



Parameterized Codes over Cycles

Manuel González Sarabia, Joel Nava Lara, Carlos Rentería Márquez and Eliseo Sarmiento Rosales

Abstract

In this paper we will compute the main parameters of the parameterized codes arising from cycles. In the case of odd cycles the corresponding codes are the evaluation codes associated to the projective torus and the results are well known. In the case of even cycles we will compute the length and the dimension of the corresponding codes and also we will find lower and upper bounds for the minimum distance of this kind of codes. In many cases our upper bound is sharper than the Singleton bound.

1 Introduction

Coding theory is a branch of mathematics that is related to other disciplines, like information theory, computer science, cryptography, graph theory and others. It was born in the middle of the last century with the publication of the work of C.E. Shannon, [14]. In this paper we develop some interesting applications of several tools of commutative algebra and algebraic geometry in order to describe the main parameters of some particular evaluation codes arising from cycles. In fact the bounds for the minimum distance that we find in the subsection 3.2.3 are good enough (for example, our upper bound is sharper than the Singleton bound in many cases). It is worth pointing out that the core of this work is the relation between the parameters of these codes

Key Words: Cycle, Parameterized code, Minimum distance.

2010 Mathematics Subject Classification: Primary 13P25, 14G50; Secondary 14G15, 11T71, 94B27, 94B05.

Received: April, 2013.

Revised: April, 2013.

Accepted: June, 2013.

(length, dimension, minimum distance) and some invariants of I_X (degree, Hilbert function, regularity).

Parameterized codes were introduced in [11]. In that paper the authors computed the length of the parameterized codes associated to any connected simple graph (Corollary 3.8). Unfortunately this is the only parameter that has been found in the general case (for any simple graph). The other two parameters (dimension and minimum distance) must be studied in particular cases. For example, the main parameters of the evaluation codes arising from complete bipartite graphs were described in [5]. We use these approximations in order to study a case that, in spite of the simplicity of the graphs (they are cycles), is very hard.

We start with some necessary definitions.

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

$$Z^{v_i} = Z_1^{v_{i1}} \dots Z_n^{v_{in}}, \quad i = 1, \dots, s,$$

where Z_1, \dots, Z_n are the indeterminates of a ring of polynomials with coefficients in K . Consider the following set parameterized by these monomials

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

where $K^* = K \setminus \{0\}$ and \mathbb{P}^{s-1} is a projective space over the field K . Following [12] we call X an *algebraic toric set* parameterized by Z^{v_1}, \dots, Z^{v_s} . The set X is a multiplicative group under componentwise multiplication.

Let $S = K[T_1, \dots, T_s] = \bigoplus_{d=0}^{\infty} S_d$ be a polynomial ring over the field K with the standard grading, let $[P_1], \dots, [P_{|X|}]$ be the points of X , and let $f_0(T_1, \dots, T_s) = T_1^d$. The *evaluation map*

$$\text{ev}_d: S_d = K[T_1, \dots, T_s]_d \rightarrow K^{|X|}, \quad f \mapsto \left(\frac{f(P_1)}{f_0(P_1)}, \dots, \frac{f(P_{|X|})}{f_0(P_{|X|})} \right) \quad (1)$$

defines a linear map of K -vector spaces. The image of ev_d , denoted by $C_X(d)$, defines a *linear code*. Following [11] 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 $d \geq 1$, for each i there is $f_i \in S_d$ such that $f_i(P_i) \neq 0$ and we can define $C_X(d)$ as the image of the evaluation map given by

$$\text{ev}_d: S_d = K[T_1, \dots, T_s]_d \rightarrow K^{|X|}, \quad f \mapsto \left(\frac{f(P_1)}{f_1(P_1)}, \dots, \frac{f(P_{|X|})}{f_{|X|}(P_{|X|})} \right). \quad (2)$$

In this generality—the resulting linear code— $C_X(d)$ is called an *evaluation code* associated to X [4]. It is also called a *projective Reed-Muller code* over the set X [3, 7]. Some families of evaluation codes have been studied extensively, including several variations of Reed-Muller codes [2, 3, 4, 5, 7, 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 is the *minimum distance* which is given by

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

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

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

The parameters of evaluation codes over finite fields have been computed in several 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 $\mathbb{A}^{s-1} \rightarrow \mathbb{P}^{s-1}$, $x \mapsto [(1, x)]$, the parameters of $C_X(d)$ are described in [2, Theorem 2.6.2]. In this paper we examine the case when X is an algebraic toric set parameterized by $Z_1Z_2, Z_2Z_3, \dots, Z_{n-1}Z_n, Z_nZ_1$.

