THE MINIMUM DISTANCE OF PARAMETERIZED CODES OF COMPLETE INTERSECTION VANISHING IDEALS OVER FINITE FIELDS

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

ABSTRACT. Let X be a subset of a projective space, over a finite field K, which is parameterized by the monomials arising from the edges of a clutter. Let $I(X)$ be the vanishing ideal of X. It is shown that $I(X)$ is a complete intersection if and only if X is a projective torus. In this case we determine the minimum distance of any parameterized linear code arising from 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 monomials. As usual if $v_i = (v_{i1}, \ldots, v_{in}) \in \mathbb{N}^n$, then we set

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

where $y_1, \ldots, y_n$ are the indeterminates of a ring of polynomials with coefficients in K. Consider the following set parameterized by these monomials

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

where $K^* = K \setminus \{0\}$ and $\mathbb{P}^{s-1}$ is a projective space over the field K. Following [14] we call X an *algebraic toric set* parameterized by $y^{v_1}, \ldots, y^{v_s}$. The set X is a multiplicative group under componentwise multiplication.

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*

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

defines a linear map of K-vector spaces. The image of ev_d, denoted by $C_X(d)$, defines a *linear code*. Following [13] we call $C_X(d)$ a *parameterized code* of order d. As usual by a *linear code* we mean a linear subspace of $K^{|X|}$.

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. Indeed if we choose a degree $d \geq 1$, there is $f_0 \in S_d$ such that $f_0(P) \neq 0$ for any $[P] \in X$ and we can define $C_X(d)$ as the image of the evaluation map given by Eq. (1.1). In this generality—the resulting linear code—$C_X(d)$ is called an *evaluation code* associated to X [6]. It is also called a *projective Reed-Muller code* over the set X [4, 9]. Some families of evaluation codes have been studied extensively, including several variations of Reed-Muller codes [3, 4, 6, 7, 9, 15]. In this paper we will only deal with parameterized codes over finite fields.

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

2000 *Mathematics Subject Classification.* Primary 13P25; Secondary 14G50, 14G15, 11T71, 94B27, 94B05.
The first author was partially supported by CONACyT. The third author was partially supported by CONACyT grant 49251-F and SNI.

is the *minimum distance* which is given by

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

where $\|v\|$ 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

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

The parameters of evaluation codes over finite fields have been computed in a number of cases. If $X = \mathbb{P}^{s-1}$, the parameters of $C_X(d)$ are described in [15, Theorem 1]. If X is the image of the affine space $\mathbb{A}^{s-1}$ under the map $\mathbb{A}^{s-1} \to \mathbb{P}^{s-1}$, $x \mapsto [(1, x)]$, the parameters of $C_X(d)$ are described in [3, Theorem 2.6.2]. In this paper we examine the case when X is an algebraic toric set parameterized by $y^{v_1}, \ldots, y^{v_s}$.

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 $C_X(d)$. In Section 3 we show upper bounds for the number of roots, over an affine torus, of a polynomial in S (see Lemma 3.1 and Theorem 3.3). The main theorem of Section 3 is a formula for the minimum distance of $C_X(d)$, where

$$X = \{[(x_1, \ldots, x_s)] \in \mathbb{P}^{s-1} |\, x_i \in K^* \text{ for all } i\}$$

is a *projective torus* (see Theorem 3.4). Evaluation codes associated to a projective torus are called *generalized projective Reed-Solomon* codes [8]. If X is a projective torus in $\mathbb{P}^1$ or $\mathbb{P}^2$, we recover some formulas of [8, 13] for the minimum distance of $C_X(d)$ (see Proposition 3.5).

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 ideal $I(X)$ is called a *complete intersection* if it can be generated by $s - 1$ homogeneous polynomials of S. In Section 4 we study the ideal $I(X)$ when $v_1, \ldots, v_s$ are the characteristic vectors of the edges of a clutter (see Definition 4.1). We are able to classify when $I(X)$ is a complete intersection (see Theorem 4.4 and Corollary 4.5). The main algebraic fact about $I(X)$ that we need for this classification is a remarkable result of [13] showing that $I(X)$ is a binomial ideal. We show an optimal upper bound for the regularity of $I(X)$ in terms of the regularity of a complete intersection (see Proposition 4.6).

For all unexplained terminology and additional information we refer to [5] (for the theory of binomial ideals), [1, 16] (for the theory of polynomial ideals and Hilbert functions), and [12, 17, 18] (for the theory of error-correcting codes and algebraic geometric codes).

2. Preliminaries: Hilbert functions and the basic parameters of codes

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 their connection with the basic parameters of parameterized linear codes. Then we present some of the results 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

$$S_d/I(X)_d \simeq C_X(d).$$

Two of the basic parameters of $C_X(d)$ can be expressed using Hilbert functions of standard graded algebras [16], as we now explain. Recall that the *Hilbert function* of $S/I(X)$ is given by

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

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 $h_X(d) = |X|$ for $d \geq |X| - 1$, see [11, Lecture 13]. This means that $|X|$ equals the *degree* of $S/I(X)$. Thus $H_X(d)$ and $\deg(S/I(X))$ equal 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 $C_X(d)$ [13].

