardinality of Λ_i.

We come to the main and unique result of this subsection.

Theorem 4.2.3 *The length of $C_{\mathcal{C}}(d)$ is $m := 1 + \sum_{i=1}^{n} d_i \cdots d_n$.*

Proof. If $\mathcal{C} := [\Lambda_0 \times \Lambda_1 \times \cdots \times \Lambda_n]$ is a projective nested cartesian set, then

$$\begin{aligned} \mathcal{C} = \quad & \left[\Lambda_0^{\neq 0} \times \Lambda_1 \times \Lambda_2 \times \cdots \times \Lambda_n\right] \cup \\ & \left[0 \times \Lambda_1^{\neq 0} \times \Lambda_2 \times \cdots \times \Lambda_n\right] \cup \\ & \qquad\qquad \vdots \\ & \left[0 \times 0 \times 0 \times \cdots \times \Lambda_{n-1}^{\neq 0} \times \Lambda_n\right] \cup \\ & [0 \times 0 \times 0 \times \cdots \times 0 \times 1]\,. \end{aligned}$$

Finally, the condition that for every $i = 1,\ldots,n$ we have $\frac{\Lambda_j}{\Lambda_{i-1}} \subseteq \Lambda_j$ for $j = i,\ldots n$, allow us to change $\Lambda_i^{\neq 0}$ for 1 in the previous equation and we have the result. $\square$

4.2.2 Dimension

Let $K := \mathbb{F}_q$ be a finite field with q elements, $\mathbb{P}^n$ a projective pace over the field $K, S := K[t_0,\ldots,t_n]$ a polynomial ring over K with $n+1$ indeterminates and $\mathcal{C} := [\Lambda_0 \times \Lambda_1 \times \cdots \times \Lambda_n]$ a projective nested cartesian set. In this section we give a set of generators $\mathcal{G}$ of the ideal $I(\mathcal{C})$ and we compute its Hilbert function. We prove that actually $\mathcal{G}$ is a Gröbner basis using the degree lexicographical order. Then we give an explicit formula for the dimension of the evaluation code associated with $\mathcal{C}$, $C_{\mathcal{C}}(d)$.

Lemma 4.2.4 *If $\mathcal{C}$ is the projective nested cartesian set over $\Lambda_0,\ldots,\Lambda_n$, then its vanishing ideal is*

$$I(\mathcal{C}) = \left(\left\{ t_i \prod_{\lambda_j \in \Lambda_j} (t_j - \lambda_j t_i)\,, i < j; i,j = 0,\ldots,n \right\}\right).$$

Proof. By induction on n. If $n=1$ then $\mathcal{C}=[1\times\Lambda_n]\cup[0\times 1]$ and trivially (using [37, Proposition 2.5 (a)]) $I(\mathcal{C})=\left(\left\{t_0\prod_{\lambda_1\in\Lambda_1}(t_1-\lambda_1 t_0)\right\}\right)$. Now we assume that the result is valid for $n-1$. Take $\mathcal{C}_1:=[1\times\Lambda_1\times\Lambda_2\times\cdots\times\Lambda_n]$, $\mathcal{C}_0:=[\Lambda_1\times\Lambda_2\times\cdots\times\Lambda_n]$ and $F\in I(\mathcal{C})$. Define

$$F:=F_1t_0+F_2,$$

where $F_2\in K[t_1,\ldots,t_n]$. Let $\mathbf{a}$ be an element of $\mathcal{C}_0$. As $\mathcal{C}$ is a projective nested cartesian set, $\mathcal{C}=\mathcal{C}_1\cup[0\times\mathcal{C}_0]$, so $[1,\mathbf{a}],[0,\mathbf{a}]\in\mathcal{C}$. We have $0=F(0,\mathbf{a})=F_2(\mathbf{a})$, then $F_2\in I(\mathcal{C}_0)$ and by induction

$$F_2\in\left(\left\{t_i\prod_{\lambda_j\in\Lambda_j}(t_j-\lambda_j t_i),i<j;i,j=1,\ldots,n\right\}\right).$$

We know also that $0=F(1,\mathbf{a})=F_1(\mathbf{a})$, then $F_1\in I(\mathcal{C}_1)$ and by [37, Proposition 2.5 (a)]

$$F_1\in\left(\left\{\prod_{\lambda_i\in\Lambda_i}(t_i-\lambda_i t_0),i=1,\ldots,n\right\}\right).$$

As $F=F_1t_0+F_2$ the result is true. $\square$

Why can we consider that $d_i\geq 2$ for $i=0,\ldots,n$? The answer is the following.

If $d_0=\cdots=d_n=1$ then $\mathcal{C}=\phi$ because $\Lambda_0=\cdots=\Lambda_n=0$. Otherwise

Lemma 4.2.5 *Assume $d_0=\cdots=d_l=1<d_{l+1}$ with $0\leq l\leq n-1$. If $\mathcal{C}:=[\Lambda_0\times\Lambda_1\times\cdots\times\Lambda_n]$ and $\mathcal{C}':=[\Lambda_{l+1}\times\cdots\times\Lambda_n]$ then $C_{\mathcal{C}}(d)$ and $C_{\mathcal{C}'}(d)$ have same basic parameters.*

Proof. The condition $d_0=\cdots=d_l=1$ means $\Lambda_0=\cdots=\Lambda_l=\{0\}$ and we have

$$I(\mathcal{C})=\left(\left\{t_0,\ldots,t_l,t_i\prod_{\lambda_j\in\Lambda_j}(t_j-\lambda_j t_i),l+1\leq i<j\leq n\right\}\right).$$

By Lemma 4.2.4 $I(\mathcal{C}')=\left(\left\{t_i\prod_{\lambda_j\in\Lambda_j}(t_j-\lambda_j t_i),l+1\leq i<j\leq n\right\}\right)$. Since $K[t_0,\ldots,t_n]/I(\mathcal{C})$ and $K[t_{l+1},\ldots,t_n]/I(\mathcal{C}')$ have the same Hilbert function for $d\geq 1$, we get that the dimension and the length of $C_{\mathcal{C}}(d)$ and $C_{\mathcal{C}'}(d)$ are the same.

(i) $C_{\mathcal{C}}(d)\subseteq C_{\mathcal{C}'}(d)$: Let $\mathbf{c}:=(f(\mathbf{0},\mathbf{p}_1),\ldots,f(\mathbf{0},\mathbf{p}_M))$ be an element of $C_{\mathcal{C}}(d)$. Then $f\in S_d$ and $f=t_0f_0+\cdots+t_lf_l+F$, with $F\in K[t_{l+1},\ldots,t_n]_d$. As $f(\mathbf{0},\mathbf{p}_i)=0$ if and only if $F(\mathbf{p}_i)=0$, $\mathbf{c}':=(f(\mathbf{p}_1),\ldots,f(\mathbf{p}_M))$ is an element of $C_{\mathcal{C}'}(d)$ with $\|\mathbf{c}'\|=\|\mathbf{c}\|$.

(ii) $C_{\mathcal{C}'}(d)\subseteq C_{\mathcal{C}}(d)$: Let $\mathbf{c}':=(f(\mathbf{p}_1),\ldots,f(\mathbf{p}_M))$ be an element of $C_{\mathcal{C}'}(d)$. Then $f\in K[t_{l+1},\ldots,t_n]_d\subset S_d$ and $\mathbf{c}:=(f(\mathbf{0},\mathbf{p}_1),\ldots,f(\mathbf{0},\mathbf{p}_M))$ is an element of $C_{\mathcal{C}}(d)$ with $\|\mathbf{c}\|=\|\mathbf{c}'\|$. $\square$

Notation 4.2.6 The calculation of dimension arises using induction on n, for that reason we consider:

$$\text{for } i = n, \ldots, 0, \mathcal{C}_i := [\Lambda_{n-i} \times \cdots \times \Lambda_n], \text{ and } I(\mathcal{C}_i) \subset K[t_{n-i}, \ldots, t_n],$$

$$\text{and for } i = n, \ldots, 1, \mathcal{C}_i^* := [1 \times \Lambda_{n+1-i} \times \cdots \times \Lambda_n], \text{ and } I(\mathcal{C}_i^*) \subset K[t_{n-i}, \ldots, t_n].$$

Lemma 4.2.7 *For any positive integer d $H_{\mathcal{C}_n}(d) = H_{\mathcal{C}_{n-1}}(d) + H_{\mathcal{C}_n^*}(d-1)$.*

Proof. From Lemma 4.2.4

$$I(\mathcal{C}_n) = \left(\left\{ t_i \prod_{\lambda_j \in \Lambda_j} (t_j - \lambda_j t_i), i < j; i, j = 0, \ldots, n \right\} \right) = \bigoplus_{d \geq 0} I_{\mathcal{C}_n}(d)$$

and

$$I(\mathcal{C}_{n-1}) = \left(\left\{ t_i \prod_{\lambda_j \in \Lambda_j} (t_j - \lambda_j t_i), i < j; i, j = 1, \ldots, n \right\} \right) = \bigoplus_{d \geq 0} I_{\mathcal{C}_{n-1}}(d)$$

and from [37, Proposition 2.5 (a)]

$$I(\mathcal{C}_n^*) = \left(\left\{ \prod_{\lambda_i \in \Lambda_i} (t_i - \lambda_i t_0); i = 1, \ldots, n \right\} \right) = \bigoplus_{d \geq 0} I_{\mathcal{C}_n^*}(d).$$

Thus $I(\mathcal{C}_n) = I(\mathcal{C}_{n-1}) + t_0 I(\mathcal{C}_n^*)$. If $1 \leq d \leq d_1$ trivially $I_{\mathcal{C}_n}(d) = I_{\mathcal{C}_{n-1}}(d) \oplus I_{\mathcal{C}_n^*}(d) = 0$. If $d > d_1$ we define the exact sequence between K-vector spaces:

$$0 \to I_{\mathcal{C}_{n-1}}(d) \xrightarrow{\phi} I_{\mathcal{C}_n}(d) \xrightarrow{\varphi} t_0 I_{\mathcal{C}_n^*}(d-1) \to 0,$$

where

$$\phi \left(f_{ij} t_i \prod_{\lambda_j \in \Lambda_j} (t_j - \lambda_j t_i) \right) = f_{ij} t_i \prod_{\lambda_j \in \Lambda_j} (t_j - \lambda_j t_i) \text{ and}$$

$$\varphi \left(\sum_{i=1}^{n} f_i \left[t_0 \prod_{\lambda_i \in \Lambda_i} (t_i - \lambda_i t_0) \right] + \sum_{1 \leq i < j \leq n} f_{ij} t_i \prod_{\lambda_j \in \Lambda_j} (t_j - \lambda_j t_i) \right) = t_0 \left[\sum_{i=1}^{n} f_i \prod_{\lambda_i \in \Lambda_i} (t_i - \lambda_i t_0) \right].$$

As

$$\sigma : t_0 I_{\mathcal{C}_n^*}(d-1) \to I_{\mathcal{C}_n}(d), \quad t_0 \left[\sum_{i=1}^{n} f_i \prod_{\lambda_i \in \Lambda_i} (t_i - \lambda_i t_0) \right] \to \sum_{i=1}^{n} f_i \left[t_0 \prod_{\lambda_i \in \Lambda_i} (t_i - \lambda_i t_0) \right]$$

is a section of φ, by [68, Proposition 5.9 (1)] $I_{\mathcal{C}_n}(d) = I_{\mathcal{C}_{n-1}}(d) \bigoplus t_0 I_{\mathcal{C}_n^*}(d-1)$. We know that $S_d = t_0 K\left[t_0, \ldots, t_n\right]_{d-1} \bigoplus K[t_1, \ldots, t_n]_d$. Then

$$S_d / I_{\mathcal{C}_n}(d) \simeq t_0 K\left[t_0, \ldots, t_n\right]_{d-1} / t_0 I_{\mathcal{C}_n^*}(d-1) \bigoplus K[t_1, \ldots, t_n]_d / I_{\mathcal{C}_{n-1}}(d) \simeq$$

$$\simeq K\left[t_0, \ldots, t_n\right]_{d-1} / I_{\mathcal{C}_n^*}(d-1) \bigoplus K[t_1, \ldots, t_n]_d / I_{\mathcal{C}_{n-1}}(d).$$

Thus we have the complete proof. □

Lemma 4.2.8 *Let $\mathcal{C} := [\Lambda_0 \times \cdots \times \Lambda_n]$ be a projective nested cartesian set. The Hilbert function of $S/I(\mathcal{C})$ is*

$$H_{\mathcal{C}}(d) = \sum_{j=0}^{n} \left[\binom{j+d-1}{d-1} - \sum_{n+1-j \le i \le n} \binom{j+d-1-d_i}{d-1-d_i} + \sum_{i<j} \binom{j+d-1-(d_i+d_j)}{d-1-(d_i+d_j)} - \right.$$

$$\left. \sum_{i<j<k} \binom{j+d-1-(d_i+d_j+d_k)}{d-1-(d_i+d_j+d_k)} + \cdots + (-1)^j \binom{j+d-1-(d_{n+1-j}+\cdots+d_n)}{d-1-(d_{n+1-j}+\cdots+d_n)} \right].$$

Proof. Using Lemma 4.2.7 we have

$$H_{\mathcal{C}}(d) = H_{\mathcal{C}_0}(d) + \sum_{j=1}^{n} H_{\mathcal{C}_j^*}(d-1).$$

$\mathcal{C}_0 = [1], I(\mathcal{C}_0) = 0$ and $H_{\mathcal{C}_0} = 1$. From [37, Theorem 3.1]

$$H_{\mathcal{C}_j^*}(d-1) = \binom{j+d-1}{d-1} - \sum_{n+1-j \le i \le n} \binom{j+d-1-d_i}{d-1-d_i} + \sum_{i<j} \binom{j+d-1-(d_i+d_j)}{d-1-(d_i+d_j)} -$$

$$\sum_{i<j<k} \binom{j+d-1-(d_i+d_j+d_k)}{d-1-(d_i+d_j+d_k)} + \cdots + (-1)^j \binom{j+d-1-(d_{n+1-j}+\cdots+d_n)}{d-1-(d_{n+1-j}+\cdots+d_n)}.$$

□

We come to one of the main results of this section.