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 .

For all unexplained terminology and additional information we refer to [1, 16] (for the theory of polynomial ideals and Hilbert functions), and [10, 17, 18] (for the theory of error-correcting codes and algebraic geometric codes).

2 Preliminaries

We continue using the notation and definitions given 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 Z^{v_1}, \dots, Z^{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), 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 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 [9, 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 $C_X(d)$ [11].

The *index of regularity* of S/I_X , denoted by $\text{reg}(S/I_X)$, 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, \dots, 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 [11] 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]).

3 Parameterized codes arising from cycles

From now on we will use $s = n$ in the definitions given in the introduction. In our case the number of monomials that parameterize an algebraic toric set is the same that the number of variables in the corresponding polynomial ring. The toric set parameterized by the edges of a cycle C_n is given by

$$X = \{[(a_1 a_2, a_2 a_3, \dots, a_{n-1} a_n, a_n a_1)] \in \mathbb{P}^{n-1} : a_i \in K^* \text{ for all } i = 1, \dots, n\}, \quad (3)$$

and when we say a projective torus of order $n - 1$ we mean the toric set

$$\mathbb{T}_{n-1} = \{[(a_1, \dots, a_n)] \in \mathbb{P}^{n-1} : a_i \in K^* \text{ for all } i = 1, \dots, n\}. \quad (4)$$

In the next section we will analyze the case where n is an odd number.

3.1 Odd cycles

We will take $n = 2k + 1$. It is immediate that the set X that appears in the Eq. (3) becomes \mathbb{T}_{2k} and in this case the parameterized codes $C_X(d)$ are called generalized Reed-Solomon codes and their main parameters are well known ([6], [13]).

Theorem 3.1. *The main characteristics of the parameterized codes arising from the edges of an odd cycle C_{2k+1} are the following:*

- *Length:* $|X| = (q - 1)^{2k}$.
- *Vanishing ideal:* $I_X = (\{T_i^{q-1} - T_1^{q-1}\}_{i=2}^{2k+1})$.
- *Hilbert series:* $F_X(t) = \frac{(1-t^{q-1})^{2k}}{(1-t)^{2k+1}}$.
- *Index of regularity:* $\text{reg}(S/I_X) = 2k(q - 2)$.
- *Dimension:* $H_X(d) = \binom{2k+d}{d} + \sum_{i=1}^{2k} (-1)^i \binom{2k}{i} \binom{2k+d-i(q-1)}{d-i(q-1)}$.
- *Minimum distance:*

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

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

3.2 Even cycles

In this case we will take $n = 2k$. The toric set X is given by Eq. (3). In the following sections we will describe the length and dimension of the parameterized codes arising from even cycles. Finally, we will find lower and upper bounds for the minimum distance of these codes.

3.2.1 Length

In the next theorem we will compute the first parameter of the parameterized codes associated to even cycles.

Theorem 3.2. *The length of the parameterized codes arising from the edges of an even cycle C_{2k} is given by:*

$$|X| = (q - 1)^{2k-2}. \quad (5)$$

Proof. Let φ be the following map:

$$\begin{aligned} \varphi : X &\rightarrow \mathbb{T}_{k-1}, \\ \varphi([(a_1 a_2, a_2 a_3, \dots, a_{2k} a_1)]) &= [(a_1 a_2, a_3 a_4, \dots, a_{2k-1} a_{2k})]. \end{aligned}$$

We note that this map just projects the original vector on its odd components. It is easy to see that φ is an homomorphism between the multiplicative groups X and \mathbb{T}_{k-1} . In fact if we take $[(a_1, a_3, \dots, a_{2k-1})] \in \mathbb{T}_{k-1}$ we define $b_{2i} = 1$ for all $i = 1, \dots, k$ and $b_{2i-1} = a_{2i-1}$ for all $i = 1, \dots, k$. Then the point $[(b_1 b_2, b_2 b_3, \dots, b_{2k} b_1)] = [(a_1, a_3, a_3, \dots, a_{2k-1}, a_{2k-1}, a_1)] \in X$ and its image under φ is $[(a_1, a_3, \dots, a_{2k-1})]$. Therefore φ is a surjective map and thus $X/\text{Ker } \varphi$ is isomorphic to \mathbb{T}_{k-1} . But

$$\text{Ker } \varphi = \{[(1, a_2 a_3, 1, a_4 a_5, 1, \dots, 1, a_{2k} a_1)] : a_i \in K^* \text{ for all } i\},$$

and then $|\text{Ker } \varphi| = (q - 1)^{k-1}$. Therefore $|X| = |\mathbb{T}_{k-1}| \cdot |\text{Ker } \varphi| = (q - 1)^{2k-2}$. \square