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

$$F_X(t) := \sum_{i=0}^{\infty} H_X(i)t^i = \sum_{i=0}^{\infty} \dim_K(S/I(X))_i t^i = \frac{h_0 + h_1 t + \cdots + h_r t^r}{1-t},$$

where $h_0, \ldots, h_r$ are positive integers. 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 [13] and by observing that $\{t_s\}$ is a regular system of parameters for $S/I(X)$ (see [16]). The number r equals the regularity index of $S/I(X)$ and the degree of $S/I(X)$ equals $h_0 + \cdots + h_r$ (see [16] or [19, Corollary 4.1.12]).

For convenience we recall the following result on complete intersections.

Proposition 2.1. [8, Theorem 1, Lemma 1] *If* $\mathbb{T} = \{[(x_1, \ldots, x_s)] \in \mathbb{P}^{s-1} |\, x_i \in K^* \,\forall\, i\}$ *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* $\deg(S/I(\mathbb{T})) = (q-1)^{s-1}$.

When $I(X)$ is a complete intersection, there is a general formula for the dimension of any projective Reed-Muller code arising from X [4]. Its proof uses the fact that the Koszul complex of a complete intersection ideal $I(X)$ gives the minimal free resolution of $S/I(X)$. For a projective torus one can find a formula for the dimension directly—without the use of a Koszul complex—as shown below.

Corollary 2.2 ([4])**.** *If* $\mathbb{T}$ *is a projective torus in* $\mathbb{P}^{s-1}$*, then the length of* $C_{\mathbb{T}}(d)$ *equals* $(q-1)^{s-1}$ *and its dimension is given by*

$$\dim_K C_{\mathbb{T}}(d) = \sum_{j=0}^{\left\lfloor \frac{d}{q-1} \right\rfloor} (-1)^j \binom{s-1}{j} \binom{s-1+d-j(q-1)}{s-1}.$$

Proof. According to Proposition 2.1, the length of $C_{\mathbb{T}}(d)$ equals $(q-1)^{s-1}$ and the Hilbert series of the graded algebra $S/I(\mathbb{T})$ is given by

$$F_{\mathbb{T}}(t) = \frac{(1-t^{q-1})^{s-1}}{(1-t)^s} = \sum_{d=0}^{\infty} H_{\mathbb{T}}(d)t^d = \left[\sum_{j=0}^{s-1} (-1)^j \binom{s-1}{j} t^{j(q-1)}\right] \left[\sum_{i=0}^{\infty} \binom{s-1+i}{s-1} t^i\right].$$

Hence comparing the coefficients of t^d on both sides of the equality we get

$$H_{\mathbb{T}}(d)=\sum_{i+j(q-1)=d}(-1)^j\binom{s-1}{j}\binom{s-1+i}{s-1}.$$

Thus making $i=d-j(q-1)$ we obtain the required expression for $\dim_K C_{\mathbb{T}}(d)$. $\Box$

In Section 3 we compute the minimum distance of $C_{\mathbb{T}}(d)$, which was an important piece of information—from the viewpoint of coding theory—missing in the literature.

3. Minimum distance in parameterized codes

We continue to use the notation and definitions used in the introduction. In this section we show some upper bounds for the number of roots, over an affine torus, of a polynomial in S. Then we determine the minimum distance of a parameterized linear code $C_X(d)$ when X is a projective torus in $\mathbb{P}^{s-1}$.

Let $\mathbb{T}^*=(K^*)^s$ be an *affine torus*. For $G\in S$, we denote the zero set of G in $\mathbb{T}^*$ by Z_G. We begin with a general bound that will be refined later in the section.

Lemma 3.1. *Let $0\neq G=G(t_1,\ldots,t_s)\in S$ be a polynomial of total degree d. If*

$$Z_G:=\{x\in(K^*)^s\,|\,G(x)=0\},$$

then $|Z_G|\leq d(q-1)^{s-1}$.

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

$$G=G(t_1,\ldots,t_s)=G_0(t_1,\ldots,t_{s-1})+G_1(t_1,\ldots,t_{s-1})t_s+\cdots+G_r(t_1,\ldots,t_{s-1})t_s^r, \quad (3.1)$$

where $G_r\neq 0$ and $0\leq r\leq d$. Let β be a generator of the cyclic group $(K^*,\,\cdot)$. We set

$$H_k=H_k(t_2,\ldots,t_s):=G(\beta^k,t_2,\ldots,t_s)$$

for $1\leq k\leq q-1$.