Theorem 4.2.9 *The dimension of $C_{\mathcal{C}}(d)$ is*

$$H_{\mathcal{C}}(d) = \sum_{j=0}^{n} \left[\binom{j+d-1}{d-1} - \sum_{n+1-j \le i \le n} \binom{j+d-1-d_i}{d-1-d_i} + \right.$$

$$\sum_{i<j} \binom{j+d-1-(d_i+d_j)}{d-1-(d_i+d_j)} - \sum_{i<j<k} \binom{j+d-1-(d_i+d_j+d_k)}{d-1-(d_i+d_j+d_k)}$$

$$\left. + \cdots + (-1)^j \binom{j+d-1-(d_{n+1-j}+\cdots+d_n)}{d-1-(d_{n+1-j}+\cdots+d_n)} \right].$$

Proof. As the kernel of the evaluation map φ_d is $S_d \cap I(\mathcal{C})$, the Hilbert function of $S/I(\mathcal{C})$ agrees with the dimension of $C_{\mathcal{C}}(d)$. By Lemma 4.2.8 we have a proof. □

Finally we show that for the degree lexicographical order $\prec$ in S, where $t_0 \prec \cdots \prec t_n$, the set

$$\mathcal{G} := \left\{ t_i \prod_{\lambda_j \in \Lambda_j} (\Lambda_j - \lambda_j \Lambda_i), i < j; i, j = 0, \ldots, n \right\}$$

is a Gröbner basis of the ideal $I(\mathcal{C})$. In what follows, $\mathbf{m}$ denotes a monomial in S.

Definition 4.2.10 The *footprint* (with respect to a monomial order $\prec$) of an ideal $I \subset S$, denoted by $\Delta(I)$, is the set of monomials which are not leading monomials of any polynomial in I.
If $\mathcal{F} := \{f_1, f_2, \dots, f_s\}$ is a subset of S, we set $\Delta(\mathcal{F}) := \{\mathbf{m} \mid \text{ for all } i,\ \mathrm{LM}(g_i) \nmid \mathbf{m}\}$, where $\mathrm{LM}(f)$ denotes the leading monomial of $f \in S$. We write $\Delta(\mathcal{F})_d$ to denote de set of monomials in $\Delta(\mathcal{F})$ of degree equal to d, for any integer $d \geq 0$.

Lemma 4.2.11 *Fix a graded monomial order in S. Let I be a homogeneous ideal of S and $\mathcal{F} = \{f_1, f_2, \dots, f_s\}$ a set of generators of I. The set $\mathcal{F}$ is a Gröbner Basis of I if and only if the Hilbert function of I is given by $H_I(d) = \#\Delta(\mathcal{F})_d$, for all $d \geq 0$.*

Proof. We know that $(\mathrm{LM}(f_1), \dots, \mathrm{LM}(\mathrm{f_s})) \subseteq (\mathrm{LM}(I))$, where equality holds if and only if $\mathcal{F}$ is a Gröbner basis. This means that $\Delta(I) \subseteq \Delta(\mathcal{F})$ and equality holds if $\mathcal{F}$ is a Gröbner basis. As the number of elements of $\Delta(I)_d$ is equal to $H_I(d)$, we have the result is true. $\square$

From now on we choose the degree lexicographical order $\prec$ in S, where $t_0 \prec \cdots \prec t_n$.

Lemma 4.2.12 *The number of elements of $\Delta(\mathcal{G})_d$ is given by*

$$\binom{n+d}{n} - \sum_{j=1}^{n}\left(\binom{n+d-d_j}{n} - \binom{n-j+d-d_j}{n-j}\right) + \cdots +$$
$$+(-1)^k \sum_{1\leq j_1<j_2<\cdots<j_k\leq n}\left(\binom{n+d-(d_{j_1}+\cdots+d_{j_k})}{n} - \binom{n-j_1+d-(d_{j_1}+\cdots+d_{j_k})}{n-j_1}\right) +$$
$$+ \cdots + (-1)^n\binom{n+d-(d_1+\cdots+d_n+1)}{n}.$$

Proof. Observe that $\Delta(\mathcal{G}) = \left\{\mathbf{m} \mid X_i X_j^{d_j} \nmid \mathbf{m}, 0 \leq i < j \leq n\right\}$. For $1 \leq j \leq n$, we define $\mathcal{M}_j := \left\{\mathbf{m} \mid \text{ there is } i, 0 \leq i < j, X_i X_j^{d_j} \mid \mathbf{m}\right\}$. Then $\Delta(\mathcal{G}) = \mathcal{M}_S - \left(\bigcup_{j=1}^n \mathcal{M}_j\right)$, where $\mathcal{M}_S$ is the set of all monomials in S. Therefore, when we count the number of monomials of degree d in $\Delta(\mathcal{G})$, from the inclusion-exclusion theorem we get

$$\begin{aligned}
\Delta(\mathcal{G})_d &= \#\left(\mathcal{M}_S\right)_d - \sum_{j=1}^{n}\#(\mathcal{M}_j)_d + \sum_{j_1<j_2}\#(\mathcal{M}_{j_1}\cap\mathcal{M}_{j_2})_d - \cdots \\
&\quad +(-1)^k \sum_{j_1<j_2<\cdots<j_k}\#(\mathcal{M}_{j_1}\cap\mathcal{M}_{j_2}\cap\cdots\cap\mathcal{M}_{j_k})_d + \cdots \\
&\quad +(-1)^n\#(\mathcal{M}_1\cap\mathcal{M}_2\cap\cdots\cap\mathcal{M}_n)_d\,.
\end{aligned}$$

Clearly $\#(\mathcal{M}_S)_d = \binom{n+d}{n}$. Let $j \in \{1, \dots, n\}$ and set $\mathbf{m} := t_0^{\alpha_0}\cdots t_n^{\alpha_n} \in (\mathcal{M}_j)_d$, then there exists $i < j$, such that $\alpha_i \geq 1$ and $\alpha_j \geq d_j$. Taking $\beta_j := \alpha_j - d_j$ and for $k \neq j$, $\beta_k := \alpha_k$, we have that $\#(\mathcal{M}_j)_d$ is the number of solutions of $\beta_0 + \cdots + \beta_n = d - d_j$, such that

$\beta_0 + \cdots + \beta_{j-1} \geq 1$. Then $\#(\mathcal{M}_j)_d$ is the number of solutions of $\beta_0 + \cdots + \beta_n = d - d_j$ minus the number of solutions of $\beta_j + \cdots + \beta_n = d - d_j$. This means

$$\#(\mathcal{M}_j)_d = \binom{n+d-d_j}{n} - \binom{n-j+d-d_j}{n-j}.$$

Now set $\mathbf{m} = t_0^{\alpha_0} \cdots t_n^{\alpha_n} \in (\mathcal{M}_{j_1} \cap \cdots \cap \mathcal{M}_{j_k})_d$, then there exists $i < j_1$, such that $\alpha_i \geq 1$ and $\alpha_{j_w} \geq d_{j_w}$, for $1 \leq w \leq k$. Taking $\beta_{j_w} = \alpha_{j_w} - d_{j_w}$, for $1 \leq w \leq k$, with $l \neq j_w$ and $\beta_l = \alpha_l$, we get that $\#(\mathcal{M}_{j_1} \cap \cdots \cap \mathcal{M}_{j_k})_d$ is the number of solutions of $\beta_0 + \cdots + \beta_n = d - (d_{j_1} + \cdots + d_{j_k})$ minus the number of solutions of $\beta_{j_1} + \cdots + \beta_n = d - (d_{j_1} + \cdots + d_{j_k})$, hence

$$\#(\mathcal{M}_{j_1} \cap \cdots \cap \mathcal{M}_{j_k})_d = \binom{n+d-(d_{j_1}+\cdots+d_{j_k})}{n} - \binom{n-j_1+d-(d_{j_1}+\cdots+d_{j_k})}{n-j_1}.$$

For $k = n$ we have $\binom{n+d-(d_1+\cdots+d_n)}{n} - \binom{n-1+d-(d_1+\cdots+d_n)}{n-1} = \binom{n+d-(d_1+\cdots+d_n+1)}{n}$. $\square$

We use the next well-known combinatorial result to check that $H_{\mathcal{C}}(d) = \#\Delta(\mathcal{G})_d$ for all $d \geq 0$.

Lemma 4.2.13 *Let a, b be non-negative integers. Then $\sum_{j=0}^{a} \binom{j+b-1}{j} = \binom{a+b}{a}$.*

Proposition 4.2.14 *Let $\mathcal{C} := [\Lambda_0 \times \cdots \times \Lambda_n]$ be a projective nested cartesian set. The set $\mathcal{G} := \left\{ t_i \prod_{\lambda_j \in \Lambda_j} (t_j - \lambda_j t_i), i < j; i, j = 0, \ldots, n \right\}$ is a Gröbner basis for $I(\mathcal{C})$.*

Proof. From Lemma 4.2.11 we only need to compare the formulas of Lemmas 4.2.8 and 4.2.12. On the formula for the Hilbert Function, we distribute the sum, use Lemma 4.2.13 and compare term by term with the formula for the footprint. The first term is

$$1 + \sum_{j=1}^{n} \binom{j+d-1}{d-1} = \sum_{j=0}^{n} \binom{j+d-1}{j} = \binom{n+d}{n},$$

the second term is

$$\begin{aligned}
\sum_{j=1}^{n} \sum_{i=n+1-j}^{n} \binom{j+d-1-d_i}{d-1-d_i} &= \sum_{i=1}^{n} \sum_{j=n+1-i}^{n} \binom{j+d-1-d_i}{j} \\
&= \sum_{j=1}^{n} \sum_{i=n+1-j}^{n} \binom{i+d-1-d_j}{i} \\
&= \sum_{j=1}^{n} \left(\sum_{i=0}^{n} \binom{i+d-d_j-1}{i} - \sum_{i=0}^{n-j} \binom{i+d-d_j-1}{i} \right) \\
&= \sum_{j=1}^{n} \left(\binom{n+d-d_j}{n} - \binom{n-j+d-d_j}{n-j} \right),
\end{aligned}$$

and the general term is

$$\sum_{j=1}^{n} \sum_{n+1-j\leq i_1<\cdots<i_k\leq n} \binom{j+d-1-(d_{i_1}+\cdots+d_{i_k})}{d-1-(d_{i_1}+\cdots+d_{i_k})} =$$

$$\sum_{1\leq i_1<\cdots<i_k\leq n} \sum_{j=n+1-i_1}^{n} \binom{j+d-1-(d_{i_1}+\cdots+d_{i_k})}{j} =$$

$$\sum_{1\leq i_1<\cdots<i_k\leq n} \left(\binom{n+d-(d_{i_1}+\cdots+d_{i_k})}{n} - \binom{n-i_1+d-(d_{i_1}+\cdots+d_{i_k})}{n-i_1}\right).$$

Finally, for the last term, the sum on the formula for the Hilbert function has only one term, and $\binom{n+d-1-(d_1+\cdots+d_n)}{d-1-(d_1+\cdots+d_n)} = \binom{n+d-(d_1+\cdots+d_n+1)}{n}$, which proves the Proposition. □

4.2.3 Minimum distance

Let $K := \mathbb{F}_q$ be a finite field with q elements, $\mathbb{P}^n$ a projective pace over the field $K, S := K[t_0,\ldots,t_n]$ a polynomial ring over K with $n+1$ indeterminates, S_d the K-vector space of all homogeneous polynomials of S of degree d union the zero polynomial, $\mathcal{C} := [\Lambda_0 \times \Lambda_1 \times \cdots \times \Lambda_n]$ the projective nested cartesian set and $C_{\mathcal{C}}(d)$, the evaluation code associated with $\mathcal{C}$. In this section we give an upper bound of the minimum distance of $C_{\mathcal{C}}(d)$. In the case that every Λ_i is a subfield of K, we give an explicit formula for the minimum distance.

We start this section by presenting an upper bound for the minimum distance of projective nested cartesian codes. Instead of $f(t_0,\ldots,t_n)$ we write simply $f(t)$ for a polynomial in S.

Lemma 4.2.15 *If $\mathcal{C}$ is the projective nested cartesian set over $\Lambda_0,\ldots,\Lambda_n$, then the minimum distance of $C_{\mathcal{C}}(d)$ satisfies $\delta_{\mathcal{C}}(d) \leq (d_{k+1}-\ell)\, d_{k+2}\cdots d_n$ if $1 \leq d \leq \sum_{i=1}^{n}(d_i-1)$, and $\delta_{\mathcal{C}}(d) = 1$ in otherwise, where $0 \leq k \leq n-1$ and $0 \leq \ell < d_{k+1}-1$ are the unique integers such that $d-1 = \sum_{i=1}^{k}(d_i-1)+\ell$.*

Proof. For all $i = 0,\ldots,n$ choose $\lambda_i \in \Lambda_i$. It is easy to see that the polynomial

$$f(t) := t_0 \prod_{i=1}^{n} \prod_{\lambda\in\Lambda_i}^{\lambda\neq\lambda_i} (t_i - \lambda t_0)$$

of degree $\sum_{i=1}^{n}(d_i-1)+1$ is zero for all points of $\mathcal{C}$ except for $[(1,\lambda_1,\ldots,\lambda_n)]$. Thus for $d > \sum_{i=1}^{n}(d_i-1)$ we get $\delta_{\mathcal{C}}(d) = 1$. Let $\Gamma \subset \Lambda_{k+1}$ be a set with ℓ elements. For

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

$$f(t):=t_0\left(\prod_{i=1}^{k}\prod_{\lambda\in\Lambda_i}^{\lambda\neq\lambda_i}(t_i-\lambda t_0)\right)\left(\prod_{\lambda\in\Gamma}(t_{k+1}-\lambda t_0)\right),$$

we obtain the desired inequality. □

We believe that this upper bound is actually the true value of the minumum distance.

Conjecture 4.2.16 *If $\mathcal{C}$ is the projective nested cartesian set over $\Lambda_0,\ldots,\Lambda_n$, then the minimum distance of $C_{\mathcal{C}}(d)$ is given by*

$$\delta_{\mathcal{C}}(d):=\begin{cases}(d_{k+1}-\ell)\,d_{k+2}\cdots d_n & \text{if} \quad 1\leq d\leq\sum_{i=1}^{n}(d_i-1)\,,\\ 1 & \text{if} \quad \sum_{i=1}^{n}(d_i-1)<d,\end{cases}$$

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

We will prove below this conjecture in the special case where the sets Λ_i are subfields of K (so it includes the projective Reed-Muller codes). Before that we study this case we prove an auxiliary result.