Remark 3.3. *The result given in Eq. (5) is an easy consequence of [11, Corollary 3.8] because even cycles are bipartite graphs. We decided to prove it with the help of the map φ because it plays a very important role in the development of this work.*

3.2.2 Dimension

In this section we will use $S = K[T_1, \dots, T_{2k}]$ and $R = K[t_1, t_3, \dots, t_{2k-1}]$ as the polynomial rings in the corresponding variables. Also I_X will be the vanishing ideal of the set X and $I_{\mathbb{T}_{k-1}}$ the corresponding vanishing ideal of the projective torus \mathbb{T}_{k-1} . Let α be the map: $\alpha : S \rightarrow R$, $\alpha(T_{2i-1}) = t_{2i-1}$ for all $i = 1, \dots, k$, $\alpha(T_{2i}) = t_{2i+1}$ for all $i = 1, \dots, k - 1$ and $\alpha(T_{2k}) = t_1$. It means that

$$\alpha : S \rightarrow R, \quad \alpha\left(\sum_{(i)} a_{(i)} T_1^{i_1} T_2^{i_2} \dots T_{2k}^{i_{2k}}\right) = \sum_{(i)} a_{(i)} t_1^{i_1+i_{2k}} t_3^{i_2+i_3} \dots t_{2k-1}^{i_{2k-2}+i_{2k-1}}. \quad (6)$$

It is immediate that α is a ring epimorphism and in fact we have the next result.

Lemma 3.4. $\alpha(I_X) = I_{\mathbb{T}_{k-1}}$.

Proof. Let f be an homogeneous polynomial in the ring S . Then

$$\alpha(f) = f(t_1, t_3, t_3, \dots, t_{2k-1}, t_{2k-1}, t_1).$$

If $[(a_1, a_3, \dots, a_{2k-1})] \in \mathbb{T}_{k-1}$ then, whenever $f \in I_X$,

$$f(a_1, a_3, a_3, \dots, a_{2k-1}, a_{2k-1}, a_1) = 0$$

because $[(a_1, a_3, a_3, \dots, a_{2k-1}, a_{2k-1}, a_1)] \in X$. Therefore

$$\alpha(f)(a_1, a_3, \dots, a_{2k-1}) = f(a_1, a_3, a_3, \dots, a_{2k-1}, a_{2k-1}, a_1) = 0.$$

Then $\alpha(f) \in I_{\mathbb{T}_{k-1}}$. It proves that $\alpha(I_X) \subseteq I_{\mathbb{T}_{k-1}}$.

By the other hand, we know that (see [6]) $I_{\mathbb{T}_{2k-1}} = (\{T_i^{q-1} - T_1^{q-1}\}_{i=2}^{2k})$ and $I_{\mathbb{T}_{k-1}} = (\{t_{2i-1}^{q-1} - t_1^{q-1}\}_{i=2}^k)$. Moreover we know that $X \subseteq \mathbb{T}_{2k-1}$ and it means that $I_{\mathbb{T}_{2k-1}} \subseteq I_X$. Then $t_{2i-1}^{q-1} - t_1^{q-1} = \alpha(T_{2i-1}^{q-1} - T_1^{q-1}) \in \alpha(I_{\mathbb{T}_{2k-1}}) \subseteq \alpha(I_X)$. Therefore $I_{\mathbb{T}_{k-1}} \subseteq \alpha(I_X)$. \square

From now on we will use the toric set

$$Y := \{[(a_1, a_3, a_3, \dots, a_{2k-1}, a_{2k-1}, a_1)] \in \mathbb{T}_{2k-1} : a_i \in K^* \text{ for all } i\}. \quad (7)$$

Lemma 3.5. *The set Y defined in (7) is a complete intersection [3], in fact,*

$$I_Y = (T_1 - T_{2k}, \{T_{2i} - T_{2i+1}\}_{i=1}^{k-1}, \{T_{2i+1}^{q-1} - T_{2k}^{q-1}\}_{i=1}^{k-1}). \quad (8)$$

