DOI: 10.2478/auom-2019-0029
An. Şt. Univ. Ovidius Constanţa **Vol. 27(2),2019, 233–258**

VANISHING IDEALS OVER ODD CYCLES

M. Eduardo Uribe-Paczka, Eliseo Sarmiento and Carlos Rentería Márquez

Abstract

Let K be a finite field. Let X^* be a subset of the affine space K^n, which is parameterized by odd cycles. In this paper we give an explicit Gröbner basis for the vanishing ideal, $\mathbf{I}(X^*)$, of X^*. We give an explicit formula for the regularity of $\mathbf{I}(X^*)$ and finally if X^* is parameterized by an odd cycle of length k, we show that the Hilbert function of the vanishing ideal of X^* can be written as linear combination of Hilbert functions of degenerate torus.

1 Introduction

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

A *linear code* C over the alphabet $\mathbb{F}_q$ is a linear subspace of $\mathbb{F}_q^n$. The elements of C are called codewords. We call n the *length* of the code C and $\dim_{\mathbb{F}_q} C$ the *dimension* of the code C as an $\mathbb{F}_q$-vector space. The *weight of* an element $a = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ is defined as $w(a) = |\{i \mid a_i \neq 0\}|$. The *minimum distance* $\delta(C)$ of a code $C \neq 0$ is given by:

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

Key Words: Toric set, Parameterized code, Hilbert function, Vanishing Ideal, Regularity index.
2010 Mathematics Subject Classification: Primary 13P25; Secondary 14G50, 14G15, 11T71, 94B27, 94B05.
Received: 12.09.2018
Accepted: 19.10.2018

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

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

The map ev_d is well-defined, i.e., it is independent of the set of representatives that we choose for the points of $\mathbb{Y}$. The map ev_d defines a linear map of K-vector spaces. The image of S_d under ev_d, denoted by $C_{\mathbb{Y}}(d)$, is called a *projective Reed-Muller-type code* of degree d over $\mathbb{Y}$ [5, 10]. It is also called an *evaluation code* associated to $\mathbb{Y}$.

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

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

Let $P_1, \ldots, P_m$ be the points of Y, and let $S_{\leq d}$ be the K-vector space of all polynomials of S of degree at most d. The *evaluation map*

$$\mathrm{ev}_d^a\colon S_{\leq d} \longrightarrow K^{|Y|}, \qquad f \mapsto (f(P_1), \ldots, f(P_m)), \tag{2}$$

defines a linear map of K-vector spaces. The image of ev_d^a, denoted by $C_Y(d)$, defines a *linear code*. We call $C_Y(d)$ the *affine Reed-Muller-type code* of degree d on Y.

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

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

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

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

where $K^* = K \setminus \{0\}$. Following [15] we call X^* an *affine algebraic toric set* parameterized by $y^{v_1}, \ldots, y^{v_s}$. The set X^* is a multiplicative group under componentwise multiplication. Following [15] we call $C_{X^*}(d)$ a *parameterized affine code* of degree d. Parameterized affine codes are special types of affine Reed-Muller codes in the sense of [21, p. 37]. If $s = n = 1$ and $v_1 = 1$, then $X^* = \mathbb{F}_q^*$ and we obtain the classical Reed-Solomon code of degree d [20, p. 42]. Some families of evaluation codes have been studied extensively, including several variations of Reed-Muller codes [4, 5, 9, 11, 10, 18].

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, the third basic parameter is the *minimum distance*. The minimum distance of $C_{X^*}(d)$ will be denoted by δ_d. 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 $\mathbb{X}^*$ is the image of the affine space K^s under the map $K^s \to \mathbb{P}^s$, $x \mapsto [(1, x)]$, the parameters of $C_{\mathbb{X}^*}(d)$ are described in [4, Theorem 2.6.2].