Case (I): $H_k(t_2,\ldots,t_s)=0$ for some $1\leq k\leq q-1$. From Eq. (3.1) we get

$$H_k(t_2,\ldots,t_s)=G_0(\beta^k,t_2,\ldots,t_{s-1})+G_1(\beta^k,t_2,\ldots,t_{s-1})t_s+\cdots+G_r(\beta^k,t_2,\ldots,t_{s-1})t_s^r=0.$$

Therefore $G_i(\beta^k,t_2,\ldots,t_{s-1})=0$ for $i=0,\ldots,r$. Hence $t_1-\beta^k$ divides $G_i(t_1,\ldots,t_{s-1})$ for all i. Thus, by Eq. (3.1), we can write

$$G(t_1,\ldots,t_s)=(t_1-\beta^k)G'(t_1,\ldots,t_s)$$

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

$$|Z_G|\leq|Z_{(t_1-\beta^k)}|+|Z_{G'(t_1,\ldots,t_s)}|\leq(q-1)^{s-1}+(d-1)(q-1)^{s-1}=d(q-1)^{s-1}.$$

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

$$Z_G\subset\bigcup_{k=1}^{q-1}(\{\beta^k\}\times Z_{H_k(t_2,\ldots,t_s)})$$

where $Z_{H_k(t_2,\ldots,t_s)}=\{(x_2,\ldots,x_s)\in(K^*)^{s-1}\,|\,H_k(x_2,\ldots,x_s)=0\}$. As deg $H_k(t_2,\ldots,t_s)+s-1<d+s$, then by induction

$$|Z_G|\leq\sum_{k=1}^{q-1}|Z_{H_k(t_2,\ldots,t_s)}|\leq(q-1)d(q-1)^{s-2}=d(q-1)^{s-1},$$

as required. □

Lemma 3.2. *Let d,d',s be positive integers such that $d=k(q-2)+\ell$ and $d'=k'(q-2)+\ell'$ for some integers k,k',ℓ,ℓ' satisfying that $k,k'\geq 0$ and $1\leq\ell,\ell'\leq q-2$. If $d'\leq d$ and $k\leq s-1$, then $k'\leq k$ and*

$$-(q-1)^{s-k'}+\ell'(q-1)^{s-k'-1}\leq-(q-1)^{s-k}+\ell(q-1)^{s-k-1}.$$

Proof. It is not hard to see that $k'\leq k$. It suffices to prove the equivalent inequality:

$$q-1-\ell\leq(q-1)^{k-k'}(q-1-\ell').$$

If $k=k'$, then $\ell\geq\ell'$ and the inequality holds. If $k\geq k'+1$, then

$$q-1-\ell\leq q-1\leq(q-1)(q-1-\ell')\leq(q-1)^{k-k'}(q-1-\ell'),$$

as required. □

Theorem 3.3. *Let $G=G(t_1,\ldots,t_s)\in S$ be a polynomial of total degree $d\geq 1$ such that $\deg_{t_i}(G)\leq q-2$ for $i=1,\ldots,s$. If $d=k(q-2)+\ell$ with $1\leq\ell\leq q-2$ and $0\leq k\leq s-1$, then*

$$|Z_G|\leq(q-1)^{s-k-1}((q-1)^{k+1}-(q-1)+\ell).$$

Proof. By induction on s. If $s=1$, then $k=0$ and $d=\ell$. Then $|Z_G|\leq\ell$ because a non-zero polynomial in one variable of degree d has at most d roots. Assume $s\geq 2$. By Lemma 3.1 we may also assume that $k\geq 1$. There are $r\geq 0$ distinct elements $\beta_1,\ldots,\beta_r$ in K^* and $G'\in S$ such that

$$G=(t_1-\beta_1)^{a_1}\cdots(t_1-\beta_r)^{a_r}G',\qquad a_i\geq 1\,\forall\,i,$$

and $G'(\beta,t_2,\ldots,t_s)\neq 0$ for any $\beta\in K^*$. Notice that $r\leq\sum_i a_i\leq q-2$ because the degree of G in t_1 is at most $q-2$. We can write $K^*=\{\beta_1,\ldots,\beta_{q-1}\}$. Let d_i' be the degree of $G'(\beta_i,t_2,\ldots,t_s)$ and let $d'=\max\{d_i'|\ r+1\leq i\leq q-1\}$. If $d'=0$, then $|Z_G|=r(q-1)^{s-1}$ and consequently

$$r(q-1)^{s-1}\leq(q-2)(q-1)^{s-1}\leq(q-1)^{s-k-1}((q-1)^{k+1}-(q-1)+\ell).$$

The second inequality uses that $k\geq 1$. Thus we may assume that $d'>0$ and also that $\beta_{r+1},\ldots,\beta_m$ are the elements β_i of $\{\beta_{r+1},\ldots,\beta_{q-1}\}$ such that $G'(\beta_i,t_2,\ldots,t_s)$ has positive degree. Notice that $d=\sum_i a_i+\deg(G')\geq r+d'$. The polynomial

$$H:=(t_1-\beta_1)^{a_1}\cdots(t_1-\beta_r)^{a_r}$$

has exactly $r(q-1)^{s-1}$ roots in $(K^*)^s$. Hence counting the roots of G' that are not in Z_H we obtain:

$$|Z_G|\leq r(q-1)^{s-1}+\sum_{i=r+1}^{m}|Z_{G'(\beta_i,t_2,\ldots,t_s)}|. \tag{3.2}$$

For each $r+1\leq i\leq m$, we can write $d_i'=k_i'(q-2)+\ell_i'$, with $1\leq\ell_i'\leq q-2$. The proof will be divided in three cases.