Proof. We will use the lexicographic ordering $T_1 > T_2 > \dots > T_{2k}$. Let $f \in I_Y$. By using the division algorithm, f can be written as

$$f = f_1(T_1 - T_{2k}) + f_3(T_2 - T_3) + f_5(T_4 - T_5) + \dots + f_{2k-1}(T_{2k-2} - T_{2k-1}) + r,$$

where $f_i, r \in S$ for all i , and r is a K -linear combination of monomials none of which is divisible by any of $T_1, T_2, T_4, \dots, T_{2k-2}$. Then $r(T_1, \dots, T_{2k}) = r(T_3, T_5, \dots, T_{2k-1}, T_{2k})$. Let $[(a_3, a_5, \dots, a_{2k-1}, a_{2k})] \in \mathbb{T}_{k-1}$. Thus

$$[(a_{2k}, a_3, a_3, \dots, a_{2k-1}, a_{2k-1}, a_{2k})] \in Y$$

and

$$0 = f(a_{2k}, a_3, a_3, \dots, a_{2k-1}, a_{2k-1}, a_{2k}) = r(a_3, a_5, \dots, a_{2k-1}, a_{2k}).$$

Then $r \in I_{\mathbb{T}_{k-1}}$. Therefore (see [6]) $r \in (\{T_{2i+1}^{q-1} - T_{2k}^{q-1}\}_{i=1}^{k-1})$ and

$$I_Y \subseteq (T_1 - T_{2k}, \{T_{2i} - T_{2i+1}\}_{i=1}^{k-1}, \{T_{2i+1}^{q-1} - T_{2k}^{q-1}\}_{i=1}^{k-1}).$$

The inclusion \supseteq is clear and the claim follows. \square

Lemma 3.6. *The vanishing ideal of the toric set Y is given by*

$$I_Y = I_X + \text{Ker } \alpha. \quad (9)$$

Proof. The inclusion $I_Y \subseteq I_X + \text{ker } \alpha$ follows from Lemma 3.5 because $T_1 - T_{2k} \in \text{Ker } \alpha$, $\{T_{2i} - T_{2i+1}\}_{i=1}^{k-1} \subseteq \text{Ker } \alpha$ and $\{T_{2i+1}^{q-1} - T_{2k}^{q-1}\}_{i=1}^{k-1} \subseteq I_X$. Let $[(a_1, a_3, a_3, \dots, a_{2k-1}, a_{2k-1}, a_1)] \in Y$ and $f \in I_X$, $g \in \text{Ker } \alpha$. Then, because $[(a_1, a_3, a_3, \dots, a_{2k-1}, a_{2k-1}, a_1)] \in X$, we get

$$f(a_1, a_3, a_3, \dots, a_{2k-1}, a_{2k-1}, a_1) = 0.$$

Let $g(T_1, \dots, T_{2k}) = \sum_{(i)} b_{(i)} T_1^{i_1} \dots T_{2k}^{i_{2k}}$. Thus

$$\alpha(g)(t_1, t_3, \dots, t_{2k-1}) = \sum_{(i)} b_{(i)} t_1^{i_1+i_{2k}} t_3^{i_2+i_3} \dots t_{2k-1}^{i_{2k-2}+i_{2k-1}},$$

and due to the fact that $\alpha(g) = 0$ we conclude that

$$0 = \alpha(g)(a_1, a_3, \dots, a_{2k-1}) = \sum_{(i)} b_{(i)} a_1^{i_1+i_{2k}} a_3^{i_2+i_3} \dots a_{2k-1}^{i_{2k-2}+i_{2k-1}},$$

and of course $g(a_1, a_3, a_3, \dots, a_{2k-1}, a_{2k-1}, a_1) = 0$.

Therefore $f + g \in I_Y$ and the equality (9) follows. \square

Remark 3.7. *We note that $Y \subseteq X \subseteq \mathbb{T}_{2k-1}$ and then $I_{\mathbb{T}_{2k-1}} \subseteq I_X \subseteq I_Y$. Actually we have that*

$$I_X + \text{Ker } \alpha = I_Y = I_{\mathbb{T}_{2k-1}} + \text{Ker } \alpha.$$

In order to compute the dimension of the parameterized codes over an even cycle we need to introduce the map $\bar{\alpha}$.

$$\bar{\alpha} : S/I_X \rightarrow R/I_{\mathbb{T}_{k-1}}, \quad \bar{\alpha}(f + I_X) = \alpha(f) + I_{\mathbb{T}_{k-1}}. \quad (10)$$

This is a ring epimorphism and in fact we have the following result.