In this article we focus on linear codes parameterized by the edges of a graph $\mathcal{G}$ (see Definition 2.4) which has m components and each component is an odd cycle; all our work is based on the affine space. In [16], the authors work with codes parameterized by even cycles over the projective space, they find an explicit description for a set of generators of the vanishing ideal (see Definition 1.1) associated to an even cycle. In the same article, we can also find the length of the code associated to a graph $\mathcal{G}$ with m connected components (see [16, Theorem 3.2]). In [12], the authors work with codes parameterized by odd cycles over the projective space and they prove that parameterized sets by odd cycles over the projective space are projective torus. Therefore, if we work with codes parameterized by odd cycles over the projective space, we get parameterized codes over projective torus, and these codes are very well known. There is not any paper that works with parameterized codes by odd cycles over the affine space, in contrast with [12], we are going to see that if $2 \mid q - 1$ then affine sets parameterized by odd cycles are not affine torus.

The contents of this paper are as follows. In Section 2 we introduce the preliminaries and explain the connection between the codes and graphs. In Section 3 we provide an explicit description of a set of generators from the vanishing ideal of an affine set parameterized by a graph $\mathcal{G}$ with m connected components, where each component is an odd cycle (see Theorem 3.11). The set parameterized by the edges of a graph $\mathcal{G}$ will be denoted by $X^*_{\mathcal{G}}$ (see Definition 2.4) .

Definition 1.1. (i) Let $X \subseteq K^s$. We set:

$$\mathbf{I}(X) = \{f \in S \mid f(x_1, \ldots, x_s) = 0 \ \forall x = (x_1, \ldots, x_s) \in X\}.$$

(ii) Let $\mathbb{X} \subseteq \mathbb{P}_K^{s-1}$. We set:

$$\mathbf{I}(\mathbb{X}) = \langle \{f \in S \mid f \text{ is homogeneous and } f(x) = 0 \ \forall x \in \mathbb{X}\} \rangle$$

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

For a set X^* parameterized by monomials, the main algebraic fact about $\mathbf{I}(X^*)$ that we use is a remarkable result of [15] showing that $\mathbf{I}(X^*)$ is a binomial ideal. In Section 4 we give an explicit formula for the regularity of $\mathbf{I}(X^*_{\mathcal{G}})$, where $\mathcal{G}$ is graph with m connected components and each component is an odd cycle. Finally, in Section 5, if $\mathcal{G}$ is an odd cycle of length k, we prove that the Hilbert function of $\mathbf{I}(X^*_{\mathcal{G}})$ can be written as a linear combination of Hilbert functions of degenerate torus.

For all unexplained terminology and additional information we refer to [7] (for the theory of binomial ideals), [2, 19] (for the theory of polynomial ideals and Hilbert functions).

2 Preliminaries: Codes Associated to a Graphs

We will use the notation and definitions used in the introduction. In this section, we introduce the connection between graphs and codes and we present the basic theory of Hilbert functions that we will use later.

Theorem 2.1. (Combinatorial Nullstellensatz [1, Theorem 1.2]) *Let $R = K[y_1, \ldots, y_n]$ be a polynomial ring over a field K, let $f \in R$, and let $a = (a_1, \ldots, a_n) \in \mathbb{N}^n$. Suppose that the coefficient of y^a in f is non zero and* $\deg(f) = a_1 + \cdots + a_n$. *If $S_1, \ldots, S_n$ are subsets of K, with $|S_i| > a_i$ for all i, then there are $s_1 \in S_1, \ldots, s_n \in S_n$ such that $f(s_1, \ldots, s_n) \neq 0$.*

Let $X^* \subseteq K^{s-1}$ be an affine algebraic toric set parameterized by $y^{v_1}, \ldots, y^{v_{s-1}}$. The kernel of the evaluation map ev_d, defined in Eq. (2), is $\mathbf{I}(X^*)_{\leq d}$; in other words $\mathbf{I}(X^*)_{\leq d}$ is the set of all the polynomials of degree less or equal to d that are in $\mathbf{I}(X^*)$, thus there is an isomorphism of K-vector spaces:

$$S_{\leq d}/\mathbf{I}(X^*)_{\leq d} \simeq C_{X^*}(d).$$

The *affine Hilbert function* of $\mathbf{I}(X^*)$ is given by:

