ON THE VANISHING IDEAL OF AN ALGEBRAIC TORIC SET AND ITS PARAMETERIZED LINEAR CODES

ELISEO SARMIENTO, MARIA VAZ PINTO, AND RAFAEL H. VILLARREAL

Abstract. Let K be a finite field and let X be a subset of a projective space, over the field K, which is parameterized by monomials arising from the edges of a clutter. We show some estimates for the degree-complexity, with respect to the revlex order, of the vanishing ideal $I(X)$ of X. If the clutter is uniform, we classify the complete intersection property of $I(X)$ using linear algebra. We show an upper bound for the minimum distance of certain parameterized linear codes along with certain estimates for the algebraic invariants of $I(X)$.

1. Introduction

Let $K=\mathbb{F}_q$ be a finite field with q elements and let $y^{v_1},\ldots,y^{v_s}$ be a finite set of square-free monomials with $s\geq 2$. As usual if $v_i=(v_{i1},\ldots,v_{in})\in\mathbb{N}^n$, then we set

$$y^{v_i}=y_1^{v_{i1}}\cdots y_n^{v_{in}},\qquad i=1,\ldots,s,$$

where $y_1,\ldots,y_n$ are the indeterminates of a ring of polynomials with coefficients in K. We shall always assume that $\mathcal{A}=\{v_1,\ldots,v_s\}$ is the set of all characteristic vectors of the edges of a clutter (see Definitions 3.1 and 3.2). In particular this means that the entries of v_i are in $\{0,1\}$ for all i. Consider the following set parameterized by these monomials

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

where $K^*=K\setminus\{0\}$ and $\mathbb{P}^{s-1}$ is a projective space over the field K. Following [18] we call X an *algebraic toric set* parameterized by $y^{v_1},\ldots,y^{v_s}$. Let $S=K[t_1,\ldots,t_s]=\oplus_{d=0}^{\infty}S_d$ be a polynomial ring over the field K with the standard grading, let $[P_1],\ldots,[P_m]$ be the points of X, and let $f_0(t_1,\ldots,t_s)=t_1^d$. The *evaluation map*

$$\text{(1.1)}\qquad \mathrm{ev}_d\colon S_d=K[t_1,\ldots,t_s]_d\to K^{|X|},\qquad f\mapsto\left(\frac{f(P_1)}{f_0(P_1)},\ldots,\frac{f(P_m)}{f_0(P_m)}\right)$$

defines a linear map of K-vector spaces. The image of ev_d, denoted by $C_X(d)$, defines a *linear code*. Following [17] we call $C_X(d)$ a *parameterized linear code* of order d. As usual by a *linear code* we mean a linear subspace of $K^{|X|}$. The *dimension* and *length* of $C_X(d)$ are given by $\dim_K C_X(d)$ and $|X|$ respectively. The dimension and length are two of the *basic parameters* of a linear code. A third basic parameter is the *minimum distance* which is given by

$$\delta_d=\min\{\|v\|\colon 0\neq v\in C_X(d)\},$$

where $\|v\|$ is the norm of the Hamming distance, i.e., $\|v\|$ is the number of non-zero entries of v. The basic parameters of $C_X(d)$ are related by the Singleton bound for the minimum distance

$$\delta_d\leq|X|-\dim_K C_X(d)+1.$$

2000 *Mathematics Subject Classification.* Primary 13P25; Secondary 14G50, 14G15, 11T71, 94B27, 94B05.

The first author was partially supported by CONACyT. The second author is a member of the Center for Mathematical Analysis, Geometry and Dynamical Systems. The third author was partially supported by CONACyT grant 49251-F and SNI.

Parameterized linear codes are a nice family of *evaluation codes* (the notion of an evaluation code is introduced in Section 2). They were introduced and studied in [17]. Some other families of evaluation codes have been studied extensively [3, 4, 10, 22].

The *vanishing ideal* of X, denoted by $I(X)$, is the ideal of S generated by the homogeneous polynomials of S that vanish on X. The contents of this paper are as follows. In Section 2 we introduce the preliminaries and explain the connection between the invariants of the vanishing ideal of X and the parameters of $C_X(d)$.

The ideal $I(X)$ is called a *complete intersection* if it can be generated by $s-1$ homogeneous polynomials of S. In [19] it is shown that $I(X)$ is a complete intersection if and only if X is a projective torus in $\mathbb{P}^{s-1}$ (see Definition 2.4). If the clutter has all its edges of the same cardinality, in Section 3 we classify the complete intersection property of $I(X)$ using linear algebra (see Theorem 3.9).

Let $\succ$ be the reverse lexicographical order on the monomials of S. Recall that the ideal $I(X)$ has a unique reduced Gröbner basis with respect to $\succ$. The *degree-complexity* of $I(X)$, with respect to $\succ$, is the maximum degree in the reduced Gröbner basis of $I(X)$. In Section 4 we study the structure of the reduced Gröbner basis of $I(X)$ and show an upper bound for the degree-complexity of $I(X)$ (see Theorem 4.1). This means that the algebraic methods of [17] to compute the invariants of $I(X)$ will probably work better using the revlex order.

In Section 5 we show upper bounds for the minimum distance of $C_X(d)$ for a certain family of algebraic toric sets X arising from normal edge ideals (see Theorem 5.1(b)). For this family we also show estimates for the algebraic invariants of $I(X)$. The bounds on the minimum distance indicate that the codes $C_X(d)$ that emerge from unicyclic connected graphs are especially attractive from the point of view of their error-correcting capacity and so are the codes $C_X(d)$ with $d = 1$ (see Remark 5.3). We give examples, within our family, of parameterized codes having a large minimum distance relative to $|X|$ (see Example 5.4). Such examples of linear codes with large minimum distance are essential, as they show that our construction is attractive in the context of coding theory. The codes $C_X(d)$ are only interesting when d lies within a certain range because $\delta_d = 1$ for $d \gg 0$. This range is determined by $\operatorname{reg}(S/I(X))$, the index of regularity of $S/I(X)$ (see Proposition 2.3). This is one of the motivations to study the index of regularity. Another motivation comes from commutative algebra because, in our situation, $\operatorname{reg}(S/I(X))$ is equal to the Castelnuovo-Mumford regularity which is an algebraic invariant of central importance in the area [5]. The problem of finding a good decoding algorithm for our family of parameterized codes is not considered here. The reader is referred to [2, Chapter 9], [15, 27] and the references there for some available decoding algorithms for some families of linear codes.

For all unexplained terminology and additional information we refer to [6] (for the theory of binomial ideals), [1, 23] (for the theory of Gröbner bases and Hilbert functions), and [16, 24, 26] (for the theory of error-correcting codes and algebraic geometric codes).

2. Preliminaries

We continue to use the notation and definitions used in the introduction. In this section we introduce the basic algebraic invariants of $S/I(X)$ and recall their connection with the basic parameters of parameterized linear codes. Then, we present a result on complete intersections that will be needed later.