Lemma 4.2.17 *Let $\mathcal{C}:=[\Lambda_0\times\cdots\times\Lambda_n]$ be a projective nested cartesian set. For all $j=0,\ldots,n$ set $\lambda_j\in\Lambda_j^{\neq0}$ and define $\Gamma_j:=\lambda_j^{-1}\Lambda_j$. Then $\mathcal{D}:=[\Gamma_0\times\cdots\times\Gamma_n]$ is a projective nested cartesian set such that $1\in\Gamma_j$, for all $j=0,\ldots,n$, and $C_{\mathcal{C}}(d)=C_{\mathcal{D}}(d)$, for all degree d.*

Proof. Assume $\mathcal{C}=\{\mathbf{p}_1,\ldots,\mathbf{p}_m\}$ and $\mathcal{D}=\{\mathbf{q}_1,\ldots,\mathbf{q}_m\}$, where $\mathbf{p}_i=[(x_0,\ldots,x_n)]$ and $\mathbf{q}_i=[(\lambda_0^{-1}x_0,\ldots,\lambda_n^{-1}x_n)]$ for all $i=0,\ldots,n$. Let v be an element of $C_{\mathcal{C}}(d)$, then $v=[(f(\mathbf{p}_1),\ldots,f(\mathbf{p}_m))]$ for some $f\in S_d$. Define $g(t_0,\ldots,t_n):=f(\lambda_0t_0,\ldots,\lambda_nt_n)\in S_d$. It is easy to see that $v=[(g(\mathbf{q}_1),\ldots,g(\mathbf{q}_m))]$, so $C_{\mathcal{C}}(d)\subseteq C_{\mathcal{D}}(d)$. The proof of $C_{\mathcal{D}}(d)\subseteq C_{\mathcal{C}}(d)$ is similar. □

Thus we see that one may always assume that $1\in\Lambda_j$, for all $j=0,\ldots,n$. We present now the special class of projective nested cartesian set for whose associated codes we will determine the minimum distance.

Definition 4.2.18 Let $K_0\subseteq\cdots\subseteq K_n$ be subfields of K, with $|K_i|=d_i$ for all $0\leq i\leq n$. Observe that $d_{i+1}=d_i^{r_i}$, for some $r_i\geq1$ and $q=d_n^{r_n}$. Then $\mathcal{C}:=[K_0\times\cdots\times K_n]$ is a projective nested cartesian set which is called a *projective nested product of fields.*

Clearly $\mathbb{P}^n$ is a projective nested product of fields, so our results on codes defined over such sets extend the results on projective Reed-Muller codes.

Definition 4.2.19 Let g be a polynomial in S of degree d not necessarily homogeneous. We say that g is *homogeneous on* $\mathcal{C}$, and we write $g \in \widetilde{S}_d$, if for every $i \in \{0, \ldots, n\}$ and every $x := [(0, \ldots, 0, 1, x_{i+1}, \cdots, x_n)] \in \mathcal{C}$ we have that for any given $\lambda \in \Lambda_i^{\neq 0}$ there exists $\tilde{\lambda} \in \Lambda_i^{\neq 0}$ such that

$$g(0, \ldots, 0, \lambda, \lambda x_{i+1}, \ldots, \lambda x_n) = \tilde{\lambda} g(0, \ldots, 0, 1, x_{i+1}, \ldots, x_n)\,.$$

Definition 4.2.20 Let $\mathcal{C} := [\Lambda_0 \times \cdots \times \Lambda_n]$ be a projective nested cartesian set. For a set $\mathcal{E} \subseteq \mathcal{C}$ and $f \in \widetilde{S}_d \backslash I(\mathcal{E})$, define

$$Z_{\mathcal{E}}(f) := \{\mathbf{p} \in \mathcal{E} \mid f(\mathbf{p}) = 0\}\,.$$

In this way, for a codeword $v := (f(\mathbf{p}_1), \ldots, f(\mathbf{p}_m)) \neq 0$, where $f(t) \in S_d \backslash I(\mathcal{C})_d$, the weight of v is $|\mathcal{C} \backslash Z_{\mathcal{C}}(f)|$, and the minimum distance of $C_{\mathcal{C}}(d)$ is given by

$$\delta_{\mathcal{C}}(d) = \min\left\{|\mathcal{C} \backslash Z_{\mathcal{C}}(f)| : f \in S_d \backslash I(\mathcal{C})_d\right\}.$$

Lemma 4.2.21 *Let f be an element of $\widetilde{S}_d$ such that for all $\ell \leq j \leq n$ we have $Z_{\mathcal{C}}(t_j) \subseteq Z_{\mathcal{C}}(f)$. Then there exists $g_\ell(t)$ in $\widetilde{S}_{d-(n-\ell+1)}$ such that $f - g_\ell \cdot t_\ell \cdots t_n \in I(\mathcal{C})$.*

Proof. Write $f = g_n t_n + h_n$, where $h_n \in K[t_0, \ldots, t_{n-1}]$. For any $\mathbf{p} := [(x_0, \cdots, x_{n-1}, 0)]$ in $\mathcal{C}$ we have $f(\mathbf{p}) = 0$. This implies that $h_n \in I([K_0 \times \cdots \times K_{n-1}])$, and a fortiori we have $h_n \in I(\mathcal{C})$. By induction on k, suppose that for some $\ell + 1 \leq k \leq n$ we have $f = g_k t_k \cdots t_n + h_k$, where $h_k \in I(\mathcal{C})$. Write $g_k = g_{k-1} t_{k-1} + \tilde{h}_{k-1}$, where $\tilde{h}_{k-1} \in K[t_0, \ldots, t_{k-2}, t_k \ldots, t_n]$. For any $\mathbf{p} := [(x_0, \ldots, x_{k-2}, 0, x_k, \ldots, x_n)] \in \mathcal{C}$, we have $f(\mathbf{p}) = 0$. This implies $(\tilde{h}_{k-1} t_k \cdots t_n)(\mathbf{p}) = 0$, which means $\tilde{h}_{k-1} t_k \cdots t_n \in I([K_0 \times \cdots \times K_{k-2} \times K_k \times \cdots \times K_n]) \subseteq I(\mathcal{C})$. We have then $f = g_{k-1} t_{k-1} \cdots t_n + \tilde{h}_{k-1} t_k \cdots t_n + h_k$, where $\tilde{h}_{k-1} t_k \cdots t_n + h_k \in I(\mathcal{C})$. By induction on k, our result is proved. It is easy to see that $g_\ell \in \widetilde{S}_{d-(n-\ell+1)}$. $\square$

Proposition 4.2.22 *Let $\mathcal{C}$ be the projective nested product of fields over $K_0, \ldots, K_n$, and let $f \notin I(\mathcal{C})$ be a not necessarily homogeneous polynomial on S of degree at most d and homogeneous on $\mathcal{C}$. If $1 \leq d < \sum\limits_{i=1}^{n} (d_i - 1)$, then*

$$|\mathcal{C} \backslash Z_{\mathcal{C}}(f)| \geq (d_{k+1} - \ell)\, d_{k+2} \cdots d_n\,,$$

where $0 \leq k \leq n-1$ and $0 \leq \ell < d_{k+1} - 1$ are the unique integers such that $d - 1 = \sum\limits_{i=1}^{k} (d_i - 1) + \ell$.

Proof. We will make an induction on n. If $n=1$, then $\mathcal{C}=[K_0\times K_1]$ and set $x:=[(x_0,x_1)]\in\mathcal{C}$. Assume that $x_0\neq 0$, since f is homogeneous on $\mathcal{C}$ we have $f(x_0,x_1)=0$ if and only if $f(1,x_1/x_0)=0$. The last one is a polynomial of degree at most d on x_1/x_0, which has no more than d roots. If f has a root on $[(0,1)]$, then writing $f=t_0g+f_1$, with $f_1\in K[t_1]$ we get that $f_1(a)=0$ for all $a\in K_1$. Hence $f(1,a)=0$ if and only if $g(1,a)=0$ (for all $a\in K_1$), and $g(1,t_1)$ has degree at most $d-1$. In both cases we have

$$|\mathcal{C}\backslash Z_{\mathcal{C}}(f)|\geq (d_1+1)-d=d_1-(d-1)\,.$$

Now we assume that the theorem is valid for the product $[K_0\times K_1\times\cdots\times K_{n-1}]$. Define

$$\mathcal{D}_n^*:=[1\times K_1\times\cdots\times K_n] \text{ and } \mathcal{D}_{n-1}:=[0\times K_1\times\cdots\times K_n].$$

Observe that $\mathcal{C}=\mathcal{D}_n^*\cup\mathcal{D}_{n-1}$. Let $f\notin I(\mathcal{C})$ be a homogeneous polynomial on $\mathcal{C}$ of degree at most d.

Suppose that $f\in I(\mathcal{D}_n^*)$ (so $f\notin I(\mathcal{D}_{n-1})$). From Theorem 3.3.3 (and the fact that K_j is a finite field with d_j elements, for $j=1,\ldots,n$) we get that $I(\mathcal{D}_n^*)$ is generated by $\tilde{\mathcal{G}}=\{t_j^{d_j}-t_jt_0^{d_j-1}\,|\,j=1,\ldots,n\}$. Endowing S with a graded-lexicographic order $\prec$ such that $t_0\prec t_1\prec\cdots\prec t_n$ we get that $\mathrm{lm}(t_j^{d_j}-t_jt_0^{d_j-1})=t_j^{d_j}$, for all $j=1,\ldots,n$. Thus any pair of these leading monomials are coprime, so $\tilde{\mathcal{G}}$ is a Gröbner basis for $I(\mathcal{D}_n^*)$, with respect to $\prec$ (see [75, p. 104]). Dividing f by the elements of $\tilde{\mathcal{G}}$ we find polynomials g_j of degree at most $d-d_j$ $(j=1,\ldots,n)$ such that $f(t)=\sum_{j=1}^n g_j(t)(t_j^{d_j}-t_jt_0^{d_j-1})$. Define $g(t):=\sum_{j=1}^n g_j(t)t_j$, which is a polynomial of degree $\tilde{d}\leq d-d_1+1$. Observe that $g\mid_{\mathcal{D}_{n-1}}=f\mid_{\mathcal{D}_{n-1}}$, which implies that for any $x:=(0,\ldots,0,1,x_{i+1},\ldots x_n)$ and any $\lambda\in K_i^{\neq 0}$ there exists $\tilde{\lambda}\in K_i^{\neq 0}$ such that $g(\lambda x)=f(\lambda x)=\tilde{\lambda}f(x)=\tilde{\lambda}g(x)$. So g is homogeneous on $\mathcal{D}_{n-1}$. Since $f\notin I(\mathcal{D}_{n-1})$, we must have $g\notin I(\mathcal{D}_{n-1})$, and as $\tilde{d}-1\leq d-1-(d_1-1)=\sum\limits_{i=2}^{k}(d_i-1)+\ell$, we can apply the induction hypothesis obtaining

$$|\mathcal{C}\backslash Z_{\mathcal{C}}(f)|=|\mathcal{D}_{n-1}\backslash Z_{\mathcal{D}_{n-1}}(g)|\geq (d_{k+1}-\ell)\,d_{k+2}\cdots d_n.$$

Suppose now that $f\in I(\mathcal{D}_{n-1})$ and write $f=h+t_0g$ where $h(t)=f(0,t_1,\ldots,t_n)$. Since $f|_{\mathcal{D}_{n-1}}=0$ we have $h|_{\mathcal{D}_{n-1}}=0$ and a fortiori $h|_{\mathcal{D}_n^*}=0$ so $h\in I(\mathcal{C})$. Observe that $f|_{\mathcal{D}_n^*}=g|_{\mathcal{D}_n^*}$ and clearly the number of zeros of g in $\mathcal{D}_n^*$ is the same of the number of zeros of $g(1,t_1,\ldots,t_n)$ in the cartesian product $K_1\times\cdots\times K_n$. Since $\deg(g)\leq d-1$ a lower bound for the number of non-zeros of g in $\mathcal{D}_n^*$ may be obtained from Theorem 3.3.12, and we have

$$|\mathcal{C}\backslash Z_{\mathcal{C}}(f)|=|\mathcal{D}_n^*\backslash Z_{\mathcal{D}_n^*}(g)|\geq (d_{k+1}-\ell)\,d_{k+2}\cdots d_n\,.$$

Finally suppose that $f\notin I(\mathcal{D}_n^*)$ and $f\notin I(\mathcal{D}_{n-1})$.

For $k=n-1$, i.e. when $d=\sum\limits_{i=1}^{n-1}(d_i-1)+\ell+1$, we have

$$|\mathcal{D}_n^*\backslash Z_{\mathcal{D}_n^*}(f)|\geq d_n-\ell-1$$

since, as above, we may consider the number of nonzero points of $f(1, t_1, \ldots, t_n)$ in $K_1 \times \cdots \times K_n$ and use Theorem 3.3.12. From $f \notin I(\mathcal{D}_{n-1})$ we get

$$|\mathcal{D}_{n-1} \backslash Z_{\mathcal{D}_{n-1}}(f)| \geq 1\,,$$

which implies

$$|\mathcal{C} \backslash Z_{\mathcal{C}}(f)| \geq d_n - \ell$$

and settles the case $k = n-1$. We treat now the case $k < n-1$, and we start by assuming that $l + d_1 \leq d_{k+1}$.

We have that $d = \sum_{i=1}^{k} (d_i - 1) + \ell + 1$ and $d - 1 = \sum_{i=2}^{k} (d_i - 1) + \ell + d_1 - 1$, then

$$\begin{aligned} |\mathcal{D}_n^* \backslash Z_{\mathcal{D}_n^*}(f)| &\geq (d_{k+1} - \ell - 1) d_{k+2} \cdots d_n\,, \\ |\mathcal{D}_{n-1} \backslash Z_{\mathcal{D}_{n-1}}(f)| &\geq (d_{k+1} - (\ell + d_1 - 1)) d_{k+2} \cdots d_n \geq d_{k+2} \cdots d_n\,. \end{aligned}$$

Adding both inequalities we obtain the desired result.

From now on we can assume that

$$f \notin I(\mathcal{D}_n^*), f \notin I(\mathcal{D}_{n-1}), 0 \leq k < n - 1 \text{ and } l + d_1 > d_{k+1}.$$

In particular $l \geq 1$. In what follows we generalize some methods used by Sørensen [56] to treat projective Reed-Muller codes. Define the set of hyperplanes

$$\Pi := \{\pi = Z(h) \subseteq \mathbb{P}^n \mid h = \lambda_0 t_0 + \cdots + \lambda_{n-1} t_{n-1} + t_n \in K_n[t]\}.$$

For all $\pi \in \Pi$, we want to estimate $|(\pi \cap \mathcal{C}) \backslash Z_{\mathcal{C}}(f))|$.