$$H_{X^*}(d) = \dim_K S_{\leq d}/\mathbf{I}(X^*)_{\leq d} = \dim_K C_{X^*}(d).$$

Let $\mathbb{X} \subseteq \mathbb{P}_K^{s-1}$ be the projective closure of X^* and let $C_{\mathbb{X}}(d)$ be a projective Reed-Muller code of degree d. It is shown that the codes $C_{\mathbb{X}}(d)$ and $C_{X^*}(d)$ have the same basic parameters (see [15, Theorem 2.4]). The kernel of the evaluation map ev_d, defined in Eq. (1), is precisely $\mathbf{I}(\mathbb{X})_d$ the degree d piece of $\mathbf{I}(\mathbb{X})$. Hence there is an isomorphism of K-vector spaces

$$S_d/\mathbf{I}(\mathbb{X})_d \simeq C_{\mathbb{X}}(d).$$

Two of the basic parameters of $C_{\mathbb{X}}(d)$ can be expressed using Hilbert functions of standard graded algebras [19], as we now explain. Recall that the *Hilbert function* of $\mathbf{I}(\mathbb{X})$ is given by

$$H_{\mathbb{X}}(d) := \dim_K (S/\mathbf{I}(\mathbb{X}))_d = \dim_K\ S_d/\mathbf{I}(\mathbb{X})_d = \dim_K C_{\mathbb{X}}(d).$$

The unique polynomial $h_{\mathbb{X}}(t) = \sum_{i=0}^{k-1} c_i t^i \in \mathbb{Z}[t]$ of degree $k-1 = \dim(S/\mathbf{I}(\mathbb{X}))-1$ such that $h_{\mathbb{X}}(d) = H_{\mathbb{X}}(d)$ for $d \gg 0$ is called the *Hilbert polynomial* of $\mathbf{I}(\mathbb{X})$. The integer $c_{k-1}(k-1)!$, denoted by $\deg(S/\mathbf{I}(\mathbb{X}))$, is called the *degree* or *multiplicity* of $S/\mathbf{I}(\mathbb{X})$. In our situation $h_{\mathbb{X}}(t)$ is a non-zero constant because $S/\mathbf{I}(\mathbb{X})$ has dimension 1. Furthermore $h_{\mathbb{X}}(d) = |\mathbb{X}|$ for $d \geq |\mathbb{X}|-1$, see [13, Lecture 13]. This means that $|\mathbb{X}|$ equals the *degree* of $S/\mathbf{I}(\mathbb{X})$. Thus $H_{\mathbb{X}}(d)$ and $\deg(S/\mathbf{I}(\mathbb{X}))$ equal the dimension and the length of $C_{\mathbb{X}}(d)$ respectively. There are algebraic methods, based on elimination theory and Gröbner bases, to compute the dimension and the length of $C_{\mathbb{X}}(d)$ [17].

Definition 2.2. The *regularity index* of $S/\mathbf{I}(\mathbb{X})$, denoted by $\mathrm{reg}(S/\mathbf{I}(\mathbb{X}))$, is the least integer $p \geq 0$ such that $h_{\mathbb{X}}(d) = H_{\mathbb{X}}(d)$ for $d \geq p$.

As $S/\mathbf{I}(\mathbb{X})$ is a 1-dimensional Cohen-Macaulay graded algebra [8], the regularity index of $S/\mathbf{I}(\mathbb{X})$ is the Castelnuovo-Mumford regularity of $S/\mathbf{I}(\mathbb{X})$ [6]. By Hilbert-Serre Theorem, the Hilbert series of $S/\mathbf{I}(\mathbb{X})$ can be uniquely written as $F_{\mathbb{X}}(t) = \frac{f(t)}{1-t}$, where f is a polinomial of degree equal to the regularity of $S/\mathbf{I}(\mathbb{X})$. From the exact sequence:

$$0 \to (S/\mathbf{I}(\mathbb{X}))[-1] \stackrel{t_s}{\to} S/\mathbf{I}(\mathbb{X}) \to S/(t_s, \mathbf{I}(\mathbb{X})) \to 0,$$

we deduce $F(S/(t_s, \mathbf{I}(\mathbb{X})), t) = f(t)$, where $F(S/(t_s, \mathbf{I}(\mathbb{X})), t)$ is the Hilbert series of $S/(t_s, \mathbf{I}(\mathbb{X}))$.