Recall that the *projective space* of dimension $s-1$ over K, denoted by $\mathbb{P}^{s-1}$, is the quotient space

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

where two points α, β in $K^s \setminus \{0\}$ are equivalent if $\alpha = \lambda\beta$ for some $\lambda \in K$. We denote the equivalence class of α by $[\alpha]$. Let $X \subset \mathbb{P}^{s-1}$ be an algebraic toric set parameterized by $y^{v_1}, \ldots, y^{v_s}$ and let $C_X(d)$ be a parameterized code of order d. The kernel of the evaluation map ev_d, defined in Eq. (1.1), is precisely $I(X)_d$ the degree d piece of $I(X)$. Therefore there is an isomorphism of K-vector spaces

$$S_d/I(X)_d \simeq C_X(d). \tag{2.1}$$

Two of the basic parameters of $C_X(d)$ can be expressed using Hilbert functions of standard graded algebras [17, 23], as we explain below. Recall that the *Hilbert function* of $S/I(X)$ is given by

$$H_X(d) := \dim_K\,(S/I(X))_d = \dim_K\; S_d/I(X)_d.$$

The unique polynomial $h_X(t) = \sum_{i=0}^{k-1} c_i t^i \in \mathbb{Z}[t]$ of degree $k-1 = \dim(S/I(X))-1$ such that $h_X(d) = H_X(d)$ for $d \gg 0$ is called the *Hilbert polynomial* of $S/I(X)$. The integer $c_{k-1}(k-1)!$, denoted by $\deg(S/I(X))$, is called the *degree* or *multiplicity* of $S/I(X)$. In our situation $h_X(t)$ is a non-zero constant because $S/I(X)$ has dimension 1. Furthermore:

Proposition 2.1. ([14, Lecture 13], [8]) $h_X(d) = |X|$ *for* $d \geq |X|-1$.

This result means that $|X|$ is equal to the *degree* of $S/I(X)$. From Eq. (2.1), we get the equality $H_X(d) = \dim_K C_X(d)$. Thus, we have:

Proposition 2.2. [8, 12] $H_X(d)$ *and* $\deg(S/I(X))$ *are equal to the dimension and the length of* $C_X(d)$ *respectively.*

There are algebraic methods, based on elimination theory and Gröbner bases, to compute the dimension and the length of $C_X(d)$ [17].

The *index of regularity* of $S/I(X)$, denoted by $\mathrm{reg}(S/I(X))$, is the least integer $p \geq 0$ such that $h_X(d) = H_X(d)$ for $d \geq p$. The degree and the index of regularity can be read off the Hilbert series as we now explain. The Hilbert series of $S/I(X)$ can be written as

$$F_X(t) := \sum_{d=0}^{\infty} H_X(d)t^d = \frac{h_0 + h_1 t + \cdots + h_r t^r}{1-t},$$

where $h_0, \ldots, h_r$ are positive integers. Indeed $h_i = \dim_K(S/(I(X), t_s))_i$ for $0 \leq i \leq r$ and $\dim_K(S/(I(X), t_s))_i = 0$ for $i > r$. This follows from the fact that $I(X)$ is a Cohen-Macaulay lattice ideal [17] and by observing that $\{t_s\}$ is a regular system of parameters for $S/I(X)$ (see [23]). The number r is equal to the index of regularity of $S/I(X)$ and the degree of $S/I(X)$ is equal to $h_0 + \cdots + h_r$ (see [23] or [29, Corollary 4.1.12]).

A good parameterized code should have large $|X|$ and with $\dim_K C_X(d)/|X|$ and $\delta_d/|X|$ as large as possible. The following result gives an indication of where to look for non-trivial parameterized codes. Only the codes $C_X(d)$ with $1 \leq d < \mathrm{reg}(S/I(X))$ have the potential to be good linear codes.

Proposition 2.3. $\delta_d = 1$ *for* $d \geq \mathrm{reg}(S/I(X))$.

Proof. Since $H_X(d)$ is equal to the dimension of $C_X(d)$ and $H_X(d) = |X|$ for $d \geq \mathrm{reg}(S/I(X))$, by a direct application of the Singleton bound we get that $\delta_d = 1$ for $d \geq \mathrm{reg}(S/I(X))$. □

The definition of $C_X(d)$ can be extended to any finite subset $X \subset \mathbb{P}^{s-1}$ of a projective space over a field K [10, 12]. In this generality—the resulting linear code—$C_X(d)$ is called an *evaluation code* associated to X (see for instance [10]). It is also called a *projective Reed-Muller code* over the set X (see [4, 12]). In this paper we will only deal with parameterized codes over finite fields.

The parameters of evaluation codes associated to X have been computed in a number of cases. If $X = \mathbb{P}^{s-1}$, the parameters of $C_X(d)$ are described in [22, Theorem 1]. If X is the image of the affine space $\mathbb{A}^{s-1}$ under the map $x \mapsto [(1, x)]$, the parameters of $C_X(d)$ are described in [3, Theorem 2.6.2]. If X is a projective torus, the parameters of $C_X(d)$ are described in [4] and [19]. In this paper we give upper bounds for the parameters of certain parameterized codes.

As seen above, parameterized codes are a special type of evaluation codes. What makes a parameterized code interesting is the fact that the vanishing ideal of X is a binomial ideal [17], which allows the computation of the dimension and length using the computer algebra system *Macaulay*2 [13]. The index of regularity of $S/I(X)$ can also be computed using *Macaulay*2, which is useful to find genuine parameterized codes (see Proposition 2.3).

Definition 2.4. The set $\mathbb{T} = \{[(x_1, \ldots, x_s)] \in \mathbb{P}^{s-1} \,|\, x_i \in K^* \text{ for all } i\}$ is called a *projective torus* in $\mathbb{P}^{s-1}$.

An algebraic toric set is a multiplicative group under componentwise multiplication. Thus, a projective torus is a multiplicative group. For future reference we recall the following result on complete intersections.

Proposition 2.5. [11, Theorem 1, Lemma 1] *If* $\mathbb{T}$ *is a projective torus in* $\mathbb{P}^{s-1}$*, then*

(a) $I(\mathbb{T}) = (\{t_i^{q-1} - t_1^{q-1}\}_{i=2}^{s})$.
(b) $F_{\mathbb{T}}(t) = (1 - t^{q-1})^{s-1}/(1 - t)^s$.
(c) $\operatorname{reg}(S/I(\mathbb{T})) = (s - 1)(q - 2)$ *and* $\deg(S/I(\mathbb{T})) = (q - 1)^{s-1}$.

3. The complete intersection property of $I(X)$

We continue to use the notation and definitions used in the introduction and in the preliminaries. The main result of this section is a structure theorem for the complete intersection property of $I(X)$.