Case (I): Assume $\ell > r$ and $k = s-1$. By [2, Theorem 1.2], the nonzero polynomial $G'(\beta_i, t_2, \ldots, t_s)$ cannot be the zero-function on $(K^*)^{s-1}$ for any i because its degree in each variable is at most $q-2$. Thus by Eq. (3.2) we get

$$|Z_G| \leq r(q-1)^{s-1} + (q-1-r)((q-1)^{s-1}-1) \leq (q-1)^s - (q-1) + \ell.$$

Case (II): Assume $\ell > r$ and $k \leq s-2$. Then $d - r = k(q-2) + (\ell - r)$ with $1 \leq \ell - r \leq q-2$. Since $d'_i \leq d - r$ for $i = r+1, \ldots, m$, by Lemma 3.2, we get $k'_i \leq k$ for $r+1 \leq i \leq m$. Then by induction hypothesis, using Eq. (3.2) and Lemma 3.2, we obtain:

$$\begin{aligned}
|Z_G| &\leq r(q-1)^{s-1} + \sum_{i=r+1}^{m} |Z_{G'(\beta_i, t_2, \ldots, t_s)}| \\
&\leq r(q-1)^{s-1} + \sum_{i=r+1}^{m} \left[(q-1)^{(s-1)-k'_i-1}((q-1)^{k'_i+1} - (q-1) + \ell'_i)\right] \\
&\leq r(q-1)^{s-1} + (q-1-r)\left[(q-1)^{(s-1)-k-1}((q-1)^{k+1} - (q-1) + (\ell - r))\right] \\
&\leq (q-1)^{s-k-1}((q-1)^{k+1} - (q-1) + \ell).
\end{aligned}$$

Case (III): Assume $\ell \leq r$. Then we can write $d - r = k_2(q-2) + \ell_2$ with $k_2 = k-1$ and $\ell_2 = q - 2 + \ell - r$. Notice that $0 \leq k_2 \leq s-2$ and $1 \leq \ell_2 \leq q-2$ because $k \geq 1$, $r \leq q-2$ and $k \leq s-1$. Since $d'_i \leq d - r$ for $i > r$, by Lemma 3.2, we get $k'_i \leq k_2$ for $i = r+1, \ldots, m$. Then by induction hypothesis, using Eq. (3.2) and Lemma 3.2, we obtain:

$$\begin{aligned}
|Z_G| &\leq r(q-1)^{s-1} + \sum_{i=r+1}^{m} |Z_{G'(\beta_i, t_2, \ldots, t_s)}| \\
&\leq r(q-1)^{s-1} + \sum_{i=r+1}^{m} \left[(q-1)^{(s-1)-k'_i-1}((q-1)^{k'_i+1} - (q-1) + \ell'_i)\right] \\
&\leq r(q-1)^{s-1} + (q-1-r)\left[(q-1)^{(s-1)-k_2-1}((q-1)^{k_2+1} - (q-1) + \ell_2)\right] \\
&= r(q-1)^{s-1} + (q-1-r)\left[(q-1)^{s-k-1}((q-1)^{k} - (q-1) + (q-2+\ell-r))\right] \\
&\leq (q-1)^{s-k-1}((q-1)^{k+1} - (q-1) + \ell).
\end{aligned}$$

The last inequality uses that $r \leq q-2$. This completes the proof of the result. □

We come to the main result of this section.

Theorem 3.4. *If $X = \{[(x_1, \ldots, x_s)] \in \mathbb{P}^{s-1} | \, x_i \in K^* \text{ for all } i\}$ is a projective torus and $d \geq 1$, then the minimum distance of $C_X(d)$ is given by*

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

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

Proof. First we consider the case $1 \leq d \leq (q-2)(s-1)-1$. Then in this case we have that $k \leq s-2$. Let $\prec$ be the graded reverse lexicographical order (grevlex) on the monomials of S.

In this order $t_1 \succ \cdots \succ t_s$. Let F be a homogeneous polynomial of S of degree d such that F does not vanish on X. By the division algorithm [1, Theorem 1.5.9, p. 30], we can write

$$F = h_1(t_1^{q-1} - t_s^{q-1}) + \cdots + h_{s-1}(t_{s-1}^{q-1} - t_s^{q-1}) + F', \tag{3.3}$$

with $\deg_{t_i}(F') \leq q-2$ for $i = 1, \ldots, s-1$ and $d' = \deg(F') \leq d$. We set

$$\begin{aligned} Z_{F(t_1,\ldots,t_{s-1},1)} &= \{(x_1, x_2, \ldots, x_{s-1}, 1) \in (K^*)^{s-1} \times \{1\} \,|\, F(x_1, x_2, \ldots, x_{s-1}, 1) = 0\}, \\ A_F &= \{[x] \in X \,|\, F(x) = 0\}. \end{aligned}$$