Let $>$ be a monomial order on S and let $\langle 0 \rangle \neq I \subseteq S$ be an ideal. If f is a non-zero polynomial in S, we can write:

$$f = \lambda_1 t^{\alpha_1} + \cdots + \lambda_r t^{\alpha_r},$$

with $\lambda_i \in K^*$ for all i and $t^{\alpha_1} > \cdots > t^{\alpha_r}$. The *leading monomial* t^{α_1} of f is denoted by $LM(f)$ and the *leading term* $\lambda_1 LM(f)$ of f is denoted by $LT(f)$. We denote by $LT(I)$ the set of leading terms of elements of I. The *ideal of leading terms* of I is the monomial ideal of S given by:

$$\langle LT(I)\rangle.$$

Definition 2.3. Let $\langle 0\rangle \neq I \subseteq S$ be and ideal. A monomial t^a is called a *standard monomial* of S/I, with respect to $>$, if t^a is not the leading monomial of any polynomial in I, that is, $t^a \notin \langle LT(I)\rangle$. A polynomial f is called *standard* if $f \neq 0$ and f is k-linear combination of standard monomials.

The set of standard monomials, denoted by $\Delta_>(I)$, is called the *footprint* of S/I. The image of $\Delta_>(I)$, under the canonical map $S \longrightarrow S/I$, is a basis of S/I as a K-vector space. In particular If $X^* \subseteq K^{s-1}$ is an affine algebraic toric set parameterized by $y^{v_1}, \ldots, y^{v_{s-1}}$, then $H_{X^*}(d)$ is the number of standard monomials of degree less or equal to d.

The affine algebraic toric set parameterized by $y_1, \ldots, y_s$ will be denoted by T^s. We call T^s an affine torus;

$$T^s = \{(x_1, \ldots, x_s) \mid x_i \in K^*\}.$$

It is known that $\mathbf{I}(T^s) = \left\langle \{t_i^{q-1} - 1\}_{i=1}^{s} \right\rangle$. Let $X^* \subseteq K^s$ be an affine algebraic toric set parameterized by $y^{v_1}, \ldots, y^{v_s}$. By [15] we know that $\mathbf{I}(X^*)$ is generated by binomials $t^a - t^b \in S$ where $a, b \in \mathbb{N}^s$. In addition there are a few observations to be made.

- Since $X^* \subseteq T^s$, then $\mathbf{I}(T^s) \subseteq \mathbf{I}(X^*)$, hence $\{t_i^{q-1} - 1\}_{i=1}^{s} \subseteq \mathbf{I}(X^*)$.
- Let $f = t^a - t^b$ be a nonzero binomial of S. If $\gcd(t^a, t^b) \neq 1$, then we can factor the greatest common divisor t^c from both t^a and t^b to obtain $f = t^c(t^{a'} - t^{b'})$, for some $a', b' \in \mathbb{N}^s$. Since t^c never is zero on T^s, for any $c \in \mathbb{N}^s$, we deduce that $f \in \mathbf{I}(X^*)$ if and only if $t^{a'} - t^{b'} \in \mathbf{I}(X^*)$. Accordingly, when looking for binomials generators of $\mathbf{I}(X^*)$ we may restrict ourselves to those binomials $t^a - t^b$ such that t^a and t^b have no common divisors.
- Given $a = (a_1, \ldots, a_s) \in \mathbb{N}^s$, we set $|a| = a_1 + \cdots + a_s$ and $\operatorname{supp}(a) = \{i \mid a_i \neq 0\}$. Then clearly, t^a and t^b have no common divisors if and only if $\operatorname{supp}(a) \cap \operatorname{supp}(b) = \emptyset$.

Let $\mathcal{G}$ be a simple graph with vertex set $V_{\mathcal{G}} = \{v_1, \ldots, v_n\}$ and edge set $E_{\mathcal{G}} = \{e_1, \ldots, e_s\}$. For and edge $e_i = \{v_j, v_k\}$, where $v_j, v_k \in V_{\mathcal{G}}$, let $\nu_i = \mathbf{e}_j + \mathbf{e}_k \in \mathbb{N}^n$, where, for $1 \leq j \leq n$, $\mathbf{e}_j$ is the $j-$th element of the canonical basis of $\mathbb{Q}^n$.