Definition 3.1. A *clutter* $\mathcal{C}$ is a family E of subsets of a finite ground set $Y = \{y_1, \ldots, y_n\}$ such that if $f_1, f_2 \in E$, then $f_1 \not\subset f_2$. The ground set Y is called the *vertex set* of $\mathcal{C}$ and E is called the *edge set* of $\mathcal{C}$, they are denoted by $V_\mathcal{C}$ and $E_\mathcal{C}$ respectively.

Clutters are special hypergraphs and are sometimes called *Sperner families* in the literature. One important example of a clutter is a graph with the vertices and edges defined in the usual way for graphs.

Definition 3.2. Let $\mathcal{C}$ be a clutter with vertex set $V_\mathcal{C} = \{y_1, \ldots, y_n\}$ and let f be an edge of $\mathcal{C}$. The *characteristic vector* of f is the vector $v = \sum_{y_i \in f} e_i$, where e_i is the *ith* unit vector in $\mathbb{R}^n$.

Throughout this paper we assume that $\mathcal{A} := \{v_1, \ldots, v_s\}$ is the set of all characteristic vectors of the edges of a clutter $\mathcal{C}$.

Definition 3.3. If $a \in \mathbb{R}^s$, its *support* is defined as $\operatorname{supp}(a) = \{i \,|\, a_i \neq 0\}$. Note that $a = a^+ - a^-$, where a^+ and a^- are two non negative vectors with disjoint support called the *positive* and *negative* part of a respectively.

Lemma 3.4. *Let $\mathcal{C}$ be a clutter and let $f \neq 0$ be a homogeneous binomial of $I(X)$ of the form $t_i^b - t^c$ with $b \in \mathbb{N}$, $c \in \mathbb{N}^s$ and $i \notin \operatorname{supp}(c)$. Then*

(a) $\deg(f) \geq q-1$.

(b) *If $\deg(f) = q-1$, then $f = t_i^{q-1} - t_j^{q-1}$ for some $j \neq i$.*

Proof. For simplicity of notation assume that $f = t_1^b - t_2^{c_2} \cdots t_r^{c_r}$, where $c_j \geq 1$ for all j and $b = c_2 + \cdots + c_r$. Then

$$(x_1^{v_{11}} \cdots x_n^{v_{1n}})^b = (x_1^{v_{21}} \cdots x_n^{v_{2n}})^{c_2} \cdots (x_1^{v_{r1}} \cdots x_n^{v_{rn}})^{c_r} \quad \forall\, (x_1, \ldots, x_n) \in (K^*)^n, \tag{3.1}$$

where $v_i = (v_{i1}, \ldots, v_{in})$. Let β be a generator of the cyclic group $(K^*, \cdot)$.

(a) We proceed by contradiction. Assume that $b < q-1$. First we claim that if $v_{1k} = 1$ for some $1 \leq k \leq n$, then $v_{jk} = 1$ for $j = 2, \ldots, r$. To prove the claim assume that $v_{1k} = 1$ and $v_{jk} = 0$ for some $j \geq 2$. Then, making $x_i = 1$ for $i \neq k$ in Eq. (3.1), we get $(x_k^{v_{1k}})^b = x_k^b = x_k^m$, where $m = v_{2k}c_2 + \cdots + v_{rk}c_r < b$. Then $x_k^{b-m} = 1$ for $x_k \in K^*$. In particular $\beta^{b-m} = 1$. Hence $b - m$ is a multiple of $q-1$ and consequently $b \geq q-1$, a contradiction. This completes the proof of the claim. Therefore $\operatorname{supp}(v_1) \subset \operatorname{supp}(v_j)$ for $j = 2, \ldots, r$. Since $\mathcal{C}$ is a clutter we get that $v_1 = v_j$ for $j = 2, \ldots, r$, a contradiction because $v_1, \ldots, v_r$ are distinct. Hence $b \geq q-1$.

(b) It suffices to show that $r = 2$. Assume $r \geq 3$. We claim that if $v_{2k} = 1$ for some $1 \leq k \leq n$, then $v_{jk} = 1$ for $j \geq 3$. Otherwise, if $v_{2k} = 1$ and $v_{jk} = 0$ for some $j \geq 3$, making $x_i = 1$ for $i \neq k$ and $b = q-1$ in Eq. (3.1) we get $1 = x_k^m$ for any $x_k \in K^*$, for some $0 < m < q-1$. A contradiction because $\beta^m \neq 1$. This proves the claim. Therefore $\operatorname{supp}(v_2) \subset \operatorname{supp}(v_j)$ for $j \geq 3$. As in part (a) we get $v_2 = v_j$ for $j \geq 3$, a contradiction. Hence $r = 2$. □

The complete intersection property of $I(X)$ was first studied in [19]. We complement the following result by showing a characterization of this property—valid for uniform clutters—using linear algebra (see Theorem 3.9).

Theorem 3.5. [19] *Let $\mathcal{C}$ be a clutter with s edges and let $\mathbb{T}$ be a projective torus in $\mathbb{P}^{s-1}$. The following are equivalent:*

(c_1) *$I(X)$ is a complete intersection.*

(c_2) $I(X) = (t_1^{q-1} - t_s^{q-1}, \ldots, t_{s-1}^{q-1} - t_s^{q-1})$.

(c_3) $X = \mathbb{T} \subset \mathbb{P}^{s-1}$.

For use below recall that the *toric ideal* associated to $\mathcal{A} = \{v_1, \ldots, v_s\}$, denoted by $I_{\mathcal{A}}$, is the prime ideal of $S = K[t_1, \ldots, t_s]$ given by (see [25]):

$$I_{\mathcal{A}} = \left(t^a - t^b \middle|\, a = (a_i), b = (b_i) \in \mathbb{N}^s, \textstyle\sum_i a_i v_i = \sum_i b_i v_i\right) \subset S. \tag{3.2}$$

A clutter is called *uniform* if all its edges have the same number of elements.