Notice that there is a bijection

$$Z_{F(t_1,\ldots,t_{s-1},1)} \longrightarrow A_F, \qquad (x_1, \ldots, x_{s-1}, 1) \mapsto [(x_1, \ldots, x_{s-1}, 1)].$$

Hence $|A_F| = |Z_{F(t_1,\ldots,t_{s-1},1)}|$. Using Eq. (3.3), we get $Z_{F(t_1,\ldots,t_{s-1},1)} = Z_{F'(t_1,\ldots,t_{s-1},1)}$. Now we set

$$H = H(t_1, \ldots, t_{s-1}) = F'(t_1, \ldots, t_{s-1}, 1) \ \text{ and } \ Z_H = \{x \in (K^*)^{s-1} \,|\, H(x) = 0\}.$$

The polynomial H does not vanish on $(K^*)^{s-1}$. This follows from Eq. (3.3) and using that F is homogeneous and that F does not vanish on X. We may assume that $d' \geq 1$, otherwise $Z_{F'(t_1,\ldots,t_{s-1},1)} = \emptyset$ and $|A_F| = 0$. Then we can write $d' = k'(q-2) + \ell'$ for some integers $k' \geq 0$ and $1 \leq \ell' \leq q-2$. Since $k \leq s-2$, by Lemma 3.2, we obtain that $k' \leq k$ and

$$-(q-1)^{s-1-k'} + \ell'(q-1)^{s-2-k'} \leq -(q-1)^{s-1-k} + \ell(q-1)^{s-2-k}. \tag{3.4}$$

Then $k' \leq s-2$ and H is a non-zero polynomial of degree $d' \geq 1$ in $s-1$ variables such that $\deg_{t_i}(H) \leq q-1$ for $i = 1, \ldots, s-1$. Therefore applying Theorem 3.3 to H and then using Eq. (3.4) we derive

$$\begin{aligned} |A_F| = |Z_H| &\leq (q-1)^{s-k'-2}((q-1)^{k'+1} - (q-1) + \ell') \\ &\leq (q-1)^{s-k-2}((q-1)^{k+1} - (q-1) + \ell). \end{aligned}$$

Since F was an arbitrary homogeneous polynomial of degree d such that F does not vanish on X we obtain

$$M := \max\{|A_F| \colon F \in S_d;\, F \not\equiv 0\} \leq (q-1)^{s-k-2}((q-1)^{k+1} - (q-1) + \ell),$$

where $F \not\equiv 0$ means that F is not the zero function on X. We claim that

$$M = (q-1)^{s-k-2}((q-1)^{k+1} - (q-1) + \ell).$$

Let M_1 be the expression in the right hand side. It suffices to show that M is bounded from below by M_1 or equivalently it suffices to exhibit a homogeneous polynomial $F \not\equiv 0$ of degree d with exactly M_1 roots in X. Let β be a generator of the cyclic group $(K^*, \cdot)$. Consider the polynomial $F = f_1 f_2 \cdots f_k g_\ell$, where $f_1, \ldots, f_k, g_\ell$ are given by

$$\begin{aligned} f_1 &= (\beta t_1 - t_2)(\beta^2 t_1 - t_2) \cdots (\beta^{q-2} t_1 - t_2), \\ f_2 &= (\beta t_1 - t_3)(\beta^2 t_1 - t_3) \cdots (\beta^{q-2} t_1 - t_3), \\ &\ \ \vdots \qquad\qquad\qquad \vdots \\ f_k &= (\beta t_1 - t_{k+1})(\beta^2 t_1 - t_{k+1}) \cdots (\beta^{q-2} t_1 - t_{k+1}), \\ g_\ell &= (\beta t_1 - t_{k+2})(\beta^2 t_1 - t_{k+2}) \cdots (\beta^{\ell} t_1 - t_{k+2}). \end{aligned}$$

Now, the roots of F in X are in one to one correspondence with the union of the sets:

$$\begin{gathered}\{1\}\times\{\beta^i\}_{i=1}^{q-2}\times(K^*)^{s-2},\\ \{1\}\times\{1\}\times\{\beta^i\}_{i=1}^{q-2}\times(K^*)^{s-3},\\ \vdots\\ \{1\}\times\cdots\times\{1\}\times\{\beta^i\}_{i=1}^{q-2}\times(K^*)^{s-(k+1)},\\ \{1\}\times\cdots\times\{1\}\times\{\beta^i\}_{i=1}^{\ell}\times(K^*)^{s-(k+2)}.\end{gathered}$$