Definition 2.4. The *affine algebraic toric set associated* to $\mathcal{G}$ is the affine toric set parameterized by the $n-$tuples $\nu_1, \ldots, \nu_s \in \mathbb{N}^n$, obtained from the edges of $\mathcal{G}$. If $X^*_{\mathcal{G}}$ is the affine parameterized toric set associated to $\mathcal{G}$ we call its associated linear code $C_{X^*_{\mathcal{G}}}(d)$ the *parameterized affine code associated* to $\mathcal{G}$ and we refer to the vanishing ideal of $X^*_{\mathcal{G}}$ as the *vanishing ideal* over $\mathcal{G}$.

If $x = (x_1, \ldots, x_n) \in (K^*)^n$ and $e_i = \{v_j, v_k\}$ is an edge of $\mathcal{G}$, we set $x^{e_i} = x^{\mathbf{e}_j + \mathbf{e}_k} = x_j x_k$, so that the structural map $\theta : (K^*)^n \to X^*_{\mathcal{G}}$ is given by $x \to (x^{e_1}, \ldots, x^{e_s})$. If $\mathcal{G}$ is a graph with m connected components, of which ϵ are non-bipartite, the length of $C_{X^*_{\mathcal{G}}}(d)$ has been determined.

Theorem 2.5. *Let $\mathcal{G}$ be a graph with m connected components, of which ϵ are non-bipartite. Suppose that $\mathcal{G}$ has n vertices. Then:*

$$o(X^*_{\mathcal{G}}) = \begin{cases} (q-1)^{n-m+\epsilon} & \text{if } 2 \nmid q-1 \\ \dfrac{(q-1)^{n-m+\epsilon}}{2^\epsilon} & \text{if } 2 \mid q-1 \end{cases}$$

Proof. It follows from [16, Lemma 3.1]. □

Corollary 2.6. *Let $\mathcal{G}$ be a graph with m connected components. Suppose that each component is a k-cycle and k is odd. Then:*

$$o(X^*_{\mathcal{G}}) = \begin{cases} (q-1)^{km} & \text{if } 2 \nmid q-1 \\ \dfrac{(q-1)^{km}}{2^m} & \text{if } 2 \mid q-1 \end{cases}$$

3 Vanishing Ideals of Odd Cycles

In this Section we give an explicit description of the vanishing ideal associated to a graph $\mathcal{G}$ with m connected components and each component is an odd cycle.

We continue to use the notation and definitions used in the introduction. Let $\mathcal{G}$ be a graph with m connected components, suppose that each component is a k-cycle with $k = 2\gamma+1$. Let $C_1^k = x_1 \cdots x_k x_1$, $C_2^k = x_{k+1} \cdots x_{2k} x_{k+1}, \ldots$, $C_{m-1}^k = x_{(m-2)k+1} \cdots x_{(m-1)k} x_{(m-2)k+1}$, $C_m^k = x_{(m-1)k+1} \cdots x_{mk} x_{(m-1)k+1}$ be the m components of $\mathcal{G}$. If $2 \nmid q-1$, then $o(X^*_{\mathcal{G}}) = (q-1)^{km}$, therefore $X^*_{\mathcal{G}}$ is an affine torus. Suppose that $2 \mid q-1$. Let:

$$F_1 = \{A \subseteq \{1,\dots,k\} \mid |A| = \gamma\},$$
$$F_2 = \{A \subseteq \{k+1,\dots,2k\} \mid |A| = \gamma\},$$
$$\vdots$$
$$F_m = \{A \subseteq \{(m-1)k+1,\dots,mk\} \mid |A| = \gamma\}.$$

Let $A_i = \{t_{\alpha_1}^{\frac{q-1}{2}} \cdots t_{\alpha_\gamma}^{\frac{q-1}{2}} - t_{w_1}^{\frac{q-1}{2}} \cdots t_{w_{\gamma+1}}^{\frac{q-1}{2}} \mid \{\alpha_1,\dots,\alpha_\gamma\} \in F_i$ and $\{w_1,\dots,w_{\gamma+1}\} = \{(i-1)k+1,\dots,ik\} - \{\alpha_1,\dots,\alpha_\gamma\}\}$. Note that $A_i \subseteq K[t_{(i-1)k+1},\dots,t_{ik}]$.