Lemma 3.8. $\text{Ker } \bar{\alpha} = I_Y/I_X$.

Proof. Let $f + I_X \in I_Y/I_X$. Thus (by Lemma 3.6) $f = g + h$ with $g \in I_X$, $h \in \text{Ker } \alpha$. Then $\alpha(f) = \alpha(g) + \alpha(h) = \alpha(g) \in \alpha(I_X) = I_{\mathbb{T}_{k-1}}$ (by Lemma 3.4). Therefore $f + I_X \in \text{Ker } \bar{\alpha}$.

By the other hand, let $f + I_X \in \text{Ker } \bar{\alpha}$. Then $\alpha(f) \in I_{\mathbb{T}_{k-1}} = \alpha(I_X)$. Then there exists $g \in I_X$ so that $\alpha(f) = \alpha(g)$. Thus $f - g \in \text{Ker } \alpha$, $f \in I_X + \text{Ker } \alpha = I_Y$ and the result is completely proved. \square

Now, we are able to give the main result of this section.

Theorem 3.9. *For all $d \geq 0$ the dimension of the parameterized codes arising from the edges of an even cycle C_{2k} is given by*

$$H_X(d) = H_{\bar{\alpha}}(d) + H_{\mathbb{T}_{k-1}}(d), \quad (11)$$

where $H_{\bar{\alpha}}$ is the Hilbert function of I_Y/I_X , i.e., $H_{\bar{\alpha}}(d) = \dim_K I_Y(d)/I_X(d)$.

Proof. Let $d \geq 0$. Because the map $\bar{\alpha}$ is graded, it induces the surjective linear transformation $\bar{\alpha}(d) : S_d/I_X(d) \rightarrow R_d/I_{\mathbb{T}_{k-1}}(d)$, $f + I_X(d) = \alpha(f) + I_{\mathbb{T}_{k-1}}(d)$. Then $\dim_K S_d/I_X(d) = \dim_K \text{Ker}(\bar{\alpha})(d) + \dim_K R_d/I_{\mathbb{T}_{k-1}}(d)$. But, by Lemma 3.8, $\dim_K \text{Ker}(\bar{\alpha})(d) = \dim_K I_Y(d)/I_X(d)$ and the Eq. (11) follows immediately. \square

Remark 3.10. *We note that*

$$\begin{aligned} H_{\mathbb{T}_{k-1}}(d) = H_X(d) - H_{\bar{\alpha}}(d) &= \dim_K S_d - \dim_K I_X(d) - \dim_K I_Y(d) + \\ &\dim_K I_X(d) = \dim_K S_d/I_Y(d) = H_Y(d). \end{aligned}$$

In the following corollary and the example given in section 4, we will use (see Section 2) $r_X := \text{reg}(S/I_X)$, $r_{\mathbb{T}_{k-1}} := \text{reg}(R/I_{\mathbb{T}_{k-1}})$ and $r_{\bar{\alpha}} = \text{reg}(I_Y/I_X)$.

Corollary 3.11. *With the notation used above, the index of regularity of S/I_X , where X is the toric set parameterized by the edges of an even cycle C_{2k} , is given by*

$$r_X = \max \{r_{\bar{\alpha}}, r_{\mathbb{T}_{k-1}}\}. \quad (12)$$

Proof. In order to prove Eq. (12) it suffices to show that the function $H_{\bar{\alpha}}(d)$ is non decreasing (see Eq. (11)). We define the map $\Delta : I_Y(d)/I_X(d) \rightarrow I_Y(d+1)/I_X(d+1)$, $\Delta(f + I_X(d)) = T_1 f + I_X(d+1)$. If $f + I_X(d) \in \text{Ker} \Delta$ then $T_1 f \in I_X(d+1)$. It means that $(T_1 f)(a_1 a_2, a_2 a_3, \dots, a_{2k} a_1) = 0$ for all $[(a_1 a_2, a_2 a_3, \dots, a_{2k} a_1)] \in X$. Thus

$$a_1 a_2 f(a_1 a_2, a_2 a_3, \dots, a_{2k} a_1) = 0,$$

but then $f(a_1 a_2, a_2 a_3, \dots, a_{2k} a_1) = 0$ for all $[(a_1 a_2, a_2 a_3, \dots, a_{2k} a_1)] \in X$ and $\text{Ker} \Delta = I_X(d)$. Therefore $\dim_K I_Y(d)/I_X(d) \leq \dim_K I_Y(d+1)/I_X(d+1)$ and thus $H_{\bar{\alpha}}(d) \leq H_{\bar{\alpha}}(d+1)$ for all $d \geq 0$. \square