Therefore the number of zeros of F in X is given by

$$\begin{aligned}|A_F| &= (q-2)(q-1)^{s-2}+(q-2)(q-1)^{s-3}+\cdots+(q-2)(q-1)^{s-(k+1)}+\ell(q-1)^{s-(k+2)}\\ &= (q-1)^{s-(k+2)}\left[(q-2)(q-1)^k+\cdots+(q-2)(q-1)+\ell\right]\\ &= (q-1)^{s-(k+2)}\left[(q-2)(q-1)((q-1)^{k-1}+\cdots+1)+\ell\right]\\ &= (q-1)^{s-(k+2)}\left[(q-1)^{s-(k+2)}\left((q-2)(q-1)\left(\frac{(q-1)^k-1}{q-2}\right)+\ell\right)\right]\\ &= (q-1)^{s-(k+2)}\left[(q-1)((q-1)^k-1)+\ell\right]\\ &= (q-1)^{s-(k+2)}\left[(q-1)^{k+1}-(q-1)+\ell\right],\end{aligned}$$

as required. Thus $M=M_1$ and the claim is proved. Therefore

$$\begin{aligned}\delta_d &= \min\{\|\mathrm{ev}_d(F)\|\colon \mathrm{ev}_d(F)\neq 0; F\in S_d\}=|X|-\max\{|A_F|\colon F\in S_d;\ F\not\equiv 0\}\\ &= (q-1)^{s-1}-\left((q-1)^{s-k-2}((q-1)^{k+1}-(q-1)+\ell)\right)\\ &= (q-1)^{s-k-2}((q-1)-\ell),\end{aligned}$$

where $\|\mathrm{ev}_d(F)\|$ is the number of non-zero entries of $\mathrm{ev}_d(F)$. This completes the proof of the case $1\leq d\leq (q-2)(s-1)-1$.

Next we consider the case $d\geq (q-2)(s-1)$. By the Singleton bound we get

$$1\leq \delta_d\leq |X|-H_X(d)+1=1$$

for $d\geq \mathrm{reg}(S/I(X))$. Hence, applying Proposition 2.1, we get $\delta_d=1$ for $d\geq (s-1)(q-2)$. □

The next proposition is an immediate consequence of our result. Recall that a linear code is called *maximum distance separable* (MDS for short) if equality holds in the Singleton bound.

Proposition 3.5 ([8, 13])**.** *If X is a projective torus in $\mathbb{P}^1$, then $C_X(d)$ is an MDS code and its minimum distance is given by*

$$\delta_d=\begin{cases} q-1-d & \text{if } 1\leq d\leq q-3,\\ 1 & \text{if } d\geq q-2.\end{cases}$$

If X is a projective torus in $\mathbb{P}^2$, then the minimum distance of $C_X(d)$ is given by

$$\delta_d=\begin{cases} (q-1)^2-d(q-1) & \text{if } 1\leq d\leq q-2,\\ 2q-d-3 & \text{if } q-1\leq d\leq 2q-5,\\ 1 & \text{if } d\geq 2q-4.\end{cases}$$

Parameterized codes arising from complete bipartite graphs have been studied in [7]. In this case one can use our result together with the following theorem to compute the minimum distance.

Theorem 3.6 ([7]). *Let $\mathcal{K}_{k,\ell}$ be a complete bipartite graph, let X be the toric set parameterized by the edges of $\mathcal{K}_{k,\ell}$, and let X_1 and X_2 be the projective torus of dimension $\ell-1$ and $k-1$ respectively. Then the length, dimension and minimum distance of $C_X(d)$ are equal to*

$$(q-1)^{k+\ell-2},\quad H_{X_1}(d)H_{X_2}(d),\quad \text{and}\quad \delta_1\delta_2$$

respectively, where δ_i is the minimum distance of $C_{X_i}(d)$.

4. Complete intersection ideals of parameterized sets of clutters

We continue to use the notation and definitions used in the introduction and in the preliminaries.

Definition 4.1. 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 example of a clutter is a graph with the vertices and edges defined in the usual way for graphs.

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 section we assume that $v_1,\ldots,v_s$ is the set of all characteristic vectors of the edges of $\mathcal{C}$.

Definition 4.2. 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 4.3. *Let $\mathcal{C}$ be a clutter. If $f\neq 0$ is a homogeneous polynomial 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 $\deg(f)\geq q-1$. Moreover if $b=q-1$, 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

$$(x_1^{v_{11}}\cdots x_n^{v_{1n}})^b=(x_1^{v_{21}}\cdots x_n^{v_{2n}})^{c_2}\cdots(x_1^{v_{r1}}\cdots x_n^{v_{rn}})^{c_r}\qquad\forall\,(x_1,\ldots,x_n)\in(K^*)^n, \tag{4.1}$$

where $v_i=(v_{i1},\ldots,v_{in})$. 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 $j=2,\ldots,r$, otherwise if $v_{jk}=0$ for some $j\geq 2$, then making $x_i=1$ for $i\neq k$ in Eq. (4.1) we get $(x_k^{v_{1k}})^b=x_k^b=x_k^m$, where $m<b$. Then $x_k^{b-m}=1$ for $x_k\in K^*$. In particular if β is a generator of the cyclic group $(K^*,\,\cdot)$, then $\beta^{b-m}=1$. 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.