For each $h = \lambda_0 t_0 + \cdots + \lambda_{n-1} t_{n-1} + t_n$, define $H : \mathbb{P}^n \mapsto \mathbb{P}^n$ by

$$H([(x_0, \ldots, x_n)]) = [(x_0, \ldots, x_{n-1}, h(x_0, \ldots, x_n))]\,.$$

It is easy to see that H is a projectivity that induces a bijection of $\mathcal{C}$ and sends the plane π to the plane $Z(t_n)$, in fact

$$\mathbf{p} \in \pi = Z(h) \Longleftrightarrow H(\mathbf{p}) \in Z(t_n)\,.$$

It is also easy to check that $f(H(t)) := f(t_0, \ldots, t_{n-1}, \lambda_0 t_0 + \cdots + \lambda_{n-1} t_{n-1} + t_n)$ is a polynomial of degree at most d and homogeneous on $\mathcal{C}$, and that the inverse projectivity H^{-1} is the one associated to $h^* = -\lambda_0 t_0 - \cdots - \lambda_{n-1} t_{n-1} + t_n$. Define $g_h(t) := f(H^{-1}(t))$, then we have a bijection between the zeros of f in $\mathcal{C}$ and the zeros of g in $H(\mathcal{C})(= \mathcal{C})$ given by

$$\mathbf{p} \in Z_{\mathcal{C}}(f) \Longleftrightarrow f(\mathbf{p}) = 0 \Longleftrightarrow g_h(H(\mathbf{p})) = 0 \Longleftrightarrow H(\mathbf{p}) \in Z_{\mathcal{C}}(g_h)\,,$$

which implies that $H((Z(h) \cap \mathcal{C}) \backslash Z_{\mathcal{C}}(f)) = (Z(t_n) \cap \mathcal{C}) \backslash Z_{\mathcal{C}}(g_h)$.

To proceed we consider the following cases, regarding the possibility of $Z_{\mathcal{C}}(f)$ to contain or not a set $\pi \cap \mathcal{C}$, with $\pi \in \Pi$.
(a) Assume that $Z_{\mathcal{C}}(f)$ does not contain any set $\pi \cap \mathcal{C}$, where $\pi \in \Pi$, and define the set of pairs

$$\Lambda_f := \{(\mathbf{p}, \pi) \in (\mathcal{C} \backslash Z_{\mathcal{C}}(f)) \times \Pi \mid \mathbf{p} \in \pi\}.$$

Set $\mathcal{C}' := [K_0 \times \cdots \times K_{n-1}]$ and for $\pi = Z(h)$ define $g'_h(t_0, \ldots, t_{n-1}) := g_h(t_0, \ldots, t_{n-1}, 0)$. Since $Z(h) \cap \mathcal{C} \nsubseteq Z_{\mathcal{C}}(f)$ we have that g'_h does not vanish on $\mathcal{C}'$, is homogeneous on $\mathcal{C}'$ and has degree at most d. Thus, from $|(Z(t_n) \cap \mathcal{C}) \backslash Z_{\mathcal{C}}(g_h)| = |\mathcal{C}' \backslash Z_{\mathcal{C}'}(g'_h)|$ and by the induction hypothesis we get that

$$|Z(h) \cap \mathcal{C} \backslash Z_{\mathcal{C}}(f)| \geq (d_{k+1} - \ell)\, d_{k+2} \cdots d_{n-1}.$$

So for each $\pi \in \Pi$ we have at least $(d_{k+1} - \ell)\, d_{k+2} \cdots d_{n-1}$ points $\mathbf{p}$ such that $(\mathbf{p}, \pi) \in \Lambda_f$. From $|\Pi| = d_n^n$ we have

$$|\Lambda_f| \geq (d_{k+1} - \ell)\, d_{k+2} \cdots d_{n-1} d_n^n. \tag{4.2.1}$$

Let $\mathbf{p} := [(b_0, \ldots, b_n)]$ be an element of $\mathcal{C} \backslash Z_{\mathcal{C}}(f)$. If $[(b_0, \ldots, b_{n-1})] \neq 0$ then there are d_n^{n-1} hyperplanes $\pi \in \Pi$ such that $\mathbf{p} \in \pi$. If $\mathbf{p} = [(0, \ldots, 0, 1)]$, there is no hyperplane $\pi \in \Pi$ such that $\mathbf{p} \in \pi$, so

$$|\Lambda_f| \leq |\mathcal{C} \backslash Z_{\mathcal{C}}(f)| d_n^{n-1}. \tag{4.2.2}$$

From (4.2.1) and (4.2.2) we get

$$|\mathcal{C} \backslash Z_{\mathcal{C}}(f)| \geq (d_{k+1} - \ell)\, d_{k+2} \cdots d_n.$$

(b) Assume that $Z_{\mathcal{C}}(f)$ contains a set $\pi \cap \mathcal{C}$, for some $\pi \in \Pi$. To complete the proof we will consider two subcases.

Subcase b.1: Assume that $d_{k+1} < d_n$. Applying the projectivity H corresponding to π and passing from $f(t)$ to $f(H^{-1}(t))$ we may assume that $\pi = Z(t_n)$. From Lemma 4.2.21 there exists a polynomial g of degree at most $d-1$ and homogeneous on $\mathcal{C}$ such that $f - gt_n \in I(\mathcal{C})$, which means $Z_{\mathcal{C}}(f) = Z_{\mathcal{C}}(gt_n)$. For $\widetilde{\mathcal{C}} := [1 \times K_1 \times \cdots \times K_{n-1} \times K_n^{\neq 0}]$ we have $\mathcal{D}_n^* \setminus Z_{\mathcal{D}_n^*}(f) = \widetilde{\mathcal{C}} \setminus Z_{\widetilde{\mathcal{C}}}(g)$. As before we may get a lower bound for $\widetilde{\mathcal{C}} \backslash Z_{\widetilde{\mathcal{C}}}(g)$ by using Theorem 3.3.12 to obtain a lower bound for the number of nonzero points of $g(1, t_1, \ldots, t_n)$ in $K_1 \times \cdots \times K_{n-1} \times K_n^{\neq 0} \in \mathbb{A}^n$. To do this we observe that $g(1, t_1, \ldots, t_n)$ is a polynomial of degree at most $d-1$, and also that $d_1 \leq \cdots \leq d_{n-1}$ and $d_{k+1} \leq d_n - 1$. Thus when we write $K_1, \ldots, K_{n-1}, K_n^{\neq 0}$ in order of increasing size the set $K_n^{\neq 0}$ does not appear before K_{k+1}. In [37] the authors prove that this reordering does not affect the lower bound in Theorem 3.3.12 (2) so we get

$$|\widetilde{\mathcal{C}} \backslash Z_{\widetilde{\mathcal{C}}}(g)| \geq (d_{k+1} - \ell) d_{k+2} \cdots d_{n-1}(d_n - 1).$$

On the set $\mathcal{D}_{n-1}$ we can use the induction hypothesis, observing that $d - 1 = \sum_{i=2}^{k+1} (d_i - 1) + \ell + d_1 - d_{k+1}$ and $0 < \ell + d_1 - d_{k+1} \leq d_{k+2} - 1$, so

$$|\mathcal{D}_{n-1} \backslash Z_{\mathcal{D}_{n-1}}(f)| \geq (d_{k+2} - (\ell + d_1 - d_{k+1})) d_{k+3} \cdots d_n \geq (d_{k+1} - \ell) d_{k+2} \cdots d_{n-1}. \tag{4.2.3}$$

Adding both inequalities, we obtain the desired result.

Subcase b.2: Assume that $d_{k+1} = d_n$. Let $r \in \{1, \ldots, k+1\}$ be the least index such that $K_r = K_{r+1} = \cdots = K_n$. For $r \leq j \leq n$, define

$$\Pi_j := \{\pi = Z(h) \subseteq \mathbb{P}^n \mid h = \lambda_0 t_0 + \cdots + \lambda_{j-1} t_{j-1} + t_j + \lambda_{j+1} t_{j+1} + \cdots + \lambda_n t_n \in K_n[t]\}.$$

If for some $j \in \{r, \ldots, n\}$ all sets $\pi \cap \mathcal{C}$, with $\pi \in \Pi_j$, are not contained in $Z_{\mathcal{C}}(f)$ then we may use an argument similar to the one used in (a) above to obtain the desired result. In this argument we will use Π_j instead of Π, $\mathcal{C}'_j := [K_0 \times \cdots \times \widehat{K_j} \times \cdots \times K_n]$ instead of $\mathcal{C}'$ (where $K_0 \times \cdots \times \widehat{K_j} \times \cdots \times K_n$ means that we omit the set K_j in the product) and for every $h = \lambda_0 t_0 + \cdots + \lambda_{j-1} t_{j-1} + t_j + \lambda_{j+1} t_{j+1} + \cdots + \lambda_n t_n \in K_n[t]$ we will set $g'_h(t_0, \ldots, \widehat{t_j}, \ldots, t_n) := f(t_0, \ldots, t_{j-1}, -\lambda_0 t_0 - \cdots - \lambda_{j-1} t_{j-1} - \lambda_{j+1} t_{j+1} - \cdots - \lambda_n t_n, t_{j+1}, \ldots, t_n)$; at the end we use that $|\Pi_j| = d_n^n = d_j^n$ to conclude the argument and prove the result.

If for every $r \leq j \leq n$ there exists $Z(h_j) = \pi_j \in \Pi_j$ such that $\pi_j \cap \mathcal{C} \subseteq Z_{\mathcal{C}}(f)$ then let H be the projectivity defined by

$$H([(x_0, \ldots, x_n)]) := [(x_0, \ldots, x_{r-1}, h_r(x_0, \ldots, x_n), x_{r+1}, \ldots, x_n)].$$

As before, passing from $f(t)$ to $f(H^{-1}(t))$ we may assume that $Z(t_r) \cap \mathcal{C} \subseteq Z_{\mathcal{C}}(f)$. If all sets $\pi \cap \mathcal{C}$, with $\pi \in \Pi_{r+1}$, are not contained in $Z_{\mathcal{C}}(f)$ then again we may use an argument similar to the one used in (a) above to get the result. If there is some $\pi \in \Pi_{r+1}$ such that $\pi \cap \mathcal{C} \subseteq Z_{\mathcal{C}}(f)$ then using an appropriate projectivity we may assume that $Z(t_{r+1}) \cap \mathcal{C} \subseteq Z_{\mathcal{C}}(f)$ (note that $Z(t_r) \cap \mathcal{C} \subseteq Z_{\mathcal{C}}(f)$ continues to hold). Proceeding in this manner, we either get the result or we get that $Z(t_j) \cap \mathcal{C} \subseteq Z_{\mathcal{C}}(f)$ for all $j = r, \ldots, n$, which we assume from now on. From Lemma 4.2.21, there exists a polynomial $g(t)$ of degree at most $d - (n - r + 1)$, homogeneous on $\mathcal{C}$, such that $f = g \cdot t_r \cdots t_n$. From $f \notin I(\mathcal{D}_n^*)$ we get that g is not zero on the set $\mathcal{E} = [1 \times K_1 \times \cdots \times K_r^* \times \cdots \times K_n^*]$ and also that $|\mathcal{D}_n^* \backslash Z_{\mathcal{D}_n^*}(f)| = |\mathcal{E} \backslash Z_{\mathcal{E}}(g)|$. The number of non-zero points of g in $\mathcal{E}$ is the same of the number of non-zero points of $g(1, t_1, \ldots, t_n)$ in $K_1 \times \cdots \times K_r^* \times \cdots \times K_n^* \in \mathbb{A}^n$. Observe that from the definition of r we get $d_1 \leq \cdots \leq d_{r-1} \leq d_r - 1 = \cdots = d_n - 1$ so we may apply Theorem 3.3.12, noting that $\deg(1, t_1, \ldots, t_n) \leq d - 1 - (n - r)$. To apply that result we write

$$d-1-(n-r) = \sum_{i=1}^{r-1} (d_i - 1) + \sum_{i=r}^{k} ((d_i - 1) - 1) + \ell - (n-k-1) = \sum_{i=1}^{s} \left(\tilde{d}_i - 1\right) + \tilde{\ell}, \quad (4.2.4)$$

where $\tilde{d}_i$, $0 \leq s \leq k$ and $\tilde{\ell}$ are defined by

$$\tilde{d}_i := \begin{cases} d_i & \text{if } 1 \leq i < r, \\ d_i - 1 & \text{if } r \leq i \leq n, \end{cases}$$

$$0 \leq \tilde{\ell} := \sum_{i=s+1}^{k} \left(\tilde{d}_i - 1\right) + \ell - (n - k - 1) < \tilde{d}_{s+1} - 1$$

(we note that if $r = k+1$ then we omit the term $\sum_{i=r}^{k}((d_i - 1) - 1)$ in (4.2.4)). With this notation, from Theorem 3.3.12 we have

$$|\mathcal{E} \backslash Z_{\mathcal{E}}(g)| \geq (\tilde{d}_{s+1} - \tilde{\ell})\tilde{d}_{s+2} \cdots \tilde{d}_n \,.$$

Define $\lambda_{s+1} := d_{s+1} - \tilde{d}_{s+1} + \tilde{\ell}$ and $\lambda_j := d_j - \tilde{d}_j$ for $j = s+2, \ldots, n-1$. Then

$$(\tilde{d}_{s+1} - \tilde{\ell})\tilde{d}_{s+2} \cdots \tilde{d}_{n-1} = \prod_{i=s+1}^{n-1} (d_i - \lambda_i),$$

and we have

$$\begin{aligned} \sum_{i=s+1}^{n-1} \lambda_i &= (d_{s+1} - \tilde{d}_{s+1} + \tilde{\ell}) + \sum_{i=s+2}^{n-1} (d_i - \tilde{d}_i) = \tilde{\ell} + \sum_{i=s+1}^{n-1} (d_i - \tilde{d}_i) \\ &= \sum_{i=s+1}^{k} \left(\tilde{d}_i - 1\right) + \ell - (n-k-1) + \sum_{i=s+1}^{k} (d_i - \tilde{d}_i) + (n-1-k) \\ &= \sum_{i=s+1}^{k} (d_i - 1) + \ell. \end{aligned}$$

Thus, from [9, Lemma 2.1] we get $\prod_{i=s+1}^{n-1}(d_i - \lambda_i) \geq (d_{k+1} - \ell)d_{k+2} \cdots d_{n-1}$, and a fortiori

$$|\mathcal{E} \backslash Z_{\mathcal{E}}(g)| \geq (d_{k+1} - \ell)d_{k+2} \cdots d_{n-1}(d_n - 1).$$

From the induction hypothesis, and similarly as (4.2.3), we have

$$|\mathcal{D}_{n-1} \backslash Z_{\mathcal{D}_{n-1}}(f)| \geq (d_{k+1} - \ell)d_{k+2} \cdots d_{n-1} \,.$$

Adding both inequalities we obtain the desired result. This concludes the proof of the proposition. □

We come to the main result of this section.