Proposition 3.6. *Let $\mathcal{C}$ be a uniform clutter. If $I(X)$ is a complete intersection and $q \geq 3$, then $v_1, \ldots, v_s$ are linearly independent.*

Proof. To begin with we claim that if $f = t^{a^+} - t^{a^-}$ is any non-zero homogeneous binomial in the lattice ideal $I(X)$, then

$$a = a^+ - a^- \;\equiv\; 0 \bmod (q-1),$$

that is, any entry of a is a multiple of $q-1$. By Theorem 3.5 the degree of f is at least $q-1$. To show the claim we proceed by induction on $\deg(f)$. If $\deg(f) = q-1$, then by Theorem 3.5 and Lemma 3.4(b) it is seen that $f = t_i^{q-1} - t_j^{q-1}$ for some i, j, i.e., $a = (q-1)e_i - (q-1)e_j$. Assume that $\deg(f) > q-1$. By Theorem 3.5 we obtain that t^{a^+} and t^{a^-} are divisible by some t_i^{q-1} and t_j^{q-1} respectively. Then, $a_i^+ \geq q-1$ and $a_j^- \geq q-1$ for some $i \in \text{supp}(a^+)$ and $j \in \text{supp}(a^-)$. Therefore using that $f \in I(X)$ and the fact that $(K^*, \cdot)$ is a cyclic group of order $q-1$, it follows readily that the binomial

$$f' = \frac{t^{a^+}}{t_i^{q-1}} - \frac{t^{a^-}}{t_j^{q-1}}$$

is homogeneous, of degree $\deg(f) - (q-1)$, and belongs to $I(X)$. Hence by induction hypothesis the vector $(a^+ - (q-1)e_i) - (a^- - (q-1)e_j)$ is a multiple of $q-1$, and so is $a = a^+ - a^-$. This completes de proof of the claim.

To show that $v_1, \ldots, v_s$ are linearly independent we proceed by contradiction. Assume that $v_1, \ldots, v_s$ are linearly dependent. As $\mathcal{C}$ is uniform, there is a non-zero homogeneous binomial $f = t^{a^+} - t^{a^-}$ of least degree in the toric ideal $I_\mathcal{A}$. This means that the degree of f is equal to the initial degree of $I_\mathcal{A}$ [29, p. 110]. Since $I_\mathcal{A} \subset I(X)$ we obtain that $a = a^+ - a^-$ is a multiple of $q-1$. Then, we can write $a^+ = (q-1)b^+$, $a^- = (q-1)b^-$ for some b^+, b^- in $\mathbb{N}^s$. We set $u = t^{b^+}$, $v = t^{b^-}$, $g = u - v$, $h = u^{q-2} + u^{q-3}v + \cdots + v^{q-2}$. From the equality $f = gh$ we obtain that $g \in I_\mathcal{A}$ or $h \in I_\mathcal{A}$ because $I_\mathcal{A}$ is a prime ideal and $q \geq 3$, a contradiction to the choice of f because g and h have degree less than that of f. □

Definition 3.7. For an ideal $I \subset S$ and a polynomial $h \in S$ the *saturation* of I with respect to h is the ideal

$$(I\colon h^\infty) := \{f \in S \mid fh^m \in I \text{ for some } m \geq 1\}.$$

We will only deal with the case where $h = t_1 \cdots t_s$.

We call $\mathcal{A}$ *homogeneous* if $\mathcal{A}$ lies on an affine hyperplane not containing the origin. Notice that if $\mathcal{C}$ is uniform, then $\mathcal{A}$ is homogeneous. Given $\Gamma \subset \mathbb{Z}^n$, the subgroup of $\mathbb{Z}^n$ generated by Γ will be denoted by $\mathbb{Z}\Gamma$.

Theorem 3.8. [17, Theorem 2.6] *Let $K = \mathbb{F}_q$ be a finite field, let $\mathcal{A} = \{v_1, \ldots, v_s\} \subset \mathbb{Z}^n$, and let $\phi\colon \mathbb{Z}^n/L \to \mathbb{Z}^n/L$ be the multiplication map $\phi(\overline{a}) = (q-1)\overline{a}$, where $L = \mathbb{Z}\{v_i - v_1\}_{i=2}^s$. If $\mathcal{A}$ is homogeneous, then*

$$((I_\mathcal{A} + (t_2^{q-1} - t_1^{q-1}, \ldots, t_s^{q-1} - t_1^{q-1}))\colon (t_1 \cdots t_s)^\infty) \subset I(X) \tag{3.3}$$

with equality if and only if the map ϕ is injective.

We come to the main result of this section, a structure theorem for complete intersections via linear algebra.

Theorem 3.9. *Let $\phi\colon \mathbb{Z}^n/L \to \mathbb{Z}^n/L$ be the multiplication map $\phi(\overline{a}) = (q-1)\overline{a}$, where L is the subgroup generated by $\{v_i - v_1\}_{i=2}^s$. If $\mathcal{C}$ is a uniform clutter and $q \geq 3$, then $I(X)$ is a complete intersection if and only if $v_1, \ldots, v_s$ are linearly independent and the map ϕ is injective.*

Proof. $\Rightarrow$) By Proposition 3.6 the vectors $v_1, \ldots, v_s$ are linearly independent. Then $I_\mathcal{A} = (0)$ and by Theorem 3.5 we get the equality $I(X) = (\{t_1^{q-1} - t_i^{q-1}\}_{i=2}^s)$. Hence, we have equality in Eq. (3.3). Therefore using Theorem 3.8 we conclude that ϕ is injective.

$\Leftarrow$) As the map ϕ is injective and $\mathcal{C}$ is uniform, using Theorem 3.8, we get the equality

$$((I_\mathcal{A} + (t_2^{q-1} - t_1^{q-1}, \ldots, t_s^{q-1} - t_1^{q-1}))\colon (t_1 \cdots t_s)^\infty) = I(X).$$

Since $\mathcal{A}$ is linearly independent one has that $I_\mathcal{A} = (0)$. Hence, the equality above becomes $(\{t_1^{q-1} - t_i^{q-1}\}_{i=2}^s) = I(X)$, i.e., $I(X)$ is a complete intersection. □

A graph with only one cycle is called *unicyclic.*

Corollary 3.10. *Let $\mathcal{C}$ be a unicyclic connected graph with n vertices. If the only cycle of $\mathcal{C}$ is odd, then $X = \mathbb{T}$ is a projective torus in $\mathbb{P}^{n-1}$.*

Proof. Assume that $\mathcal{C}$ is an odd cycle of length n. Let $y_1, \ldots, y_n$ be the vertices of $\mathcal{C}$. The characteristic vectors of the edges of $\mathcal{C}$ are

$$v_1 = e_1 + e_2,\, v_2 = e_2 + e_3, \ldots, v_{n-1} = e_{n-1} + e_n,\, v_n = e_n + e_1,$$

where e_i is the *ith* unit vector in $\mathbb{N}^n$. The vectors $v_1, \ldots, v_n$ are linearly independent because n is odd. It is not hard to see that the quotient group $\mathbb{Z}^n/\mathbb{Z}\{v_i - v_1\}_{i=2}^n$ is torsion-free. Hence, by Theorem 3.9, $I(X)$ is a complete intersection. Then, $X = \mathbb{T}$ is a projective torus in $\mathbb{P}^{n-1}$ by Theorem 3.5. If $\mathcal{C}$ is not an odd cycle, then it has a vertex of degree 1 and the proof follows by induction because removing this vertex results in a graph that is connected and has a unique odd cycle. □

The next result shows that the index of regularity of complete intersections associated to clutters provides an upper bound for the index of regularity of $S/I(X)$.