To show the second part of the lemma assume that $f=t_1^{q-1}-t_2^{c_2}\cdots t_r^{c_r}$ with $\sum_i c_i=q-1$. Assume that $r\geq 3$. Then

$$1=(x_1^{v_{21}}\cdots x_n^{v_{2n}})^{c_2}\cdots(x_1^{v_{r1}}\cdots x_n^{v_{rn}})^{c_r}\qquad\forall\,(x_1,\ldots,x_n)\in(K^*)^n. \tag{4.2}$$

We claim that if $v_{2k}=1$ for some $1\leq k\leq n$, then $v_{jk}=1$ for $j=3,\ldots,r$, otherwise if $v_{jk}=0$ for some $j\geq 3$, then making $x_i=1$ for $i\neq k$ in Eq. (4.2) we get $1=x_k^m$ for any $x_k\in K^*$, where $m<q-1$, a contradiction because $(K^*,\,\cdot\,)$ is a cyclic group of order $q-1$. This completes the proof of the claim. Therefore $\operatorname{supp}(v_2)\subset\operatorname{supp}(v_j)$ for $j=3,\ldots,r$. Since $\mathcal{C}$ is a clutter we get

that $v_2 = v_j$ for $j = 3, \ldots, r$, a contradiction because $v_1, \ldots, v_r$ are distinct. Therefore $r = 2$, as required. □

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

Theorem 4.4. *Let $\mathcal{C}$ be a clutter. If $I(X)$ is a complete intersection, then*

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

Proof. According to [13] the vanishing ideal $I(X)$ is a binomial ideal. Therefore there is a set $\mathcal{B} = \{h_1, \ldots, h_{s-1}\}$ of homogeneous binomials that generate the ideal $I(X)$. We may assume that $h_1, \ldots, h_m$ are the binomials of $\mathcal{B}$ that contain a term of the form $t_i^{c_i}$. By Lemma 4.3 we have that $\deg(h_i) \geq q-1$ for $i = 1, \ldots, m$. Thus we may assume that $h_1, \ldots, h_k$ are the binomials of $\mathcal{B}$ of degree $q-1$ that contain a term of the form t_i^{q-1} and that $h_{k+1}, \ldots, h_m$ have degree greater than $q-1$. By Lemma 4.3 the binomials $h_1, \ldots, h_k$ have the form $t_i^{q-1} - t_j^{q-1}$. Notice that $h_{m+1}, \ldots, h_{s-1}$ have both of their terms not in the set $\{t_1^{a_1}, \ldots, t_s^{a_s} \,|\, a_i \geq 1\, \forall\, i\}$. Since $t_i^{q-1} - t_s^{q-1}$ is in $I(X)$ for $i = 1, \ldots, s-1$, we can write

$$t_i^{q-1} - t_s^{q-1} = \sum_{\ell=1}^{k} \lambda_\ell h_\ell + \sum_{\ell=k+1}^{m} \mu_\ell h_\ell + \sum_{\ell=m+1}^{s-1} \theta_\ell h_\ell \qquad (\lambda_\ell,\, \mu_\ell,\, \theta_\ell \in S).$$

As $h_1, \ldots, h_{s-1}$ are homogeneous binomials we can rewrite this equality as:

$$t_i^{q-1} - t_s^{q-1} = \sum_{\ell=1}^{k} \lambda'_\ell h_\ell + \sum_{\ell=m+1}^{s-1} \theta'_\ell h_\ell,$$

where $\lambda'_\ell \in K$ for $\ell = 1, \ldots, k$ and for each $m+1 \leq \ell \leq s-1$ either $\theta'_\ell = 0$ and $\deg(h_\ell) > q-1$ or $\deg(h_\ell) \leq q-1$ and $\deg(h_\ell) + \deg(\theta'_\ell) = q-1$. Then

$$t_i^{q-1} - t_s^{q-1} - \sum_{\ell=1}^{k} \lambda'_\ell h_\ell = \sum_{\ell=m+1}^{s-1} \theta'_\ell h_\ell.$$

The left hand side of this equality has to be zero, otherwise a non-zero monomial that occur in the left hand side will have to occur in the right hand side which is impossible because monomials occurring on the left have the form λt_j^{q-1}, $\lambda \in K$, and monomials occurring on the right are never of this form. Hence we get the inclusion

$$(t_1^{q-1} - t_s^{q-1}, \ldots, t_{s-1}^{q-1} - t_s^{q-1}) \subset (h_1, \ldots, h_k).$$

Since the height of $(h_1, \ldots, h_k)$ is at most k, we get $s-1 \leq k$. Consequently $k = s-1$. Thus the inclusion above is an equality as required. □

Corollary 4.5. *Let $\mathcal{C}$ be a clutter with s edges and let $\mathbb{T} = \{[(x_1, \ldots, x_s)] \in \mathbb{P}^{s-1} |\, x_i \in K^*\}$ be a projective torus. 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) $X = \mathbb{T} \subset \mathbb{P}^{s-1}$.