Lemma 3.1. *For each $i \in \{1,\dots,m\}$ we have that $A_i \subseteq \mathbf{I}(X_{\mathcal{G}}^*)$.*

Proof. Let $i \in \{1,\dots,m\}$ and $f \in A_i$. Let $f = t_{\alpha_1}^{\frac{q-1}{2}} \cdots t_{\alpha_\gamma}^{\frac{q-1}{2}} - t_{w_1}^{\frac{q-1}{2}} \cdots t_{w_{\gamma+1}}^{\frac{q-1}{2}}$ where $\{\alpha_1,\dots,\alpha_\gamma\} \in F_i$ and $\{w_1,\dots,w_{\gamma+1}\} = \{(i-1)k+1,\dots,ik\} - \{\alpha_1,\dots,\alpha_\gamma\}$.

Let $g = t_{(i-1)k+1}^{\frac{q-1}{2}} \cdots t_{(i-1)k+\gamma}^{\frac{q-1}{2}} - t_{(i-1)k+\gamma+1}^{\frac{q-1}{2}} \cdots t_{ik}^{\frac{q-1}{2}}$. For each $j \in \{1,\dots,\gamma\}$, let:

$$G_j(t_{(i-1)k+1},\dots,t_{ik}) = \begin{cases} 1 & \text{if } \alpha_j = (i-1)k+j \\ t_{\alpha_j}^{\frac{q-1}{2}} t_{(i-1)k+j}^{\frac{q-1}{2}} & \text{if } \alpha_j \neq (i-1)k+j \end{cases}$$

Let $h = fG_1 \cdots G_\gamma$. Let $w = (x_{(i-1)k+1}x_{(i-1)k+2},\dots,x_{ik-1}x_{ik}, x_{ik}\, x_{(i-1)k+1})$ where $x_i \in K^*$. Then we obtain:

$$h(w) = f(w)\eta = g(w),$$

where $\eta \in K^*$. Therefore:

$$g(w) = (x_{(i-1)k+1}x_{(i-1)k+2})^{\frac{q-1}{2}}(x_{(i-1)k+2}x_{(i-1)k+3})^{\frac{q-1}{2}} \cdots (x_{(i-1)k+\gamma}x_{(i-1)k+\gamma+1})^{\frac{q-1}{2}} - (x_{(i-1)k+\gamma+1}x_{(i-1)k+\gamma+2})^{\frac{q-1}{2}} \cdots (x_{ik}x_{(i-1)k+1})^{\frac{q-1}{2}}.$$

Note that $g(w) = x_{(i-1)k+1}^{\frac{q-1}{2}} x_{(i-1)k+\gamma+1}^{\frac{q-1}{2}} - x_{(i-1)k+\gamma+1}^{\frac{q-1}{2}} x_{(i-1)k+1}^{\frac{q-1}{2}}$, then $g(w) = 0$. It follows that $f(w) = 0$, therefore $f \in \mathbf{I}(X_{\mathcal{G}}^*)$. □

Proposition 3.2. *Let $f = t^a - t^b$ be a binomial in $K[t_1,\dots,t_{km}]$ with* $\operatorname{supp}(a) \cap \operatorname{supp}(b) = \emptyset$. *Then $f = g + f'$ where $g \in \mathbf{I}(T^{km})$ and $f' = t^{a'} - t^{b'}$ is a binomial such that none of its two terms is divisible by any t_i^{q-1} for all i and* $\operatorname{supp}(a') \cap \operatorname{supp}(b') = \emptyset$.

Proof. If t^a and t^b are not divisible by any t_i^{q-1} for all i, we can take $g = 0$ and $f = f'$. Then we can write f as:

$$f = m_1 t_{\alpha_1}^{a_1} \cdots t_{\alpha_n}^{a_n} - m_2 t_{w_1}^{b_1} \cdots t_{w_r}^{b_r},$$

where $t^a = m_1 t_{\alpha_1}^{a_1} \cdots t_{\alpha_n}^{a_n}$ and $t^b = m_2 t_{w_1}^{b_1} \cdots t_{w_r}^{b_r}$. m_1 and m_2 are monomials such that none of them is divisible by any t_i^{q-1} for all i. m_1 is not divisible by any t_{α_i} and $a_i \geq q-1$ for all i. m_2 is not divisible by any t_{w_j} and $b_j \geq q-1$ for all j.