Proposition 3.11. [19] $\mathrm{reg}(S/I(X)) \leq (q-2)(s-1)$, *with equality if $I(X)$ is a complete intersection associated to a clutter with s edges.*

Remark 3.12. In Theorem 5.1(c) we provide another upper bound for the index of regularity of $S/I(X)$ valid for a certain family of algebraic toric sets.

4. The degree-complexity of $I(X)$

We continue to use the notation and definitions used in the introduction. The main result of this section is an upper bound for the degree-complexity of $I(X)$.

In what follows we shall assume that $\succ$ is the *reverse lexicographical order* (*revlex order* for short) on the monomials of S. This order is given by $t^b \succ t^a$ if and only if the last non-zero entry of $b - a$ is negative. As usual, if g is a polynomial of S, we denote the leading term of g by $\mathrm{in}(g)$ and the leading coefficient of g by $\mathrm{lc}(g)$.

According to [1, Proposition 6, p. 91] the ideal $I(X)$ has a unique reduced Gröbner basis. We refer to [1] for the theory of Gröbner bases. The *degree-complexity* of $I(X)$, with respect to $\succ$, is the maximum degree of the polynomials in the reduced Gröbner basis of $I(X)$. Next we study the reduced Gröbner basis and the degree-complexity of $I(X)$.

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

Theorem 4.1. *Let $\mathcal{C}$ be a clutter and let $\succ$ be the revlex order on the monomials of S. If $\mathcal{G}$ is the reduced Gröbner basis of the ideal $I(X)$, then $t_i^{q-1} - t_s^{q-1} \in \mathcal{G}$ for $i = 1, \ldots, s-1$ and $\deg_{t_i}(g) \leq q-1$ for $g \in \mathcal{G}$ and $1 \leq i \leq s$.*

Proof. The reduced Gröbner basis of $I(X)$ consists of homogeneous binomials [17]. As $I(X)$ is a lattice ideal [17], it is seen that each binomial $t^a - t^b \in \mathcal{G}$ satisfies that $\mathrm{supp}(a) \cap \mathrm{supp}(b) = \emptyset$, this follows using that each variable t_i is not a zero-divisor of $S/I(X)$. Since $t_i^{q-1} - t_s^{q-1}$ is in $I(X)$ for $i = 1, \ldots, s-1$, there is $g_i \in \mathcal{G}$ such that $g_i = t_i^{b_i} - t^{c_i}$, $b_i \leq q-1$, $c_i \in \mathbb{N}^s$, $i \notin \mathrm{supp}(c_i)$, and $\mathrm{in}(g_i) = t_i^{b_i}$. Then, by Lemma 3.4, the binomial g_i has the form $g_i = t_i^{q-1} - t_{j_i}^{q-1}$ for some $i < j_i$. As $\mathcal{G}$ is a reduced Gröbner basis we get that $g_i = t_i^{q-1} - t_s^{q-1}$ for $i = 1, \ldots, s-1$. Let $g \in \mathcal{G} \setminus \{g_1, \ldots, g_{s-1}\}$. Using that $\mathcal{G}$ is reduced we get that $\deg_{t_i}(g) \leq q-2$ for $i = 1, \ldots, s-1$. To complete the proof we need only show $\deg_{t_s}(g) \leq q-1$. Assume that $a_s = \deg_{t_s}(g) > q-1$. After permuting $t_1, \ldots, t_{s-1}$ we may assume that $\mathrm{in}(g) = t_1^{a_1} \cdots t_r^{a_r}$ and $g = t_1^{a_1} \cdots t_r^{a_r} - t_{r+1}^{a_{r+1}} \cdots t_s^{a_s}$, where $r < s$. Consider the polynomial

$$\begin{aligned} h &= t_2^{a_2} \cdots t_r^{a_r} g_1 - t_1^{q-1-a_1} g \\ &= t_s^{q-1}\left(-t_2^{a_2} \cdots t_r^{a_r} + t_1^{q-1-a_1} t_{r+1}^{a_{r+1}} \cdots t_{s-1}^{a_{s-1}} t_s^{a_s-(q-1)}\right) = t_s^{q-1} h_1. \end{aligned}$$

Since $h \in I(X)$ and using that $I(X)$ is a lattice ideal, we get that the binomial

$$h_1 = -t_2^{a_2} \cdots t_r^{a_r} + t_1^{q-1-a_1} t_{r+1}^{a_{r+1}} \cdots t_{s-1}^{a_{s-1}} t_s^{a_s-(q-1)}$$

belongs to $I(X)$. As $\mathrm{in}(h_1) = t_2^{a_2} \cdots t_r^{a_r}$, we obtain that $\mathrm{in}(g) \in (\mathrm{in}(\mathcal{G} \setminus \{g\})$, a contradiction. Thus $\deg_{t_s}(g) \leq q-1$. $\Box$

The next result is interesting because it shows that the Hilbert functions of $S/I(X)$ and $S/I_{\mathcal{A}}$ are equal up to degree $q-2$.

Proposition 4.2. *Let $\mathcal{C}$ be a clutter. If $f = t^{a^+} - t^{a^-}$ is a non-zero homogeneous binomial of $I(X)$ and $\deg(f) \leq q-2$, then $f \in I_{\mathcal{A}}$.*

Proof. We may assume that $a^+ = (a_1, \ldots, a_r, 0, \ldots, 0)$ and $a^- = (0, \ldots, 0, a_{r+1}, \ldots, a_m, 0, \ldots, 0)$ and $a_i \geq 1$ for $i = 1, \ldots, m$. Then

$$(x_1^{v_{11}} \cdots x_n^{v_{1n}})^{a_1} \cdots (x_1^{v_{r1}} \cdots x_n^{v_{rn}})^{a_r} = (x_1^{v_{r+1,1}} \cdots x_n^{v_{r+1,n}})^{a_{r+1}} \cdots (x_1^{v_{m,1}} \cdots x_n^{v_{m,n}})^{a_m} \tag{4.1}$$

for all $(x_1, \ldots, x_n) \in (K^*)^n$, where $v_i = (v_{i1}, \ldots, v_{in}) = (v_{i,1}, \ldots, v_{i,n})$. To show that $f \in I_{\mathcal{A}}$ we need only show that $Aa^+ = Aa^-$, where A is the incidence matrix of $\mathcal{C}$, i.e., A is the matrix with column vectors $v_1, \ldots, v_s$. Equivalently we need only show the equality

$$v_{1,k}a_1 + \cdots + v_{r,k}a_r = v_{r+1,k}a_{r+1} + \cdots + v_{m,k}a_m \tag{4.2}$$

for $1 \leq k \leq n$. If both sides of Eq. (4.2) are zero there is nothing to show. We proceed by contradiction assuming:

$$v_{1,k}a_1 + \cdots + v_{r,k}a_r > v_{r+1,k}a_{r+1} + \cdots + v_{m,k}a_m \geq 0. \tag{4.3}$$