Proof. (c_1)⇒(c_2): It follows at once from Theorem 4.4. (c_2)⇒(c_3): By Proposition 2.1 one has $I(X) = I(\mathbb{T}) = (\{t_i^{q-1} - t_s^{q-1}\}_{i=1}^{s-1})$. As X and $\mathbb{T}$ are both projective varieties, we get that $X = \mathbb{T}$ (see [13, Lemma 4.2] for details). (c_3)⇒(c_1): It follows at once from Proposition 2.1. □

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

Proposition 4.6. $\operatorname{reg}(S/I(X)) \leq (q-2)(s-1)$, *with equality if* $I(X)$ *is a complete intersection associated to a clutter with* s *edges.*

Proof. For $i \geq 0$, we set $h_i = \dim_K(S/(I(X), t_s))_i$. The regularity index of $S/I(X)$, denoted by r, satisfies that $h_i > 0$ for $i = 0, \ldots, r$ and $h_i = 0$ for $i > r$ (see Section 2). There is an exact sequence of graded S-modules

$$0 \longrightarrow (S/I(X))[-1] \stackrel{t_s}{\longrightarrow} S/I(X) \longrightarrow S/(I(X), t_s) \longrightarrow 0 \implies \tag{4.3}$$

$$h_i = H_X(i) - H_X(i-1) \geq 0. \tag{4.4}$$

On the other hand there is a surjection

$$D = S/(\{t_i^{q-1} - t_s^{q-1}\}_{i=1}^{s-1} \cup \{t_s\}) = K[t_1, \ldots, t_{s-1}]/(\{t_i^{q-1}\}_{i=1}^{s-1}) \longrightarrow S/(I(X), t_s) \longrightarrow 0.$$

The Hilbert series of D is equal to the polynomial $(1 + t + \cdots + t^{q-1})^{s-1}$ because the ideal $(\{t_i^{q-1}\}_{i=1}^{s-1})$ is a complete intersection [19, p. 104]. Hence $\operatorname{reg}(D) = (q-2)(s-1) + 1$. From the surjection above we get that $\dim_K D_i \geq h_i \geq 0$. If $i \geq \operatorname{reg}(D)$, we obtain $0 = \dim_K D_i \geq h_i \geq 0$. Then from Eq. (4.4) we conclude

$$H_X(i) = H_X(i-1) \quad \text{for } i \geq \operatorname{reg}(D).$$

Hence $\operatorname{reg}(S/I(X)) \leq (q-2)(s-1)$. To complete the proof assume that $I(X)$ is a complete intersection, then by Theorem 4.4 the ideal $I(X)$ is equal to $(t_1^{q-1} - t_s^{q-1}, \ldots, t_{s-1}^{q-1} - t_s^{q-1})$. Consequently $\operatorname{reg}(S/I(X)) = (q-2)(s-1)$. □

ACKNOWLEDGMENT

The authors thank Hiram López, who provided an alternative proof of Theorem 3.4, and Carlos Rentería for many stimulating discussions.

References

[1] W. W. Adams and P. Loustaunau, *An Introduction to Gröbner Bases*, GSM **3**, American Mathematical Society, 1994.
[2] N. Alon, Combinatorial Nullstellensatz, Recent trends in combinatorics (Mátraháza, 1995), Combin. Probab. Comput. **8** (1999), no. 1-2, 7–29.
[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 and B. Sturmfels, Binomial ideals, Duke Math. J. **84** (1996), 1–45.
[6] 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.
[7] M. González-Sarabia and C. Rentería, Evaluation codes associated to complete bipartite graphs, Int. J. Algebra **2** (2008), no. 1-4, 163–170.
[8] 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.
[9] 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.
[10] D. Grayson and M. Stillman, *Macaulay*2, 1996. Available via anonymous ftp from `math.uiuc.edu`.
[11] J. Harris, *Algebraic Geometry. A first course*, Graduate Texts in Mathematics **133**, Springer-Verlag, New York, 1992.
[12] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-correcting Codes, North-Holland, 1977.

[13] C. Rentería, A. Simis and R. H. Villarreal, Algebraic methods for parameterized codes and invariants of vanishing ideals over finite fields, Finite Fields Appl., to appear. Preprint, 2010, arXiv:1001.1448R.

[14] E. Reyes, R. H. Villarreal and L. Zárate, A note on affine toric varieties, Linear Algebra Appl. **318** (2000), 173–179.

[15] A. Sørensen, Projective Reed-Muller codes, IEEE Trans. Inform. Theory **37** (1991), no. 6, 1567–1576.

[16] R. Stanley, Hilbert functions of graded algebras, Adv. Math. **28** (1978), 57–83.

[17] H. Stichtenoth, Algebraic function fields and codes. Universitext, Springer-Verlag, Berlin, 1993.

[18] M. Tsfasman, S. Vladut and D. Nogin, *Algebraic geometric codes*: *basic notions*, Mathematical Surveys and Monographs **139**, American Mathematical Society, Providence, RI, 2007.

[19] 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