By the division algorithm we can write $a_i = (q-1)q_i + r_i$ where $0 \leq r_i < q-1$ for all $i = 1, \ldots, n$. Note that $q_i > 0$ for all i. Then $m_1 t_{\alpha_1}^{a_1} \cdots t_{\alpha_n}^{a_n} = t_{\alpha_1}^{r_1} m_1 (t_{\alpha_1}^{(q-1)(q_1-1)} t_{\alpha_2}^{a_2} \cdots t_{\alpha_n}^{a_n})(t_{\alpha_1}^{q-1} - 1) + t_{\alpha_1}^{r_1} m_1 (t_{\alpha_1}^{(q-1)(q_1-1)} \cdots t_{\alpha_n}^{a_n})$. Let $m_1' = m_1 t_{\alpha_1}^{a_1} \cdots t_{\alpha_n}^{a_n}$, then:

$$m_1' = \left(\sum_{j=1}^{q_1} t_{\alpha_1}^{(q-1)(q_1-j)} \right) t_{\alpha_1}^{r_1} m_1 \ (t_{\alpha_2}^{a_2} \cdots t_{\alpha_n}^{a_n}) \ (t_{\alpha_1}^{q-1} - 1) + t_{\alpha_1}^{r_1} m_1 \ (t_{\alpha_2}^{a_2} \cdots t_{\alpha_n}^{a_n}).$$

If we do the previous analysis with the term $t_{\alpha_1}^{r_1} m_1 (t_{\alpha_2}^{a_2} \cdots t_{\alpha_n}^{a_n})$ and we continue, we get:

$$m_1' = g_1 + (t_{\alpha_1}^{r_1} t_{\alpha_2}^{r_2} \cdots t_{\alpha_n}^{r_n}) m_1,$$

where $g_1 \in \mathbf{I}(T^{km})$. Let $m_2' = m_2 t_{w_1}^{b_1} \cdots t_{w_r}^{b_r}$. By the division algorithm we can write $b_j = (q-1)q_j' + b_j'$ where $0 \leq b_j' < q-1$ for all $j = 1, \ldots, r$. Note that $q_j' > 0$ for all j. If we do with m_2' the same procedure that we did with m_1', we get:

$$m_2' = g_2 + (t_{w_1}^{b_1'} t_{w_2}^{b_2'} \cdots t_{w_r}^{b_r'}) m_2,$$

where $g_2 \in \mathbf{I}(T^{km})$. Then $f = g_1 - g_2 + (t_{\alpha_1}^{r_1} t_{\alpha_2}^{r_2} \cdots t_{\alpha_n}^{r_n}) m_1 - (t_{w_1}^{b_1'} t_{w_2}^{b_2'} \cdots t_{w_r}^{b_r'}) m_2$. Let $g = g_1 - g_2$ and $f' = (t_{\alpha_1}^{r_1} t_{\alpha_2}^{r_2} \cdots t_{\alpha_n}^{r_n}) m_1 - (t_{w_1}^{b_1'} t_{w_2}^{b_2'} \cdots t_{w_r}^{b_r'}) m_2$. □

Remark 3.3. As a consequence of the last proposition we get $f \in \mathbf{I}(X_{\mathcal{G}}^*)$ if and only if $f' \in \mathbf{I}(X_{\mathcal{G}}^*)$.

Proposition 3.4. *Let* $i \in \{1, \ldots, m\}$. *Let* $f = t^a - t^b \in K[t_{(i-1)k+1}, \ldots, t_{ik}]$ *with* $\operatorname{supp}(a) \cap \operatorname{supp}(b) = \emptyset$. *Suppose that:*

- *All the coordinates of* a *and* b *are equal to* $\frac{q-1}{2}$.
- a *and* b *have no empty support.*

- $\mathrm{supp}(a)\cup\mathrm{supp}(b)=\{(i-1)k+1,\ldots,ik\}$.