3.2.3 Minimum distance

In this section we will use the following notation: If φ is the map defined in the proof of theorem 3.2 and $M = \text{Ker } \varphi = \{[R_1], \dots, [R_{|\mathbb{T}_{k-1}|}]\}$ we know that $X = \cup_{i=1}^{|\mathbb{T}_{k-1}|} M \cdot [P_i]$ (disjoint union of the corresponding cosets) and $|M| = (q-1)^{k-1}$.

In the same way let

$$\psi : \mathbb{T}_{2k-1} \rightarrow X, \quad \psi([(a_1, a_2, \dots, a_{2k})]) = [(a_1 a_2, a_2 a_3, \dots, a_{2k} a_1)]. \quad (13)$$

The map ψ is a group epimorphism and

$$\text{Ker}(\psi) = \{[(1, a_1, 1, a_1, \dots, 1, a_1)] : a_1 \in K^*\}.$$

Therefore if $N := \text{Ker}(\psi)$, $|N| = q-1$ and $\mathbb{T}_{2k-1} = \cup_{i=1}^{|X|} N \cdot [Q_i]$ (disjoint union of the corresponding cosets). We will use

$$N = \{[U_1], \dots, [U_{q-1}]\}.$$

Theorem 3.12. *If $\delta_X(d)$ is the minimum distance of the parameterized code of order d arising from the edges of an even cycle C_{2k} then*

$$\frac{\delta_{\mathbb{T}_{2k-1}}(2d)}{q-1} \leq \delta_X(d) \leq (q-1)^{k-1} \cdot \delta_{\mathbb{T}_{k-1}}(d), \quad (14)$$

where $\delta_{\mathbb{T}_{2k-1}}(2d)$ is the minimum distance of the parameterized code of order $2d$ associated to the projective torus \mathbb{T}_{2k-1} and $\delta_{\mathbb{T}_{k-1}}(d)$ is the minimum distance of the parameterized code of order d arising from the projective torus \mathbb{T}_{k-1} .

Proof. Let $\Lambda = (G(Q_1), \dots, G(Q_{|\mathbb{T}_{k-1}|})) \in C_{\mathbb{T}_{k-1}}(d)$ a codeword with minimum weight where $g(t_1, t_3, \dots, t_{2k-1}) = \sum_{(i)} a_{(i)} t_1^{i_1} t_3^{i_3} \dots t_{2k-1}^{i_{2k-1}} \in R_d$ and $G = g/g_0$ with $g_0(t_1, t_3, \dots, t_{2k-1}) = t_1^d$. If $G(Q_i) \neq 0$ we take $M \cdot [P_i] = \varphi^{-1}([Q_i])$. Therefore if $[Q_i] = [(b_1, b_3, \dots, b_{2k-1})]$ then, due to the fact that $\varphi([R_j] \cdot [P_i]) = [Q_i]$, we obtain that $[R_j] \cdot [P_i] = [(b_1, *, b_3, *, \dots, b_{2k-1}, *)]$. Let $f(T_1, \dots, T_{2k}) = \sum_{(i)} a_i T_1^{i_1} T_3^{i_3} \dots T_{2k-1}^{i_{2k-1}} \in S_d$. We will take $F = f/f_0$ where $f_0(T_1, \dots, T_{2k}) = T_1^d$. Thus $F(R_j \cdot P_i) = F(b_1, *, b_3, *, \dots, b_{2k-1}, *) = G(Q_i) \neq 0$ for all $j = 1, \dots, |M|$. Moreover, if we define the codeword

$$\Lambda' = (F(R_1 P_1), \dots, F(R_{|M|} P_1), \dots, F(R_1 P_{|\mathbb{T}_{k-1}|}), \dots, F(R_{|M|} P_{|\mathbb{T}_{k-1}|})),$$

we have that $\Lambda' \in C_X(d)$ and if $w(\Lambda')$ means the Hamming weight of the codeword Λ' then $w(\Lambda') = |M| \cdot w(\Lambda) = |M| \cdot \delta_{\mathbb{T}_{k-1}}(d)$ and therefore

$$\delta_X(d) \leq |M| \cdot \delta_{\mathbb{T}_{k-1}}(d) = (q-1)^{k-1} \cdot \delta_{\mathbb{T}_{k-1}}(d). \quad (15)$$