Theorem 4.2.23 *If $\mathcal{C}$ is the projective nested product of fields over $K_0, \ldots, K_n$, then the minimum distance of $C_{\mathcal{C}}(d)$ is given by*

$$\delta_{\mathcal{C}}(d) := \begin{cases} (d_{k+1} - \ell)\, d_{k+2} \cdots d_n & \text{if} \quad 1 \leq d \leq \sum_{i=1}^{n} (d_i - 1)\,, \\ 1 & \text{if} \quad \sum_{i=1}^{n} (d_i - 1) < d, \end{cases}$$

where $0 \leq k \leq n-1$ and $0 \leq \ell < d_{k+1} - 1$ are the unique integers such that

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

Proof. Now it is immediate by Lemma 4.2.15 and Proposition 4.2.22. □

As consequences of our main results we have the next applications and examples. We also recover the formula for the length and dimension of the Projective Reed-Muller codes.

Corollary 4.2.24 ([56, Theorem 1]; [51, Proposition 12]) *The Projective Reed-Muller code $PC_d(n,q)$ is an $[|\mathbb{P}^n|, \dim C_{\mathbb{P}^n}(d), \delta_{\mathbb{P}^n}(d)]$-code where*

(a) $|\mathbb{P}^n| = (q^{n+1}-1)/(q-1)$,

(b) $\dim C_{\mathbb{P}^n}(d) = \sum_{j=0}^{n}\sum_{k=0}^{j}(-1)^k \binom{j}{k}\binom{j+d-1-kq}{d-1-kq}$ *and*

(c)

$$\delta_{\mathbb{P}^n}(d) = \begin{cases} q^n & \textit{if} \quad 1 = d, \\ (q-\ell)\, q^{n-k-1} & \textit{if} \quad 1 < d \le n(q-1), \\ 1 & \textit{if} \quad n\,(q-1) < d; \end{cases}$$

here $0 \le k \le n-1$ and $1 \le \ell \le d_{k+1}-1$ are the unique integers such that $d = 1 + k\,(q-1) + \ell$.

Proof. Using Remark 4.2.2 and Theorems 4.2.3, 4.2.9 and 4.2.23 we have the result. □

Now we present a relationship between the parameters of codes defined over a projective nested product of fields and affine cartesian codes.

Corollary 4.2.25 *Let $K_0, \ldots, K_n$ be subfields of K such that $\mathcal{C} := [K_0 \times K_1 \times \cdots \times K_n]$ is a projective nested product of fields and $\mathcal{C}_i^* := K_{n+1-i} \times \cdots \times K_n \subseteq \mathbb{A}^i$, where $i = 1\ldots, n$. If*

$$C_{\mathcal{C}}(d) \quad \textit{is a} \quad [|\mathcal{C}|, \dim C_{\mathcal{C}}(d), \delta_{\mathcal{C}}(d)]\textit{-code}$$

and

$$C_{\mathcal{C}_i^*}(d) \quad \textit{is a} \quad \left[|\mathcal{C}_i^*|, \dim C_{\mathcal{C}_i^*}(d), \delta_{\mathcal{C}_i^*}(d)\right]\textit{-code,}$$

then

$$|\mathcal{C}| = \sum_{i=0}^{n} |\mathcal{C}_i^*|, \qquad \dim C_{\mathcal{C}}(d) = \sum_{i=0}^{n} \dim C_{\mathcal{C}_i^*}(d-1) \qquad \textit{and} \qquad \delta_{\mathcal{C}}(d) = \delta_{\mathcal{C}_n^*}(d-1),$$

where $\mathcal{C}_0^* := [1]$ and $\delta_{\mathcal{C}_n^*}(0) := d_1 \cdots d_n$.

Proof. This is a consequence of Theorems 3.3.5, 3.3.12, 4.2.3, 4.2.9 and 4.2.23. □

Corollary 4.2.26 (Relationship between Generalized and Projective Reed-Muller codes) *If the Projective Reed-Muller code*

$$PC_d(n,q) \quad \textit{is a} \quad [|\mathbb{P}^n|, \dim C_{\mathbb{P}^n}(d), \delta_{\mathbb{P}^n}(d)] \text{ - } \textit{code}$$

and for $i = 1, \ldots, n$ *the Generalized Reed-Muller code*

$$GC_d(i,q) \quad \textit{is a} \quad \left[\left|\mathbb{A}^i\right|, \dim C_{\mathbb{A}^i}(d), \delta_{\mathbb{A}^i}(d)\right] \text{ - } \textit{code} \ ,$$

then

$$|\mathbb{P}^n| = \sum_{i=0}^{n} \left|\mathbb{A}^i\right|, \qquad \dim C_{\mathbb{P}^n}(d) = \sum_{i=0}^{n} \dim C_{\mathbb{A}^i}(d-1) \qquad \textit{and} \qquad \delta_{\mathbb{P}^n}(d) = \delta_{\mathbb{A}^n}(d-1),$$

where $\ell_{\mathbb{A}^0} := 1, k_{\mathbb{A}^0}(d) := 1$ *and* $\delta_{\mathbb{A}^n}(0) := q^n$.

Proof. The generalized Reed-Muller code is an special case of the affine cartesian codes. The projective Reed-Muller code is an especial case of the codes associated with projective nested product of fields. Thus this proof is a consequence of Corollary 4.2.25. □

Example 4.2.27 Let $K := \mathbb{F}_{25}$ be a finite field with 25 elements and let $K_0 := K_1 := \mathbb{F}_5, K_2 := \mathbb{F}_{25}$ be subsets of K. Then $\mathcal{C} := [K_0 \times K_1 \times K_2]$ is a projective nested cartesian product, and the length, the dimension and the minimum distance of the code $C_{\mathcal{C}}(d)$ are:

d	1	2	3	4	5	6	7	8	9	10	25
$\lvert\mathcal{C}\rvert$	151	151	151	151	151	151	151	151	151	151	151
$\dim C_{\mathcal{C}}(d)$	3	6	10	15	21	27	33	39	45	51	141
$\delta_{\mathcal{C}}(d)$	125	100	75	50	25	24	23	22	21	20	5

Appendix A

Main Results of The Thesis

In this appendix we present the main results of this work.

A.1 Main results of Chapter 2

Let K be a field, $S := K[t_1, \ldots, t_n]$ a polynomial ring with n variables over K, $\mathcal{L}_\rho \subset \mathbb{Z}^n$ a lattice and ρ a partial character from $\mathcal{L}_\rho$. Fix a monomial order $\prec$. The following four results are well-known for pure lattice ideals. We prove them for arbitrary lattice ideals.

- **Theorem 2.1.21** *Let K be a field and $\rho : \mathcal{L}_\rho \to K^*$ a partial character. The lattice ideal $I(\rho) = \left(\left\{t^{a^+} - \rho(a)t^{a^-} \mid a \in \mathcal{L}\right\}\right)$ contains no monomials.*

- **Theorem 2.1.23***An ideal $I \subset S$ is a lattice ideal if and only if*
  - (i) *I is binomial,*
  - (ii) *I contains no monomials and*
  - (iii) *$t_i \notin \mathcal{Z}(S/I)$ for all i.*

- **Theorem 2.2.7** *$\mathcal{L}_\rho = \mathbb{Z}\{a_1, \ldots, a_r\}$ if and only if*

$$I(\rho) = \left(t^{a_1^+} - \rho(a_1)t^{a_1^-}, \ldots, t^{a_r^+} - \rho(a_r)t^{a_r^-}\right) : (t_1 \cdots t_n)^\infty .$$

- **Theorem 2.2.9***Let ρ be a partial character on a lattice $\mathcal{L}_\rho$and let $I(\rho)$ be its lattice ideal. If $I(\rho) = \left(t^{a_1} - \lambda_1 t^{b_1}, \ldots, t^{a_r} - \lambda_r t^{b_r}\right)$, then $\mathcal{L}_\rho = \mathbb{Z}\{a_1 - b_1, \ldots, a_r - b_r\}$ and $\rho(a_i - b_i) = \lambda_i$, for $i = 1, \ldots, r$. In particular, if L is a lattice ideal, there are a unique lattice $\mathcal{L}_\rho$ and a unique partial character ρ on the lattice $\mathcal{L}_\rho$ such that $L = I(\rho)$.*

By [16, Corollary 2.5] we know that a binomial ideal containing no monomials is characterized by a lattice. In some way we complement this result. We show that a binomial ideal (without restrictions) can be always characterized by a finite number of lattices.

- **Theorem 2.3.4** *Let K be a field with characteristic different than 2. An ideal I of S is a binomial ideal if and only if there are m lattices $\mathcal{L}_i := \mathbb{Z}\{a_{i1} - b_{i1}, \ldots, a_{1r_i} - b_{1r_i}\}$ and m partial characters $\rho_i \colon \mathcal{L}_i \to K^*$ such that $I = I_1 + \cdots + I_m$, where*
$$I_i := \left(t^{a_{i1}} - \rho_i(a_{i1} - b_{i1})t^{b_{i1}}, \ldots, t^{a_{ir_i}} - \rho_i(a_{ir_i} - b_{ir_i})t^{b_{ir_i}}\right),$$
and for $i \neq j$, the ideal $I_i + I_j$ contains a monomial.

We prove that with a finite number of elements of the lattice we can construct a Gröbner basis of the lattice ideal.

- **Theorem 2.4.1** *Let $\rho \colon \mathcal{L}_\rho \to K^*$ be a partial character and $\prec$ an arbitrary monomial order fixed on S. There are elements $a_1, \ldots, a_s$ of $\mathcal{L}_\rho$ such that*
$$\mathcal{G} := \left\{t^{a_1^+} - \rho(a_1)t^{a_1^-}, \ldots, t^{a_s^+} - \rho(a_s)t^{a_s^-}\right\}$$
is a Gröbner basis of $I(\rho)$. In particular the reduced Gröbner basis has this form.

The following results tell that a Gröbner basis and as a consequence some invariant algebraics of a lattice ideal are independent of the character.

- **Theorem 2.5.1** *Let $\rho \colon \mathcal{L}_\rho \to K^*$ be a partial character and $\prec$ an arbitrary monomial order fixed on S. The set $\mathcal{G} := \left\{t^{a_1^+} - \rho(a_1)t^{a_1^-}, \ldots, t^{a_r^+} - \rho(a_r)t^{a_r^-}\right\}$ is a Gröbner basis of the lattice ideal $I(\rho)$ if and only if the set $\mathcal{G}' := \left\{t^{a_1^+} - t^{a_1^-}, \ldots, t^{a_r^+} - t^{a_r^-}\right\}$ is a Gröbner basis of the pure lattice ideal $I(\mathcal{L}_\rho)$.*
- **Theorem 2.5.2**(Hilbert function of a lattice ideal is independent from the partial character) *If $\mathcal{L}$ is a lattice and ρ, ρ' are two partial characters on $\mathcal{L}$, then*
$$H_\rho(d) = H_{\rho'}(d) \qquad \text{for all } d \geq 0.$$

Let K be a field, $S := K[t_1, \ldots, t_n]$ a polynomial ring with n variables over $K, \mathcal{L}$ a lattice of $\mathbb{Z}^n$ and $\omega := (\omega_1, \ldots, \omega_n)$ a integral vector with positive entries. In the following four results we work with pure lattice ideal, i.e. we use the trivial partial character to define the lattice ideal.

- **Theorem 2.6.12** *If $I(\mathcal{L}) \subset S$ is a graded pure lattice ideal of dimension 1, then*
$$\deg S/I(\mathcal{L}) = |T(\mathbb{Z}^n/\mathcal{L})|.$$

- **Theorem 2.6.31** *Let L be the pure lattice ideal of an ω-homogeneous lattice $\mathcal{L}$ in $\mathbb{Z}^n$. If $V(L,t_i)=\{0\}$ for all i, then L is a complete intersection if and only if there are homogeneous pure binomials $h_1,\ldots,h_{n-1}$ in L satisfying the following conditions*:
  (i) $\mathcal{L}=\mathbb{Z}\left\{\widehat{h}_1,\ldots,\widehat{h}_{n-1}\right\}$.
  (ii) $V(h_1,\ldots,h_{n-1},t_i)=\{0\}$ *for all* i.
  (iii) $h_i=t^{a_i^+}-t^{a_i^-}$ *for* $i=1,\ldots,n-1$.

- **Proposition 2.6.34** *If K is a field of positive characteristic and $L\subset S$ is a ω-graded pure lattice ideal of dimension* 1*, then L is a pure binomial set theoretic complete intersection.*

- **Theorem 2.6.37** *Let $L\subset S$ be an arbitrary pure lattice ideal of height r. If* $\mathrm{char}(K)=0$ *and* $\mathrm{rad}(L)=\mathrm{rad}(g_1,\ldots,g_r)$ *for some pure binomials $g_1,\ldots,g_r$, then $L=(g_1,\ldots,g_r)$.*

Let $K:=\mathbb{F}_q$ be a finite field, $\mathcal{T}:=\{[(x_1^{v_1},\ldots,x_n^{v_n})]\,|\,x_i\in K^*$ for all $i\}\subseteq\mathbb{P}^{n-1}$ a projective degenerate torus of type $v:=(v_1,\ldots,v_n)$, P a toric ideal associated to the numerical semigroup $\mathbb{N}d_1+\cdots+\mathbb{N}d_n$, where β denotes a generator of the cyclic group $(K^*,\,\cdot\,)$ and d_i denotes $o(\beta^{v_i})$, the order of β^{v_i} for $i=1,\ldots,n$.

- **Theorem 2.7.8** (a) *If $I(\mathcal{T})$ is a complete intersection generated by binomials $h_1,\ldots,h_{n-1}$, then P is a complete intersection generated by binomials $g_1,\ldots,g_{n-1}$ such that h_i is equal to $g_i(t_1^{d_1},\ldots,t_n^{d_n})$ for all i.* (b) *If P is a complete intersection generated by binomials $g_1,\ldots,g_{n-1}$, then $I(\mathcal{T})$ is a complete intersection generated by binomials $h_1,\ldots,h_{n-1}$, where h_i is equal to $g_i(t_1^{d_1},\ldots,t_n^{d_n})$ for all i.*

- **Corollary 2.7.14** (i) $\deg(S/I(\mathcal{T}))=d_1\cdots d_n/\gcd(d_1,\ldots,d_n)$.
  (ii) *If $I(\mathcal{T})$ is a complete intersection, then*
  $$\operatorname{reg} S/I(\mathcal{T})=\gcd(d_1,\ldots,d_n)\,g(\mathcal{S}')+\textstyle\sum_{i=1}^n d_i-(n-1),$$
  where $g(\mathcal{S}')$ denotes the Frobenius number of the numerical semigroup $\mathcal{S}'$ generated by $o(\beta^{rv_1}),\ldots,o(\beta^{rv_n})$; and r is the greatest common divisor of $d_1,\ldots,d_n$.

A.2 Main results of Chapter 3

Let $K:=\mathbb{F}_q$ be a finite field with q elements and $v_1,\ldots,v_n$ a sequence of vectors in $\mathbb{N}^s$ with $v_i:=(v_{i1},\ldots,v_{is})$ for $1\le i\le n$. Let $\mathcal{Q}^*=\{(x_1^{v_{11}}\cdots x_s^{v_{1s}},\ldots,x_1^{v_{n1}}\cdots x_s^{v_{ns}})\in\mathbb{A}^n|\,x_i\in K^*$ for all $i\}$ be the affine algebraic toric set.