Making $x_i = 1$ for $i \neq k$ in Eq. (4.1), we get

$$x_k^{v_{1,k}a_1 + \cdots + v_{r,k}a_r} = x_k^{v_{r+1,k}a_{r+1} + \cdots + v_{m,k}a_m}$$

for any $x_k \in K^*$. In particular making $x_k = \beta$, where β is a generator of the cyclic group $(K^*, \cdot)$, we get that

$$(v_{1,k}a_1 + \cdots + v_{r,k}a_r) - (v_{r+1,k}a_{r+1} + \cdots + v_{m,k}a_m) \equiv \ 0 \bmod (q-1). \tag{4.4}$$

Consequently $v_{1,k}a_1 + \cdots + v_{r,k}a_r \geq q-1$, a contradiction because

$$q-2 \geq \deg(f) = a_1 + \cdots + a_r \geq v_{1,k}a_1 + \cdots + v_{r,k}a_r.$$

Hence equality in Eq. (4.2) holds for $1 \leq k \leq n$ and the proof is complete. $\Box$

Proposition 4.3. *Let A be the matrix with column vectors $v_1, \ldots, v_s$. Then*

$$I(X) = (\{t^{a^+} - t^{a^-} \,|\, Aa^+ \equiv Aa^- \bmod (q-1) \text{ and } |a^+| = |a^-|\}).$$

Proof. The inclusion "$\subset$" follows from Eq. (4.4) and from the fact that $I(X)$ is a lattice ideal [17]. To show the inclusion "$\supset$" take $f = t^{a^+} - t^{a^-}$ such that $Aa^+ \equiv Aa^- \bmod (q-1)$ and $|a^+| = |a^-|$. From the first condition it is seen that f vanishes on X and from the second condition f is homogeneous in the standard grading of S. Thus $f \in I(X)$. $\Box$

5. Upper bounds for the minimum distance

We continue to use the notation and definitions used in the introduction and in the preliminaries. Let $\mathcal{C}$ be a clutter with vertex set $V_{\mathcal{C}} = \{y_1, \ldots, y_n\}$. Throughout this section we assume that $\mathcal{A} = \{v_1, \ldots, v_s\}$ is the set of all characteristic vectors of the edges of a uniform clutter $\mathcal{C}$.

The set $(K^*)^n$ is called an *affine algebraic torus* of dimension n and is denoted by $\mathbb{T}^*$. The torus $\mathbb{T}^*$ is a multiplicative group under the product operation $(\alpha_i)(\alpha_i') = (\alpha_i\alpha_i')$, where (α_i) really means $(\alpha_1, \ldots, \alpha_n)$. Clearly, the algebraic toric set:

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

is also a multiplicative group with the product operation.

Let I be the ideal of $R = K[y_1, \ldots, y_n]$ generated by $y^{v_1}, \ldots, y^{v_s}$. The ideal I is called the *edge ideal* of $\mathcal{C}$ and the matrix A whose columns are $v_1, \ldots, v_s$ is called the *incidence matrix* of $\mathcal{C}$. Recall that the *integral closure* of I^i, denoted by $\overline{I^i}$, is the ideal of R given by

$$\overline{I^i} = (\{y^a \in R \,|\, \exists\, p \in \mathbb{N} \setminus \{0\}; (y^a)^p \in I^{pi}\}), \tag{5.1}$$

see for instance [29, Proposition 7.3.3]. The ideal I is called *normal* if $I^i = \overline{I^i}$ for $i \geq 1$. There are many interesting examples of normal ideals [25, 29]. For instance if $\mathcal{C}$ is the clutter of all subsets of $Y = \{y_1, \ldots, y_n\}$ of a fixed size $k \geq 1$, then I is normal. If $\mathcal{C}$ is the clutter of bases of a matroid, then I is also normal. There is a combinatorial description of the normality of ideals generated by square-free monomials of degree 2, i.e., of ideals such that $\mathcal{C}$ is a graph (see [20, 21]). In particular if $\mathcal{C}$ is a complete or bipartite graph, then I is normal. The edge ideal I is also normal if $\mathcal{C}$ is any odd cycle or any unicyclic graph.

Let $\mathcal{B} \subset \mathbb{Z}^{n+1}$. The *polyhedral cone* generated by $\mathcal{B}$ is denoted by $\mathbb{R}_+\mathcal{B}$. A polyhedral cone containing no lines is called *pointed*. The set $\mathcal{B}$ is called a *Hilbert basis* if $\mathbb{N}\mathcal{B} = \mathbb{R}_+\mathcal{B} \cap \mathbb{Z}^{n+1}$, where $\mathbb{N}\mathcal{B}$ is the semigroup generated by $\mathcal{B}$.

We come to the main result of this section, an upper bound for the minimum distance of $C_X(d)$ valid for certain normal edge ideals of uniform clutters.

Theorem 5.1. *Let $\mathcal{C}$ be a uniform clutter whose incidence matrix has rank n and let $I \subset R$ be its edge ideal. If I is normal and $\mathbb{T}$ is a projective torus in $\mathbb{P}^{n-1}$, then:*

(a) *The degree of $S/I(X)$ is equal to $|X| = (q-1)^{n-1}$.*
(b) $\delta_d \leq \delta_d'$, *where δ_d' is the minimum distance of the linear code $C_{\mathbb{T}}(d)$.*
(c) $\operatorname{reg}(S/I(X)) \leq \operatorname{reg}(S'/I(\mathbb{T})) = (q-2)(n-1)$, *where $S' = K[t_1, \ldots, t_n]$.*

Proof. (a) The ideal I is normal. Then by [7, Theorem 3.15] the set $\mathcal{B} = \{(v_i, 1)\}_{i=1}^s$ is a Hilbert basis. Therefore, using [17, Theorem 3.5], we obtain that $(q-1)^{n-1}$ divides $|X|$. On the other hand there is an epimorphism of multiplicative groups

$$\theta\colon \mathbb{T}^* \to X\,; \qquad (x_1, \ldots, x_n) \stackrel{\theta}{\longmapsto} [(x^{v_1}, \ldots, x^{v_s})],$$

where $\mathbb{T}^* = (K^*)^n$ is an affine algebraic torus. The kernel of θ contains the diagonal subgroup

$$\mathcal{D}^* = \{(\lambda, \ldots, \lambda) \,|\, \lambda \in K^*\}.$$

Thus $|X|$ divides $(q-1)^{n-1}$. Putting altogether, we get $|X| = (q-1)^{n-1}$.