On the other hand let $\Omega = (H(P_1), \dots, H(P_{|X|})) \in C_X(d)$ a codeword with minimum weight where $h(T_1, \dots, T_{2k}) = \sum_{(i)} b_{(i)} T_1^{j_1} T_2^{j_2} \dots T_{2k}^{j_{2k}} \in S_d$ and $H = h/h_0$ where $h_0(T_1, \dots, T_{2k}) = T_1^d$. If $H(P_i) \neq 0$ then let $N \cdot [Q_i] = \psi^{-1}([P_i])$ and thus $\psi([U_j] \cdot [Q_i]) = [P_i]$ for all $j = 1, \dots, q-1$. Moreover if $[P_i] = [(a_1 a_2, a_2 a_3, \dots, a_{2k} a_1)]$ then we can take $[Q_i] = [(a_1, a_2, \dots, a_{2k})]$ and $[U_j] = [(1, c_j, 1, c_j, \dots, 1, c_j)]$. Let

$$\ell(Z_1, \dots, Z_{2k}) = h(Z_1 Z_2, Z_2 Z_3, \dots, Z_{2k} Z_1) \in K[Z_1 Z_2, \dots, Z_{2k} Z_1]_d$$

and $L = \ell/\ell_0$ where $\ell_0(Z_1, \dots, Z_{2k}) = (Z_1 Z_2)^d$. Then

$$\begin{aligned} L(U_j \cdot Q_i) &= L(a_1, c_j a_2, a_3, c_j a_4, \dots, a_{2k-1}, c_j a_{2k}) = \\ H(c_j a_1 a_2, c_j a_2 a_3, \dots, c_j a_{2k} a_1) &= H(a_1 a_2, a_2 a_3, \dots, a_{2k} a_1) = H(P_i) \neq 0 \end{aligned}$$

for all $j = 1, \dots, q-1$. Thus if we take the codeword

$$\Omega' = (L(U_1 Q_1), \dots, L(U_{q-1} Q_1), \dots, L(U_1 Q_{|X|}), \dots, L(U_{q-1} Q_{|X|})),$$

we have that $\Omega' \in C_{\mathbb{T}_{2k-1}}(2d)$ and $w(\Omega') = (q-1) \cdot w(\Omega) = (q-1) \cdot \delta_X(d)$. Then $\delta_{\mathbb{T}_{2k-1}}(2d) \leq (q-1) \cdot \delta_X(d)$. Therefore

$$\delta_X(d) \geq \frac{\delta_{\mathbb{T}_{2k-1}}(2d)}{q-1}, \quad (16)$$

and the inequalities (14) follow from (15) and (16). \square

4 An Example

We will consider the cycle C_6 (see Fig. 1) over the finite field $K = \mathbb{Z}_5$. In this case the toric set X defined in Eq. (3) becomes

$$X = \{[(a_1 a_2, a_2 a_3, a_3 a_4, a_4 a_5, a_5 a_6, a_6 a_1)] \in \mathbb{P}^5 : a_i \in K^* \text{ for all } i\}.$$

The main parameters of the parameterized code $C_X(d)$ arising from the edges of the cycle C_6 appear below.

- **Length:** $|X| = (q-1)^4 = 256$.
- **Dimension:** By using Macaulay2 [8] we obtain the Table 1. There we compute the three different Hilbert functions which appear in Theorem 3.9. Also we note that $r_X = r_{\mathbb{T}_2} = r_{\bar{\alpha}} = 6$.