- **Theorem 3.2.1** *The length of $C_{\mathcal{Q}^*}(d)$ is* $\deg(S[u]/I(\overline{\mathcal{Q}^*}))$.

- **Corollary 3.2.12** *The dimension and the length of $C_{\mathcal{Q}^*}(d)$ can be computed using Gröbner basis.*

Let K be an arbitrary field, $\Lambda_1,\ldots,\Lambda_n$ a collection of non-empty subsets of K, $d_i := |\Lambda_i|$ for $i = 1,\ldots,n$ and $\mathcal{C}^* := \Lambda_1 \times \cdots \times \Lambda_n$ an affine cartesian product.

- **Theorem 3.3.5** *The length of $C_{\mathcal{C}^*}(d)$ 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*

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

- **Theorem 3.3.12** *Let K be a field and let $C_{\mathcal{C}^*}(d)$ be the cartesian evaluation code of degree d on the finite set $\mathcal{C}^* := \Lambda_1 \times \cdots \times \Lambda_n \subset K^n$. If $2 \leq d_i \leq d_{i+1}$ for all i, with $d_i := |\Lambda_i|$, and $d \geq 1$, then the minimum distance of $C_{\mathcal{C}^*}(d)$ is given by*

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

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

Given a non decreasing sequence of positive integers $2 \leq d_1 \leq \cdots \leq d_n$ we construct a cartesian code, over an affine degenerate torus, with prescribed parameters in terms of $d_1,\ldots,d_n$.

- **Theorem 3.3.17** *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 an affine degenerate torus $\mathcal{T}^*$ such that the length of $C_{\mathcal{T}^*}(d)$ is $d_1 \cdots d_n$, its dimension is*

$$\dim_K C_{\mathcal{T}^*}(d) = \binom{n+d}{d} - \sum_{1\leq i\leq n}\binom{n+d-d_i}{d-d_i} + \sum_{i<j}\binom{n+d-(d_i+d_j)}{d-(d_i+d_j)} - \sum_{i<j<k}\binom{n+d-(d_i+d_j+d_k)}{d-(d_i+d_j+d_k)} + \cdots + (-1)^n\binom{n+d-(d_1+\cdots+d_n)}{d-(d_1+\cdots+d_n)},$$

its minimum distance is 1 if $d \geq \sum_{i=1}^{n}(d_i-1)$, and

$$\delta_{\mathcal{T}^*}(d) = (d_{k+1}-\ell)d_{k+2}\cdots d_n \quad \text{if} \quad d \leq \sum_{i=1}^{n}(d_i-1) - 1,$$

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

A.3 Main results of Chapter 4

Let $K := \mathbb{F}_q$ be a finite field, $v := \{v_1, \ldots, v_n\}$ a sequence of positive integers and $\mathcal{T} = \{[(x_1^{v_1}, \ldots, x_n^{v_n})] \,|\, x_i \in K^* \text{ for all } i\} \subset \mathbb{P}^{n-1}$ a projective degenerate torus of type v.

- **Theorem 4.1.1** (i) *The length of $C_{\mathcal{T}}(d)$ is $d_1 \cdots d_n / \gcd(d_1, \ldots, d_n)$.*

  (ii) *If $I(\mathcal{T})$ is a complete intersection, then good codes $C_{\mathcal{T}}(d)$ can occur only if*

  $$d \leq \gcd(d_1, \ldots, d_n)\, g(\mathcal{S}') + \textstyle\sum_{i=1}^{n} d_i - (n-1),$$

  where $g(\mathcal{S}')$ denotes the Frobenius number of the numerical semigroup $\mathcal{S}'$ generated by $o(\beta^{rv_1}), \ldots, o(\beta^{rv_n})$; and r is the greatest common divisor of $d_1, \ldots, d_n$.

Let K be a finite field and $\Lambda_0, \Lambda_1, \ldots, \Lambda_n$ a collection of non-empty subsets of K such that (i) for all $i = 0, \ldots, n$ we have $0 \in \Lambda_i$, and (ii) for every $i = 1, \ldots, n$ we have $\frac{\Lambda_j}{\Lambda_{i-1}} \subset \Lambda_j$ for $j = i, \ldots, n$. Set $\mathcal{C} := [\Lambda_0 \times \Lambda_1 \times \cdots \times \Lambda_n] = \{[(\lambda_0, \cdots, \lambda_n)] | \, a_j \in \Lambda_j \text{ for all } j\} \subset \mathbb{P}^n$ a projective nested cartesian set and $d_i := |\Lambda_i|$ for $i = 0, \ldots, n$.

- **Theorem 4.2.3** *The length of $C_{\mathcal{C}}(d)$ is $m := 1 + \sum_{i=1}^{n} d_i \cdots d_n$.*

- **Theorem 4.2.9** *The dimension of $C_{\mathcal{C}}(d)$ is given by*

$$\dim_K C_{\mathcal{C}}(d) = \sum_{j=0}^{n} \left[\binom{j+d-1}{d-1} - \sum_{n+1-j \leq i \leq n} \binom{j+d-1-d_i}{d-1-d_i} + \right.$$
$$\sum_{i<j} \binom{j+d-1-(d_i+d_j)}{d-1-(d_i+d_j)} - \sum_{i<j<k} \binom{j+d-1-(d_i+d_j+d_k)}{d-1-(d_i+d_j+d_k)}$$
$$\left. + \cdots + (-1)^j \binom{j+d-1-(d_{n+1-j}+\cdots+d_n)}{d-1-(d_{n+1-j}+\cdots+d_n)} \right].$$

- **Proposition4.2.14***Let $\mathcal{C} := [\Lambda_0 \times \cdots \times \Lambda_n]$ be a projective nested cartesian set. The set $\mathcal{G} := \left\{ t_i \prod_{\lambda_j \in \Lambda_j} (t_j - \lambda_j t_i), i < j; i, j = 0, \ldots, n \right\}$ is a Gröbner basis for $I(\mathcal{C})$.*

- **Conjecture 4.2.16***If $\mathcal{C}$ is the projective nested cartesian set over $\Lambda_0, \ldots, \Lambda_n$, then the minimum distance of $C_{\mathcal{C}}(d)$ is given by*

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

  where $0 \leq k \leq n-1$ and $0 \leq \ell < d_{k+1} - 1$ are the unique integers such that $d - 1 = \sum\limits_{i=1}^{k} (d_i - 1) + \ell$.

In addition, assume that every Λ_i is a field.

- **Theorem 4.2.23** *If $\mathcal{C}$ is the projective nested product of fields over $K_0, \ldots, K_n$, then the minimum distance of $C_{\mathcal{C}}(d)$ is given by*

$$\delta_{\mathcal{C}}(d) := \begin{cases} (d_{k+1} - \ell)\, d_{k+2} \cdots d_n & \text{if} \quad 1 \leq d \leq \sum_{i=1}^{n} (d_i - 1)\,, \\ 1 & \text{if} \quad \sum_{i=1}^{n} (d_i - 1) < d, \end{cases}$$

where $0 \leq k \leq n-1$ and $0 \leq \ell < d_{k+1} - 1$ are the unique integers such that

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

As a consequence, we show some relations between affine codes and projective codes.

- **Corollary 4.2.25** *Let $K_0, \ldots, K_n$ be subfields of K such that $\mathcal{C} := [K_0 \times K_1 \times \cdots \times K_n]$ is a projective nested product of fields and $\mathcal{C}_i^* := K_{n+1-i} \times \cdots \times K_n \subseteq \mathbb{A}^i$, where $i = 1 \ldots, n$. If*

$$C_{\mathcal{C}}(d) \quad \textit{is a} \quad [|\mathcal{C}|\,, \dim C_{\mathcal{C}}(d), \delta_{\mathcal{C}}(d)]\text{-}\textit{code}$$

and

$$C_{\mathcal{C}_i^*}(d) \quad \textit{is a} \quad \left[|\mathcal{C}_i^*|\,, \dim C_{\mathcal{C}_i^*}(d), \delta_{\mathcal{C}_i^*}(d)\right]\text{-}\textit{code},$$

then

$$|\mathcal{C}| = \sum_{i=0}^{n} |\mathcal{C}_i^*|\,, \qquad \dim C_{\mathcal{C}}(d) = \sum_{i=0}^{n} \dim C_{\mathcal{C}_i^*}(d-1) \qquad \textit{and} \qquad \delta_{\mathcal{C}}(d) = \delta_{\mathcal{C}_n^*}(d-1),$$

where $\mathcal{C}_0^* := [1]$ and $\delta_{\mathcal{C}_n^*}(0) := d_1 \cdots d_n$.

- **Corollary 4.2.26** (Relationship between Generalized and Projective Reed-Muller codes). *If the Projective Reed-Muller code*

$$PC_d(n, q) \quad \textit{is a} \quad [|\mathbb{P}^n|\,, \dim C_{\mathbb{P}^n}(d), \delta_{\mathbb{P}^n}(d)] \text{ - } \textit{code}$$

and for $i = 1, \ldots, n$ the Generalized Reed-Muller code

$$GC_d(i, q) \quad \textit{is a} \quad \left[\left|\mathbb{A}^i\right|, \dim C_{\mathbb{A}^i}(d), \delta_{\mathbb{A}^i}(d)\right] \text{ - } \textit{code}\ ,$$

then

$$|\mathbb{P}^n| = \sum_{i=0}^{n} \left|\mathbb{A}^i\right|, \qquad \dim C_{\mathbb{P}^n}(d) = \sum_{i=0}^{n} \dim C_{\mathbb{A}^i}(d-1) \qquad \textit{and} \qquad \delta_{\mathbb{P}^n}(d) = \delta_{\mathbb{A}^n}(d-1),$$

where $\ell_{\mathbb{A}^0} := 1, k_{\mathbb{A}^0}(d) := 1$ and $\delta_{\mathbb{A}^n}(0) := q^n$.

Bibliography

[1] N. Alon, Combinatorial Nullstellensatz, Recent trends in combinatorics (Matŕaháza, 1995), Combin. Probab. Comput. **8** (1999), no. 1-2, 7–29.

[2] M. Barile, M. Morales and A. Thoma, Set-theoretic complete intersections on binomials, Proc. Amer. Math. Soc. **130** (2002), 1893–1903.

[3] D. Bayer and M. Stillman, Computation of Hilbert functions, J. Symbolic Comput. **14** (1992), 31–50.

[4] I. Bermejo, I. García-Marco and J. Salazar-González, An algorithm for checking whether the toric ideal of an affine monomial curve is a complete intersection, J. Symbolic Comput. **42** (2007), 971-991.

[5] I. Bermejo, I. García-Marco and J. Salazar-González, cimonom.lib, A SINGULAR 3.0.3 library for determining whether the toric ideal of an affine monomial curve is a complete intersection, 2007.

[6] I. Bermejo, P. Gimenez, E. Reyes and R. Villarreal, Complete intersections in affine monomial curves, Bol. Soc. Mat. Mexicana (3) **11** (2005), 191–203.

[7] A. Bigatti, Computation of Hilbert-Poincaré series, J. Pure Applied Algebra **119** (1997), 237–253.

[8] M. Borges-Quintana, M Borges-Trenard, P. Fitzpatrick and E. Martínez-Moro, Gröbner bases and combinatorics for binary codes, Applicable Algebra in Engineering, Communication and Computing, **19** (2008), no. 5, 393–411.

[9] C. Carvalho, On the second Hamming weight of some Reed-Muller type codes, Finite Fields **24** (2013), 88–94.

[10] H. Charalambous, A. Thoma and M. Vladoiu, Markov Bases of Lattice Ideals, preprint arXiv:1303.2303v2.

[11] E. Davis, A. Geramita and P. Maroscia, Perfect homogeneous ideals: Dubreil's theorems revisited, Bull. Sci. Math. **108** (1984), no. 2, 143–185.

[12] C. Delorme, Sous-monoides d'intersection complète de ℕ, Ann. Sci. École Norm. Sup. **9** (1976), 145–154.

[13] P. Delsarte, J. Goethals and F. MacWilliams, On generalized Reed-Muller codes and their relatives, Information and Control **16** (1970), 403–442.

[14] I. Duursma, C. Rentería and H. Tapia-Recillas, Reed-Muller codes on complete intersections, Appl. Algebra Engrg. Comm. Comput. **11** (2001), no. 6, 455–462.

[15] S. Eliahou, Idéaux de définition des courbes monomiales, in *Complete Intersections* (S. Greco and R. Strano, Eds.), Lecture Notes in Mathematics **1092**, Springer-Verlag, Heidelberg, 1984, pp. 229–240.

[16] D. Eisenbud and B. Sturmfels, Binomial ideals, Duke Math. J. **84** (1996), 1–45.

[17] S. Eliahou and R. Villarreal, On systems of binomials in the ideal of a toric variety, Proc. Amer. Math. Soc. **130** (2002), 345–351.

[18] C. Escobar, J. Martínez-Bernal and R. Villarreal, Relative volumes and minors in monomial subrings, Linear Algebra Appl. **374** (2003), 275–290.

[19] K. Eto, When is a binomial ideal equal to a lattice ideal up to radical?, Contemp. Math. **331** (2003), 111–118.

[20] J. Fitzgerald and R. Lax, Decoding affine variety codes using Göbner bases, Des. Codes and Cryptogr., **13** (1998),147–158.

[21] A. Geramita, M. Kreuzer and L. Robbiano, Cayley-Bacharach schemes and their canonical modules, Trans. Amer. Math. Soc. **339** (1993), no. 1, 163–189.

[22] 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.

[23] M. González-Sarabia and C. Rentería, Evaluation codes associated to complete bipartite graphs, Int. J. Algebra **2** (2008), no. 1-4, 163–170.

[24] M. González-Sarabia, C. Rentería and M. Hernández de la Torre, Minimum distance and second generalized Hamming weight of two particular linear codes, Congr. Numer. **161** (2003), 105–116.

[25] 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.

[26] M. González-Sarabia, C. Rentería and A. Sánchez-Hernández, Minimum distance of some evaluation codes, preprint, 2011.

[27] 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.

[28] J. Hansen, Linkage and codes on complete intersections, Appl. Algebra Engrg. Comm. Comput. **14** (2003), no. 3, 175–185

[29] R. Hemmecke and P. Malkin, Computing generating sets of lattice ideals and Markov bases of lattices, Journal of Symbolic Computation **44** (2009) 1463–1476.

[30] J. Herzog, Generators and relations of abelian semigroups and semigroup rings, Manuscripta Math. **3** (1970), 175–193.