(b) The set $\mathcal{B} = \{(v_i, 1)\}_{i=1}^s$ is a Hilbert basis (see the proof of part (a)). Hence using a result of [9], after permutation of the $(v_i, 1)$'s, we may assume that $\mathcal{B}' = \{(v_1, 1), \ldots, (v_n, 1)\}$ is a Hilbert basis and a linearly independent set. Then, it is seen that the group $\mathbb{Z}^{n+1}/\mathbb{Z}\mathcal{B}'$ is torsion-free. We set $L'=\mathbb{Z}\{v_i-v_1\}_{i=2}^n$. It is not hard to see that there is an isomorphism of groups

$$\tau\colon T(\mathbb{Z}^n/L')\rightarrow T(\mathbb{Z}^{n+1}/\mathbb{Z}\mathcal{B}')$$

given by $\tau(\overline{a})=\overline{(a,0)}$, where $T(M)$ denotes the torsion subgroup of an abelian group M, i.e., $T(M)$, is the set of all m in M such that $pm=0$ for some $0\neq p\in\mathbb{Z}$. From this isomorphism we conclude that $T(\mathbb{Z}^n/L')=0$, i.e., $\mathbb{Z}^n/L'$ is also torsion-free.

Consider the algebraic toric set parameterized by $y^{v_1},\ldots,y^{v_n}$:

$$X_1=\{[(x^{v_1},\ldots,x^{v_n})]\,|\,x_i\in K^* \text{ for all } i\}\subset\mathbb{P}^{n-1}.$$

We claim that $I(X_1)=(\{t_i^{q-1}-t_n^{q-1}\}_{i=1}^{n-1})$. We set $\mathcal{A}'=\{v_1,\ldots,v_n\}$. Notice that the set $\mathcal{A}'$ is also linearly independent. Since $I_{\mathcal{A}'}=(0)$ and $\mathbb{Z}^n/L'$ is torsion-free, by Theorem 3.8, we obtain

$$\begin{aligned}(\{t_i^{q-1}-t_n^{q-1}\}_{i=1}^{n-1}) &= (\{t_i^{q-1}-t_n^{q-1}\}_{i=1}^{n-1})\colon(t_1\cdots t_n)^\infty)\\ &= (I_{\mathcal{A}'}+(\{t_i^{q-1}-t_n^{q-1}\}_{i=1}^{n-1}))\colon(t_1\cdots t_n)^\infty)\\ &\overset{3.8}{=} I(X_1).\end{aligned}$$

Let $\mathbb{T}$ be a projective torus in $\mathbb{P}^{n-1}$. By Proposition 2.5, we have $I(\mathbb{T})=I(X_1)$. Consequently $X_1=\mathbb{T}$ because X_1 and $\mathbb{T}$ are projective varieties. Let δ_d' be the minimum distance of $C_{X_1}(d)$. Next we show that $\delta_d\leq\delta_d'$. There is a well defined epimorphism

$$\overline{\theta}_1\colon X\rightarrow X_1,\qquad [(x^{v_1},\ldots,x^{v_s})]\mapsto[(x^{v_1},\ldots,x^{v_n})]$$

induced by the projection map $[(\alpha_1,\ldots,\alpha_s)]\mapsto[(\alpha_1,\ldots,\alpha_n)]$. By part (a) one has $|X|=|X_1|=(q-1)^{n-1}$. Therefore the map $\overline{\theta}_1$ is an isomorphism of multiplicative groups. For any homogeneous polynomial F, we denote its zero set by $Z_X(F)=\{[P]\in X\,|\,F(P)=0\}$. Let $S'=K[t_1,\ldots,t_n]=\oplus_{d=0}^\infty S_d'$ and let $F_1\in S_d'$ be a polynomial such that $\mathrm{ev}_d(F_1)\neq 0$ and with $|Z_{X_1}|$ as large as possible, i.e., we choose F_1 so that $\delta_d'=|X_1|-|Z_{X_1}(F_1)|$. We can regard the polynomial $F_1=F_1(t_1,\ldots,t_n)$ as an element of S and denote it by F. The map $\overline{\theta}_1$ induces a bijective map

$$\overline{\theta}_1\colon Z_X(F)\mapsto Z_{X_1}(F_1),\qquad [P]\mapsto[\overline{\theta}_1(P)].$$

Therefore we have the inequality

$$\max\{|Z_X(F)|\colon F\in S_d;\,\mathrm{ev}_d(F)\neq 0\}\quad\geq\quad\max\{|Z_{X_1}(F_1)|\colon F_1\in S_d';\,\mathrm{ev}_d(F_1)\neq 0\}.$$

Consequently $\delta_d\leq\delta_d'$.

(c) We continue to use the notation and definitions used in the proof of part (b). Since $X_1=\mathbb{T}$, it suffices to show that $H_{X_1}(d)\leq H_X(d)$ for $d\geq 1$. Using that $I(X)$ and $I(X_1)$ are vanishing ideals generated by homogeneous polynomials, it is not hard to show that $S'\cap I(X)=I(X_1)$. Thus, we have a graded monomorphism

$$0\rightarrow K[t_1,\ldots,t_n]/I(X_1)\rightarrow K[t_1,\ldots,t_s]/I(X),\qquad \overline{F}_1\mapsto\overline{F}_1.$$

Hence $H_{X_1}(d)\leq H_X(d)$ and consequently $\mathrm{reg}(S/I(X))\leq\mathrm{reg}(S'/I(\mathbb{T}))=(q-2)(n-1)$. □

There is a nice recent formula for δ_d':

Theorem 5.2. [19, Theorem 3.4] *If $\mathbb{T}$ is a projective torus in $\mathbb{P}^{n-1}$ and $d\geq 1$, then the minimum distance of $C_{\mathbb{T}}(d)$ is given by*

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

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

Remark 5.3. (i) When d is greater than or equal to the index of regularity of $S/I(X)$, by Proposition 2.3, one has that $\delta_d = 1$. Thus, for $d \geq \text{reg}(S/I(X))$ our codes are useless from a practical point of view. For some other values of the parameters however, the bound δ'_d does not prevent our codes from having a large (although not optimal) minimum distance. In Example 5.4 we provide specific values of the parameters, for which our codes have a large minimum distance relative to $|X|$.

(ii) Let $\mathcal{C}$ be a unicyclic connected graph with n vertices and with a unique cycle of odd length. Then, $X = \mathbb{T}$ is a projective torus in $\mathbb{P}^{n-1}$ by Corollary 3.10. Thus, the minimum distance δ_d of $C_X(d)$ is equal to δ'_d by Theorem 5.2. This means that the bound of Theorem 5.1(b) is optimal.

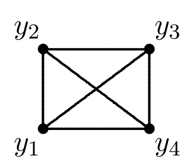
(iii) The problem of computing the minimum distance of a linear code is NP-hard [28]. It might not be easy to compute the minimum distance of $C_X(d)$ for graphs with large number of edges and vertices. However, for a complete graph with 4 vertices it is not hard to compute the minimum distance and to compare the bound δ'_d with the Singleton bound, see Example 5.5.