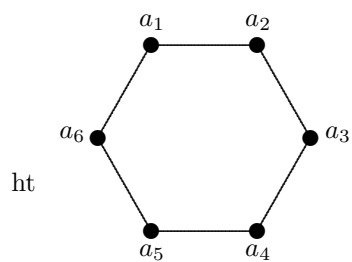
Figure 1: The cycle C_6

Table 1: Comparison of the different Hilbert functions involved in Theorem 3.9.

d	$H_X(d)$	$H_{\mathbb{T}_2}(d)$	$H_{\bar{\alpha}}(d)$
0	1	1	0
1	6	3	3
2	21	6	15
3	55	10	45
4	115	13	102
5	192	15	177
6	256	16	240

Table 2: Bounds for the minimum distance of the parameterized codes arising from the Cycle C_6 .

d	l_d	u_d	m_d
1	128	192	249
2	48	128	236
3	16	64	202
4	8	48	142
5	3	32	65
6	1	16	1

- **Minimum distance:** By using the formula to obtain the minimum distance of the parameterized codes arising from the projective torus given in [13, Theorem 3.4] we obtain the Table 2. There we can compare the upper bound for the minimum distance of the parameterized codes over the cycle C_6 obtained in this work against the Singleton bound. It shows that for $1 \leq d \leq 5$ our upper bound is sharper than the Singleton bound. Also we compute the lower bound for the studied cases. We will use $l_d = \frac{\delta_{\mathbb{T}_5}(2d)}{4}$ (lower bound), $u_d = (4)^2 \cdot \delta_{\mathbb{T}_2}(d)$ (upper bound) and m_d means the Singleton bound.

References

- [1] W. W. Adams and P. Lounstaunau, *An Introduction to Gröbner Bases* (GSM **3**, American Mathematical Society, 1994).
- [2] P. Delsarte, J. M. Goethals and F. J. MacWilliams, On generalized Reed-Muller codes and their relatives, *Information and Control* **16** (1970) 403–442.
- [3] I. M. Duursma, C. Rentería and H. Tapia-Recillas, Reed-Muller codes on complete intersections, *Appl. Algebra Engrg. Comm. Comput.* **11** (6) (2001) 455–462.
- [4] L. Gold, J. Little and H. Schenck, Cayley-Bacharach and evaluation codes on complete intersections, *J. Pure Appl. Algebra* **196** (1) (2005) 91–99.
- [5] M. González-Sarabia and C. Rentería, Evaluation codes associated to complete bipartite graphs, *Int. J. Algebra* **2** (2008) 163–170.
- [6] 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.
- [7] M. González-Sarabia, C. Rentería and H. Tapia-Recillas, Reed-Muller-type codes over the Segre variety, *Finite Fields Appl.* **8** (4) (2002) 511–518.
- [8] D. Grayson and M. Stillman, *Macaulay2* (Available via anonymous ftp from math.uiuc.edu, 1996).
- [9] J. Harris, *Algebraic Geometry. A first course* (Graduate Texts in Mathematics **133**, Springer-Verlag, New York, 1992).
- [10] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-correcting Codes* (North-Holland, 1977).

- [11] 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) 81–104.
- [12] E. Reyes, R. H. Villarreal and L. Zárate, A note on affine toric varieties, *Linear Algebra Appl.* **318** (2000) 173–179.
- [13] E. Sarmiento, M. Vaz Pinto and R. H. Villarreal, The minimum distance of parameterized codes on projective tori, *Appl. Algebra Engrg. Comm. Comput.* **22** (4) (2011) 249–264.
- [14] C.E. Shannon, The mathematical theory of communication, *Bell system technical journal* **27** (1948) 379–423, 623–656.
- [15] A. Sørensen, Projective Reed-Muller codes, *IEEE Trans. Inform. Theory* **37** (6) (1991) 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).

Manuel GONZÁLEZ SARABIA,
Departamento de Ciencias Básicas,
Unidad Profesional Interdisciplinaria en
Ingeniería y Tecnologías Avanzadas,
Instituto Politécnico Nacional,
07340, México, D.F.

Partially supported by COFAA-IPN and SNI.
Email: mgonzalezsa@ipn.mx

Joel NAVA LARA,
Departamento de Matemáticas,
Escuela Superior de Física y Matemáticas,
Instituto Politécnico Nacional,
07300, México, D.F.
Partially supported by CONACyT.
Email: josiviltj@hotmail.com

Carlos RENTERÍA MÁRQUEZ,
Departamento de Matemáticas,
Escuela Superior de Física y Matemáticas,
Instituto Politécnico Nacional,
07300, México, D.F.
Partially supported by COFAA-IPN and SNI.
Email: renteri@esfm.ipn.mx

Eliseo SARMIENTO ROSALES,
Departamento de Matemáticas,
Escuela Superior de Física y Matemáticas,
Instituto Politécnico Nacional,
07300, México, D.F.
Partially supported by SNI.
Email: esarmiento@ipn.mx