[31] M. Hochster, Rings of invariants of tori, Cohen-Macaulay rings generated by monomials and polytopes, Ann. of Math. **96** (1972), 318–337.

[32] M. Hochster, Some applications of the Frobenius in characteristic 0, Bull. Amer. Math. Soc. **84** (1978), 886–912.

[33] D. Joyner, Toric codes over finite fields, Appl. Algebra Engrg. Comm. Comput. **15** (2004), no. 1, 63–79.

[34] A. Katsabekis, M. Morales and A. Thoma, Binomial generation of the radical of a lattice ideal, J. Algebra **324** (2010), no. 6, 1334–1346.

[35] G. Lachaud, The parameters of projective Reed-Muller codes, Discrete Math. **81** (1990), no. 2, 217–221.

[36] H. López, Master in Science Thesis, CINVESTAV-IPN, 2010.

[37] H. López, C. Rentería-Márquez and R. Villarreal, Affine cartesian codes, Designs, Codes and Cryptography **71** (2014), no. 1, 5–19.

[38] H. López, E. Sarmiento, M. Vaz Pinto and R. Villarreal, Parameterized affine codes, Studia Sci. Math. Hungar., **49** (2012), no. 3, 406–418.

[39] H. López and R. Villarreal, Complete intersections in binomial and lattice ideals, International Journal of Algebra and Computation, **23** (2013), no. 6, 1419–1429.

[40] H. López and R. Villarreal, Computing the degree of a lattice ideal of dimension one, Journal of Symbolic Computation, **65** (2014), 15–28.

[41] H. López, R. Villarreal and L. Zárate, Complete intersection vanishing ideals on degenerate tori over finite fields, Arab. J. Math. (Springer) **2** (2013), no. 2, 189–197.

[42] I. Márquez-Corbella, E. Martínez-Moro, E. Suárez-Canedo, On the ideal associated to a linear code, Preprint, arXiv 1206.5124

[43] T. T. Moh, Set-theoretic complete intersections, Proc. Amer. Math. Soc. **94** (1985), 217–220.

[44] M. Morales and A. Thoma, Complete intersection lattice ideals, J. Algebra **284** (2005), 755–770.

[45] J. Neves, M. Vaz Pinto and R. Villarreal, Vanishing ideals over graphs and even cycles, Communications in Algebra **43** (2015), 1050–1075.

[46] L. O'Carroll, F. Planas-Vilanova and R. Villarreal, Degree and algebraic properties of lattice and matrix ideals, SIAM J. Discrete Math. **28**, no. 1, 394–427.

[47] M. Ohtani, Graphs and ideals generated by some 2-minors, Comm. Algebra **39** (2011), no. 3, 905–917.

[48] J. Ramírez Alfonsín, *The Diophantine Frobenius problem*, Oxford Lecture Series in Mathematics and its Applications, **30**, Oxford University Press, Oxford, 2005.

[49] C. Rentería, A. Simis and R. Villarreal, Algebraic methods for parameterized codes and invariants of vanishing ideals over finite fields, Finite Fields Appl. **17** (2011), no. 1, 81–104.

[50] C. Rentería and H. Tapia-Recillas, Linear codes associated to the ideal of points in $\mathbf{P}^d$ and its canonical module, Comm. Algebra **24** (1996), no. 3, 1083–1090.

[51] C. Rentería and H. Tapia-Recillas, Reed-Muller codes: an ideal theory approach, Commu. Algebra, **25** (1997), no. 2, 401–413.

[52] M. Saleemi and K. Zimmermann, Groebner basis for linear codes over GF(4), International Journal of Pure and Applied Mathematics **73** (2011), no. 4, 435–442.

[53] M. Saleemi and K. Zimmermann, Linear codes as binomial ideals, International Journal of Pure and Applied Mathematics **61** (2010), no. 2, 147–156.

[54] E. Sarmiento, M. Vaz Pinto and R. Villarreal, The minimum distance of parameterized codes on projective tori, Appl. Algebra Engrg. Comm. Comput. **22** (2011), no. 4, 249–264.

[55] E. Sarmiento, M. Vaz Pinto and R. Villarreal, On the vanishing ideal of an algebraic toric set and its parameterized linear codes, J. Algebra Appl. 11 (2012), no. 4, 1250072.

[56] A. Sørensen, Projective Reed-Muller codes, IEEE Trans. Inform. Theory **37** (1991), no. 6, 1567–1576.

[57] R. Stanley, Hilbert functions of graded algebras, Adv. Math. **28** (1978), 57–83.

[58] A. Thoma, On the set-theoretic complete intersection problem for monomial curves in $\mathbb{A}^n$ and $\mathbb{P}^n$, J. Pure Applied Algebra **104** (1995), 333-344.

[59] S. Tohăneanu, Lower bounds on minimal distance of evaluation codes, Appl. Algebra Engrg. Comm. Comput. **20** (2009), no. 5-6, 351–360.

[60] A. Vardy, Algorithmic complexity in coding theory and the minimum distance problem, STOC'97 (El Paso, TX), 92109 (electronic), ACM, New York, 1999.

Computational Algebraic Systems

[61] D. Grayson and M. Stillman, *Macaulay*2, a software system for research in algebraic geometry, 1996. Avalaible from `http://www.math.uiuc.edu/Macaulay2/`.

[62] W. Bruns and B. Ichim, *Normaliz 2.0*, Computing normalizations of affine semigroups 2008. Available from `http://www.math.uos.de/normaliz`.

[63] *CoCoA*, Computations in Commutative Algebra Available from `http://cocoa.dima.unige.it/`.

[64] B. Char, K. Geddes, G. Gonnet and S. Watt, Maple V Language Reference Manual, Springer-Verlag, Berlin, 1991.

[65] G. Gert-Martin Greuel and P. Gerhard, *A* **Singular** *introduction to Commutative Algebra*, Springer-Verlag 2002, 2008. Available from `http://www.singular.uni-kl.de/`.

Books

[66] W. Adams and P. Loustaunau, *An Introduction to Gröbner Bases*, GSM **3**, American Mathematical Society, 1994.

[67] J. Alperin and R. Bell, *Groups and representations*, Graduate Texts in Mathematics **162**, Springer-Verlag, 1995.

[68] A. Altman and S. Kleiman, *A Term of Commutative Algebra*, Worldwide Center of Mathematics, version of September 3, 2012.

[69] M. Beck and S. Robins, *Computing the continuous discretely*, Springer, New York, 2007.

[70] T. Becker and V. Weispfenning, *Gröbner Bases - A computational approach to commutative algebra*, Berlin, Germany: Springer Verlag, 1998, 2nd. pr.

[71] C. Berge, *Graphs and hypergraphs*, North-Holland Mathematical Library, Vol. 6, North-Holland Publishing Co., Amsterdam-London; American Elsevier Publishing Co., Inc., New York, 1976.

[72] J. Bondy and U. Murty, *Graph Theory*, Graduate Texts in Mathematics **244**, Springer-Verlag, 2008.

[73] W. Bruns and J. Herzog, *Cohen-Macaulay Rings*, Cambridge University Press, Cambridge, Revised Edition, 1997.

[74] G. Cornuéjols, *Combinatorial optimization: Packing and covering*, CBMS-NSF Regional Conference Series in Applied Mathematics 74, SIAM (2001).

[75] D. Cox, J. Little and D. O'Shea, *Ideals, Varieties and Algorithms*, Springer-Verlag, 1992.

[76] D. Cox, J. Little and D. O'Shea, *Using Algebraic Geometry*, Graduate Texts in Mathematics **185**, Springer-Verlag, 1998.

[77] R. Diestel, Graph Theory, Graduate Texts in Mathematics **173**, Springer-Verlag, New York, 2005.

[78] D. Eisenbud, *Commutative Algebra with a view toward Algebraic Geometry*, Graduate Texts in Mathematics **150**, Springer-Verlag, 1995.

[79] D. Eisenbud, D. Grayson and M. Stillman, eds., *Computations in algebraic geometry with Macaulay 2*, Algorithms and Computation in Mathematics **8**, Springer-Verlag, Berlin, 2002.

[80] D. Eisenbud, *A second course in Commutative Algebra and Algebraic Geometry*, Copyright David Eisenbud, 2002. http://www.msri.org/people/staff/de/ready.pdf.

[81] S. Eliahou, *Courbes monomiales et algèbre de Rees symbolique*, PhD thesis, Université de Genève, 1983.

[82] V. Ene and J. Herzog, *Gröbner Bases in Commutative Algebra*, Graduate Studies in Mathematics **130**, American Mathematical Society, Providence, RI, 2012.

[83] W. Fulton, *Introduction to Toric Varieties* Princeton University Press, 1993.

[84] R. Gilmer, *Commutative Semigroup Rings,* Chicago Lectures in Math., Univ. of Chicago Press, Chicago, 1984.

[85] M. Golumbic, *Algorithmic graph theory and perfect graphs*, second edition, Annals of Discrete Mathematics 57, Elsevier Science B.V., Amsterdam, 2004.

[86] J. Harris, *Algebraic Geometry. A first course*, Graduate Texts in Mathematics **133**, Springer-Verlag, New York, 1992.

[87] N. Jacobson, *Basic Algebra I*, Second Edition, W. H. Freeman and Company, New York, 1996.

[88] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-correcting Codes, North-Holland, 1977.

[89] H. Matsumura, *Commutative Algebra*, Benjamin-Cummings, Reading, MA, 1980.

[90] H. Matsumura, *Commutative Ring Theory*, Cambridge Studies in Advance Mathematics **8**, Cambridge University Press, 1986.

[91] E. Miller and B. Sturmfels, *Combinatorial Commutative Algebra*, Graduate Texts in Mathematics **227**, Springer, 2004.

[92] M. Newman, *Integral Matrices*, Pure and Applied Mathematics **45** , Academic Press, New York, 1972.

[93] W. M. Schmidt, *Equations over finite fields, An elementary approach*, Lecture Notes in Mathematics **536**, Springer-Verlag, Berlin-New York, 1976.

[94] A. Schrijver, *Combinatorial Optimization*, Algorithms and Combinatorics **24**, Springer-Verlag, Berlin, 2003.

[95] R. Stanley, *Enumerative Combinatorics I*, Wadsworth-Brooks/Cole, Monterey, California, 1986.

[96] I. Stewart and D. Tall, *Algebraic Number Theory*, Chapman and Hall Mathematics Series, 1979.

[97] B. Sturmfels, *Gröbner Bases and Convex Polytopes*, University Lecture Series **8**, American Mathematical Society, Rhode Island, 1996.

[98] H. Stichtenoth, *Algebraic function fields and codes*, Universitext, Springer-Verlag, Berlin, 1993.

[99] M. Tsfasman, S. Vladut and D. Nogin, *Algebraic geometric codes*: *basic notions*, Mathematical Surveys and Monographs **139**, American Mathematical Society, Providence, RI, 2007.

[100] J. Van Lint, *Introduction to coding theory*, Third edition, Graduate Texts in Mathematics **86**, Springer-Verlag, Berlin, 1999.

[101] R. Villarreal, *Combinatorial Optimization Methods in Commutative Algebra,* Preliminary version, Mexico City, D.F., March 12, 2012.

[102] R. Villarreal, *Monomial Algebras*, Monographs and Textbooks in Pure and Applied Mathematics **238**, Marcel Dekker, New York, 2001.

[103] R. Villarreal, *Monomial Algebras*, Second Edition, Monographs and Textbooks in Pure and Applied Mathematics, CRC Press, 2015.

Notation

C code, xvi
$C_{\mathcal{C}^*}(d)$ affine cartesian code, xix, 68
$C_{\mathcal{C}}(d)$ proj. nested cart. code, xxii, 83
$C_{\mathcal{Q}^*}(d)$ parameterized affine code, xix, 61
$C_{\mathcal{T}}(d)$ parameterized projective code, xxi
$C_{\mathcal{X}^*}(d)$ affine code, xvii, 59
$C_{\mathcal{X}}(d)$ projective code, xxi
$E\,(\mathbf{G})$ set of edges of a graph, 4
$GC_d(i,q)$ gene. Reed-Muller code, 91
HP_I Hilbert series of S/I, 12
H_I Hilbert function of S/I, 12
$H_{\mathcal{X}^*}(d)$ Hilbert function of $S/I(\mathcal{X}^*)$, xvii
$H_{\overline{\mathcal{X}^*}}(d)$ Hilbert func. of $S[u]/I(\overline{\mathcal{X}^*})$, xviii
$I(\mathcal{L})$ pure lattice ideal, xi, 22
$I(\mathcal{Q})$ vanishing ideal of $\mathcal{Q}$, xiv
$I(\mathcal{T})$ vanishing ideal of $\mathcal{T}$, xiv
$I(\mathcal{X})$ vanishing ideal of $\mathcal{X}$, 2
$I(\mathcal{X}^*)$ vanishing ideal of $\mathcal{X}^*$, xvii, 2
$I(\rho)$ lattice ideal, xi, 22
$I(\overline{\mathcal{X}^*})$ vanishing ideal of $\overline{\mathcal{X}^*}$, xvii
$I : J$ ideal quotient, 6
$I : J^\infty$ saturation, 6
$I_{\mathcal{A}}$ toric ideal, 18
K a field, xi
$K[\mathcal{F}]$ mono. subring generated by $\mathcal{F}$, 17
K^* multiplicative group of K, xi
P toric ideal, xiv
$PC_d(n,q)$ proj. Reed-Muller code, 83, 91
$P_{\mathcal{F}}$ toric ideal, 18
R ring, 11
S polynomial ring, xi, 1
$S_{\leq d}$ polynomials of degree at most d, xvi
S_d homogeneous polynomials of deg. d, 1
T projective torus, 3
$T(M)$ torsion subgroup, 4
T^* affine torus, 3
$V(I)$ variety of an ideal, 2, 86
$V\,(\mathbf{G})$ set of vertices of the graph $\mathbf{G}$, 4
$\Delta(I)$ footprint, 87
αt^a is a term, where $\alpha \in K$, 1
$\deg(S/I)$ degree of an ideal, 13
$\deg(\mathbf{x})$ degree of a vertex, 4
$\deg_{\prec}(f)$ degree of a polynomial, 8
$\delta(C)$ minimum distance of a code, xvi
$\dim(M)$ dimension of a module, 15
$\dim(R)$ Krull dimension of a ring, 6
$\dim(S/I(\mathcal{X}^*))$ Krull dimension, xvii
$\dim(S[u]/I(\overline{\mathcal{X}^*}))$ Krull dimension, xviii
$\dim(\mathcal{P})$ dimension of a polytope, 4
$\dim_K C$ dimension of a code, xvi
$\dim_{\mathbb{R}}(\mathbb{R}\mathcal{A}')$ dimen. as $\mathbb{R}$-vector space, 4
$\ell(M)$ length of a module, 15
$\ell_R(M)$ length of a R-module, 15
$\frac{\Lambda}{\Lambda'}$ the set $\left\{\frac{\lambda}{\lambda'} \mid \lambda \in \Lambda, 0 \neq \lambda' \in \Lambda'\right\}$, 82
$\langle V(\mathbf{H})\rangle$ induced subgraph, 5
$\mathbb{A}^n$ affine space, xvi
$\mathbb{A}^n_K$ affine space over a field K, 2
$\mathbb{F}_q$ finite field, xiv
$\mathbb{N}_+$ abbreviation for $\{1, 2, \ldots\}$, 1
$\mathbb{N}$ abbreviation for $\mathbb{Z}_{\geq 0}$, 1
$\mathbb{P}^n$ projective space, xxi
$\mathbb{P}^n_K$ projective space over a field K, 2
$\mathbb{R}$ real numbers, 1
$\mathbb{R}_+$ abbreviation for $\mathbb{R}_{\geq 0}$, 1
$\mathbb{R}_{\geq d}$ real numbers $\geq d$, 1
$\mathbb{Z}$ integers, 1
$\mathbb{Z}\mathcal{A}$ lattice generated by $\mathcal{A}$, 22
$\mathbb{Z}_{\geq d}$ integers $\geq d$, 1
$\mathcal{C}$ projective cartesian product, xxii, 82
$\mathcal{C}^*$ affine cartesian product, xix