Example 5.4. Let $\mathcal{C}$ be a cycle of length 3, let X be the algebraic toric set parameterized by y_1y_2, y_2y_3, y_1y_3 and let $C_X(d)$ be the parameterized code of order d over the field $K = \mathbb{F}_{11}$. Using *Macaulay2*, together with Remark 5.3(ii), we obtain its basic parameters:

d	1	2	3	4	5	6	7	8	9	10	11	12	13
$\|X\|$	100	100	100	100	100	100	100	100	100	100	100	100	100
$\dim C_X(d)$	3	6	10	15	21	28	36	45	55	64	72	79	85
δ_d	90	80	70	60	50	40	30	20	10	9	8	7	6

d	14	15	16	17	18
$\|X\|$	100	100	100	100	100
$\dim C_X(d)$	90	94	97	99	100
δ_d	5	4	3	2	1

Example 5.5. Let $\mathcal{C}$ be the following complete graph on four vertices and let X be the algebraic toric set parameterized by all y_iy_j such that $\{y_i, y_j\}$ is an edge of $\mathcal{C}$.



Let $C_X(d)$ be the parameterized code of order d over the field $K = \mathbb{F}_3$, let b_d (resp. δ'_d) be the Singleton bound (resp. the bound of Theorem 5.1), and let δ_d be the minimum distance of $C_X(d)$. Using *Macaulay2*, we obtain:

d	1	2	3
b_d	3	1	1
δ'_d	4	2	1
δ_d	2	1	1

If $C_X(d)$ is the parameterized code of order d over the field $K = \mathbb{F}_4$, then we get:

d	1	2	3	4	5	6
b_d	22	9	1	1	1	1
δ'_d	18	9	6	3	2	1
δ_d	12	3	1	1	1	1

ACKNOWLEDGMENT

We thank Hiram López and Carlos Rentería for many stimulating discussions. We also thank the referees for their careful reading of the paper and for the improvements that they suggested.

REFERENCES

[1] D. Cox, J. Little and D. O'Shea, *Ideals, Varieties, and Algorithms*, Springer-Verlag, 1992.
[2] D. Cox, J. Little and D. O'Shea, *Using Algebraic Geometry*, Graduate Texts in Mathematics **185**, Springer-Verlag, 1998.
[3] P. Delsarte, J. M. Goethals and F. J. MacWilliams, On generalized Reed-Muller codes and their relatives, Information and Control **16** (1970), 403–442.
[4] I. M. Duursma, C. Rentería and H. Tapia-Recillas, Reed-Muller codes on complete intersections, Appl. Algebra Engrg. Comm. Comput. **11** (2001), no. 6, 455–462.
[5] D. Eisenbud, *The geometry of syzygies: A second course in commutative algebra and algebraic geometry*, Graduate Texts in Mathematics **229**, Springer-Verlag, New York, 2005.
[6] D. Eisenbud and B. Sturmfels, Binomial ideals, Duke Math. J. **84** (1996), 1–45.
[7] C. Escobar, J. Martínez-Bernal and R. H. Villarreal, Relative volumes and minors in monomial subrings, Linear Algebra Appl. **374** (2003), 275–290.
[8] A. V. Geramita, M. Kreuzer and L. Robbiano, Cayley-Bacharach schemes and their canonical modules, Trans. Amer. Math. Soc. **339** (1993), no. 1, 163–189.
[9] A. M. H. Gerards and A. Sebö, Total dual integrality implies local strong unimodularity, Math. Programming **38** (1987), no. 1, 69–73.
[10] 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.
[11] 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.
[12] 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.
[13] D. Grayson and M. Stillman, *Macaulay*2, 1996. Available via anonymous ftp from `math.uiuc.edu`.
[14] J. Harris, *Algebraic Geometry. A first course*, Graduate Texts in Mathematics **133**, Springer-Verlag, New York, 1992.
[15] D. Joyner, Toric codes over finite fields, Appl. Algebra Engrg. Comm. Comput. **15** (2004), no. 1, 63–79.
[16] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-correcting Codes*, North-Holland, 1977.
[17] C. Rentería, A. Simis and R. H. Villarreal, Algebraic methods for parameterized codes and invariants of vanishing ideals over finite fields, Finite Fields Appl. **17** (2011), no. 1, 81-104.
[18] E. Reyes, R. H. Villarreal and L. Zárate, A note on affine toric varieties, Linear Algebra Appl. **318** (2000), 173–179.
[19] E. Sarmiento, M. Vaz Pinto and R. H. Villarreal, The minimum distance of parameterized codes on projective tori, Appl. Algebra Engrg. Comm. Comput., to appear. Preprint, 2010, arXiv:1009.4966v2 [math.AC].
[20] A. Simis, W. V. Vasconcelos and R. H. Villarreal, On the ideal theory of graphs, J. Algebra, **167** (1994), 389–416.
[21] A. Simis, W. V. Vasconcelos and R. H. Villarreal, The integral closure of subrings associated to graphs, J. Algebra **199** (1998), 281–289.
[22] A. Sørensen, Projective Reed-Muller codes, IEEE Trans. Inform. Theory **37** (1991), no. 6, 1567–1576.
[23] R. Stanley, Hilbert functions of graded algebras, Adv. Math. **28** (1978), 57–83.
[24] H. Stichtenoth, *Algebraic function fields and codes*, Universitext, Springer-Verlag, Berlin, 1993.

[25] B. Sturmfels, *Gröbner Bases and Convex Polytopes*, University Lecture Series **8**, American Mathematical Society, Rhode Island, 1996.
[26] M. Tsfasman, S. Vladut and D. Nogin, *Algebraic geometric codes*: *basic notions*, Mathematical Surveys and Monographs **139**, American Mathematical Society, Providence, RI, 2007.
[27] J. H. van Lint, *Introduction to coding theory*, Third edition, Graduate Texts in Mathematics **86**, Springer-Verlag, Berlin, 1999.
[28] A. Vardy, Algorithmic complexity in coding theory and the minimum distance problem, STOC'97 (El Paso, TX), 92109 (electronic), ACM, New York, 1999.
[29] R. H. Villarreal, *Monomial Algebras*, Monographs and Textbooks in Pure and Applied Mathematics **238**, Marcel Dekker, New York, 2001.

Departamento de Matemáticas, Centro de Investigación y de Estudios Avanzados del IPN, Apartado Postal 14–740, 07000 Mexico City, D.F.

E-mail address: esarmiento@math.cinvestav.mx

Departamento de Matemática, Instituto Superior Tecnico, Universidade Técnica de Lisboa, Avenida Rovisco Pais, 1, 1049-001 Lisboa, Portugal

E-mail address: vazpinto@math.ist.utl.pt

Departamento de Matemáticas, Centro de Investigación y de Estudios Avanzados del IPN, Apartado Postal 14–740, 07000 Mexico City, D.F.

E-mail address: vila@math.cinvestav.mx