$\mathcal{G}$ Gröbner basis, 9
$\mathcal{K}_n$ complete graph, 5
$\mathcal{K}_{1,n}$ star, 5
$\mathcal{K}_{m,n}$ complete bipartite graph, 5
$\mathcal{L}$ lattice, 22
$\mathcal{L}_\rho$ lattice, xi
$\mathcal{O}$ lattice d-simplex, 41
$\mathcal{P}$ lattice polytope, 3
$\mathcal{Q}$ projective algebraic toric set, xiv, 3
$\mathcal{Q}^*$ affine algebraic toric set, xviii, 3
$\mathcal{S}$ semigroup, xiv
$\mathcal{T}$ projective degenerate torus, xiv, xxi, 3
$\mathcal{T}^*$ affine degenerate torus, 3
$\mathcal{X}$ projective set, xxi
$\mathcal{X}^*$ affine set, xvi
$\mathcal{Z}(M)$ zero divisors of a module, 14
$\mathfrak{f}(a)$ abbr. for $t^{a^+} - \rho(a)t^{a^-}$, 24
$\mathfrak{g}(\gamma, b_1, b_2)$ abbreviation for the polynomial $\rho(b_2)t^{\gamma-b_2} - \rho(b_1)t^{\gamma-b_1}$, 24
$\mathfrak{m}$ maximal ideal, 15
$\mathfrak{p}$ prime ideal, 6
$\overline{b}^{\mathcal{A}}$ the element $b \ominus a_{b1} \ominus \cdots \ominus a_{bs}$, 28
$\overline{f}^{\mathcal{F}}$ remainder of f by $\mathcal{F}$, 9
$\sqrt{I}$ radical, 6
$\succ$ monomial order, 8
$\succ_{Dp}$ degree lexicographical order, 8
$\succ_{dp}$ degree reverse lex. order, 8
$\succ_{lex}$ lexicographical order, 8
$\succ_{revlex}$ reverse lexicographical order, 8
$\mathrm{LC}(f)$ lead. coefficient of a polynomial, 9
$\mathrm{LM}(f)$ lead. mono. of a polynomial, 9
$\mathrm{LT}(f)$ leading term of a polynomial, 9
$\mathrm{S}(f, g)$ S-polynomial of f and g, 10
$\mathrm{ann}(y)$ annihilator of an element, 15
$\mathrm{ann}_R(M)$ annihilator of a module, 15
$\mathrm{codim}(M)$ codimension of a module, 15
$\mathrm{conv}(\mathfrak{B})$ convex hull of $\mathfrak{B}$, 3
$\deg_{t_i}(f)$ deg. respect to t_i of a poly., 9
$\deg_{total}(f)$ total degree of a polynomial, 9
$\mathrm{depth}(M)$ depth of a module, 15
$\gcd(\mathrm{LM}(f), \mathrm{LM}(g))$ grtst. com. div., 10
$\mathrm{ht}(I)$ height of an ideal, 6
$\mathrm{ht}(\mathfrak{p})$ height of a prime ideal, 6
$\mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))$ least com. mult., 10
$\mathrm{multideg}(f)$ multideg. of a polynomial, 8
$\mathrm{rad}(I)$ radical of an ideal, 6
$\mathrm{supp}(c)$ support of a vector, 22
$\mathrm{supp}(f)$ support of a binomial, 22
$\mathrm{supp}(t^a)$ support of a monomial, 22
φ_d evaluation map (proj. case), xxi, 81
$a(I)$ a-invariant of an ideal, 13
$a(S/I)$ a-invariant of an ideal, 13
c^+ positive part of a vector, 22
c^- negative part of a vector, 22
$d(\mathbf{x}, \mathbf{y})$ distance between vertices, 6
$h_I(t)$ Hilbert polynomial of S/I, 13
$h_{\mathcal{X}^*}(t)$ Hilbert poly. of $S/I(\mathcal{X}^*)$, xvii
$h_{\overline{\mathcal{X}^*}}(t)$ Hilbert poly. of $S[u]/I(\overline{\mathcal{X}^*})$, xviii
t^a abbreviation for $t_1^{a_1} \cdots t_n^{a_n}$, 1, 22
$\mathbf{G}$ graph, 4
$\mathbf{G}[V(\mathbf{H})]$ induced subgraph, 5
$\mathbf{H} = \mathbf{G}_{V(\mathbf{H})}$ induced subgraph, 5
$\mathrm{LT}(I)$ initial ideal, 9
ev_d evaluation map (affine case), xvi
$\mathrm{reg}(S/I)$ index of regularity of S/I, 13
$\mathrm{reg}\left(S[u]/I(\overline{\mathcal{X}^*})\right)$ index of regularity, xviii
$\#$ cardinality of a set, 86

Index

a-invariant of an ideal, 13

adjacent vertices, 4
affine
  algebraic toric set, xix, 3
  cartesian code, xix, 68
  cartesian product, xix, 67
  code, xvii, 59
  code parameterized, xix
  degenerate torus, 3
  evaluation code, xvii, 59
  evaluation map, 59
  Hilbert function, 61
  set, xvi
  space, xvi, 2
  torus, 3
algorithm division, 9
annihilator
  of a module, 15
  of an element, 15
ascending chain condition, 7
associated matrix, 18

basic parameters, xvi
binary code, xvi
binomial, 22
  ideal, 22
  pure, 22
  pure primitive, 18
  set theoretic complete intersection, 47
  support of a, 22
bipartite graph, 5
bipartition, 5

code, xvi
  q-ary, xvi
  affine, xvii, 59
  affine cartesian, xix, 68
  affine evaluation, xvii, 59
  associated to a graph, 67
  basic parameters, xvi
  binary, xvi
  dimension, xvi
  length, xvi
  linear, xvi, 59
  maximum distance separable, xvi
  minimum distance, xvi
  parameterized affine, xix, 61
  parameterized projective, xxi, 82
  projective, xviii, xxi, 60, 81
  projective cartesian, 82
  projective evaluation, xviii, xxi, 60, 81
  projective nested cartesian, xxii, 83
  ternary, xvi
codimension
  of a module, 15
  of an ideal, 6
Cohen-Macaulay
  module, 15, 16
  ring, 15, 16
complete
  bipartite graph, 5
  graph, 5
  intersection, 7, 51
composition series, 15
congruence, 23
connected
  component even, 5
  component odd, 5
  components, 5

graph, 5
convex
combination, 3
hull, 3
set, 3
cycle, 5
even, 5
odd, 5

degree
of a vertex, 4
of an ideal, 13
depth of a module, 15
dimension
code, xvi
Krull, 6
of a lattice polytope, 4
of a module, 15
of an ideal, 6
distance between vertices, 6
division algorithm, 9

edges set, 4
ends, 4
endvertices, 4
evaluation code
affine, xvii, 59
projective, xviii, xxi, 60, 81
evaluation map
(affine case), xvi, 59
(projective case), xxi

footprint, 87
forest, 5
Frobenius number, xv, 56
function Hilbert, 12
of $S/I(\mathcal{X}^*)$, xvii
of $S[u]/I(\overline{\mathcal{X}^*})$, xviii

Gröbner basis, 9
minimal, 11
reduced, 11
universal, 19
graded
ideal, 12
ring, 11
graph, 4
bipartite, 5
complete, 5
complete bipartite, 5
connected, 5
discrete, 5
invariant, 5
order of a, 5
graphs
automorphism of, 5
homomorphism of, 4
isomorphic, 4
group
torsion free, 4

height
of a prime ideal, 6
of an ideal, 6
Hilbert
function, 12
function affine, 61
function of $S/I(\mathcal{X}^*)$, xvii
function of $S[u]/I(\overline{\mathcal{X}^*})$, xviii
polynomial, 13
series, 12
homogeneous
elements of degree d, 11
ideal, 12
lattice, 36
homogenization
of a polynomial, 66
of an ideal, 66
homomorphism of graphs, 4

ideal
ω-graded, 12
a-invariant of an, 13
binomial, 22
binomial set theoretic complete intersection, 47
codimension of an, 6
complete intersection, 51

degree of an, 13
dimension of an, 6
Gröbner basis of an, 9
graded, 12
height of a prime, 6
height of an, 6
homogeneous, 12
homogenization of an, 66
initial, 9
lattice, xi, 22
pure binomial, 22
pure binomial set theoretic complete intersection, 47
pure lattice, xi, 22
quotient, 6
standard graded, 12
toric, xiv, 18
vanishing of $\mathcal{Q}$, xiv
vanishing of $\mathcal{X}$, 2
vanishing of $\mathcal{X}^*$, xvii, 2
vanishing of $\overline{\mathcal{X}^*}$, xvii
variety of an, 86
index of regularity, 13
of $S[u]/I(\overline{\mathcal{X}^*})$, xviii
initial ideal, 9
Invariant factors of a matrix, 41
isolated vertex, 4
isomorphic graphs, 4

Krull dimension, 6

lattice, xi, 22
ω-homogeneous, 37
d-simplex, 41
homogeneous, 36
ideal, xi, 22
polytope, 3
leading
coefficient of a polynomial, 9
monomial of a polynomial, 9
term of a polynomial, 9
length
of a code, xvi
of a cycle, 5
of a module, 15
of a walk, 5
loop, 4

matrix
Invariant factors of a, 41
Smith normal form of a, 41
maximal condition, 7
maximum distance separable, xvi
minimal Gröbner basis, 11
minimum distance, xvi
module
annihilator of a, 15
codimension of a, 15
Cohen-Macaulay, 15, 16
composition series of a, 15
depth of a, 15
dimension of a, 15
length of a , 15
of finite length, 15
regular element of a, 14
regular sequence of a, 14
simple, 15
system of parameters of a, 16
zero divisor of a, 14
monomial
order, 8
subring, 17
support of a, 22
monomials
greatest common divisor of, 10
least common multiple of, 10
multigraph, 4

negative part of a vector, 22
Noetherian ring, 7
normalized volume, 41
numerical semigroup, 51

order
degree lexicographical, 8
degree reverse lexicographical, 8
elimination, 66
lexicographical, 8

- monomial, 8
- of a graph, 5
- reverse lexicographical, 8

parameterized
- affine code, xix, 61
- projective code, xxi, 82

partial character, xi, 22
- extension of a, 22
- trivial, xi

path, 5
polynomial, 7
- degree of a, 8
- degree with respect to t_i of a, 9
- Hilbert, 13
- homogenization of a, 66
- leading coefficient of a, 9
- leading monomial of a, 9
- leading term of a, 9
- multidegree of a, 8
- simple, 23
- total degree of a, 9

positive part of a vector, 22
primitive pure binomial, 18
product
- affine cartesian, 67
- projective cartesian, 82

projective
- algebraic toric set, xiv, 3
- cartesian code, 82
- cartesian product, xxii, 82
- closure, xvi, 2
- code, xviii, xxi, 60, 81
- code parameterized, xxi
- degenerate torus, xiv, xxi, 3
- evaluation code, xviii, xxi, 60, 81
- nested cartesian code, xxii, 83
- nested cartesian set, xxii, 83
- set, xxi
- space, 2
- torus, 3
- variety, 2

pure
- binomial, 22
- binomial ideal, 22
- binomial set theoretic complete intersection, 47
- lattice ideal, xi, 22

quotient ideal, 6

radical, 6
reduced Gröbner basis, 11
regular
- element, 14
- sequence, 14

relative volume, 3
ring
- ω-graded, 12
- Cohen-Macaulay, 15, 16
- graded, 11
- Noetherian, 7
- with the grading induced by ω, 12
- with the standard grading, 12

S-polynomial, 10
saturation, 6
semigroup, xiv
- numerical, xiv, 51

series Hilbert, 12
set
- affine, xvi
- affine algebraic toric, xix, 3
- affine cartesian product, xix
- affine degenerate torus, 3
- affine torus, 3
- associated to a graph, 67
- convex, 3
- of edges, 4
- of vertices, 4
- projective, xxi
- projective algebraic toric, xiv, 3
- projective cartesian product, xxii
- projective degenerate torus, xiv, xxi, 3
- projective nested cartesian, xxii, 83
- projective torus, 3

zero, 2, 65
simple
components, 23
polynomial, 23
Singleton bound, xvi
Smith normal form of a matrix, 41
space
affine, xvi, 2
projective, 2
square, 5
star, 5
subgraph, 5
induced, 5
spanning, 5
subgroup
torsion, 4
subring
monomial, 17
suites distinguées, xv
support
of a binomial, 22
of a monomial, 22
of a vector, 22
system of parameters, 16

ternary code, xvi
toric ideal, xiv, 18
torsion
free group, 4
subgroup, 4
tree, 5
triangle, 5

unital, 22

vanishing ideal
of $\mathcal{Q}$, xiv
of $\mathcal{X}$, 2
of $\mathcal{X}^*$, xvii, 2
of $\mathcal{Q}^*$, 61
of $\overline{\mathcal{X}^*}$, xvii
variety, 2, 86
projective, 2
vector
negative part of a, 22
positive part of a, 22
support of a, 22
vertex
degree of a , 4
isolated, 4
vertices
adjacent, 4
distance between, 6
set of, 4
volume normalized, 41

walk, 5
closed, 5

Zariski topology
on $\mathbb{A}^n$, 2
on $\mathbb{P}^n$, 2
zero
divisor, 14
set, 2, 65