Then we obtain:

$$f\in\left\langle\left\{t_i^{q-1}-1\right\}_{i=1}^{km}\bigcup\left(\bigcup_{i=1}^{m}A_i\right)\right\rangle.$$

Proof. Let $J=\left\langle\left\{t_i^{q-1}-1\right\}_{i=1}^{km}\bigcup\left(\bigcup_{i=1}^{m}A_i\right)\right\rangle$. We can write f as:

$$f=t_{a_1}^{\frac{q-1}{2}}\cdots t_{a_n}^{\frac{q-1}{2}}-t_{b_1}^{\frac{q-1}{2}}\cdots t_{b_r}^{\frac{q-1}{2}},$$

where $t^a=t_{a_1}^{\frac{q-1}{2}}\cdots t_{a_n}^{\frac{q-1}{2}}$ and $t^b=t_{b_1}^{\frac{q-1}{2}}\cdots t_{b_r}^{\frac{q-1}{2}}$. By hypothesis we have that $\mathrm{supp}(a)\cup\mathrm{supp}(b)=\{(i-1)k+1,\ldots,ik\}$, therefore $n+r=k$. Suppose that $r>\gamma$. Let $r=\gamma+\beta$. On the other hand we have:

$$-t_{b_{\gamma+1}}^{\frac{q-1}{2}}\cdots t_{b_{\gamma+\beta}}^{\frac{q-1}{2}}[t_{b_1}^{\frac{q-1}{2}}\cdots t_{b_\gamma}^{\frac{q-1}{2}}-(t_{b_{\gamma+1}}^{\frac{q-1}{2}}\cdots t_{b_{\gamma+\beta}}^{\frac{q-1}{2}})t^a]=-t^b+t^a(t_{b_{\gamma+1}}^{q-1}\cdots t_{b_{\gamma+\beta}}^{q-1}),$$

note that $\beta+n=\gamma+1$, therefore $t_{b_1}^{\frac{q-1}{2}}\cdots t_{b_\gamma}^{\frac{q-1}{2}}-(t_{b_{\gamma+1}}^{\frac{q-1}{2}}\cdots t_{b_{\gamma+\beta}}^{\frac{q-1}{2}})t^a\in J$. We can write $m'=t^a(t_{b_{\gamma+1}}^{q-1}\cdots t_{b_{\gamma+\beta}}^{q-1})$ as $m'=t^a(t_{b_{\gamma+2}}^{q-1}\cdots t_{b_{\gamma+\beta}}^{q-1})[t_{b_{\gamma+1}}^{q-1}-1]+t^a(t_{b_{\gamma+2}}^{q-1}\cdots t_{b_{\gamma+\beta}}^{q-1})$. If we do the same with the term $t^a(t_{b_{\gamma+2}}^{q-1}\cdots t_{b_{\gamma+\beta}}^{q-1})$ and we continue, we get:

$$m'=g+t^a,$$

where $g\in\mathbf{I}(T^{km})$. Then $-t_{b_{\gamma+1}}^{\frac{q-1}{2}}\cdots t_{b_{\gamma+\beta}}^{\frac{q-1}{2}}[t_{b_1}^{\frac{q-1}{2}}\cdots t_{b_\gamma}^{\frac{q-1}{2}}-(t_{b_{\gamma+1}}^{\frac{q-1}{2}}\cdots t_{b_{\gamma+\beta}}^{\frac{q-1}{2}})t^a]=-t^b+g+t^a$, therefore $f=-t_{b_{\gamma+1}}^{\frac{q-1}{2}}\cdots t_{b_{\gamma+\beta}}^{\frac{q-1}{2}}[t_{b_1}^{\frac{q-1}{2}}\cdots t_{b_\gamma}^{\frac{q-1}{2}}-(t_{b_{\gamma+1}}^{\frac{q-1}{2}}\cdots t_{b_{\gamma+\beta}}^{\frac{q-1}{2}})t^a]-g$. It follows that $f\in J$. If $r\leq\gamma$, it is easy to see that $n>\gamma$, then we use the same proof as above. □

Lemma 3.5. *Let $f\in\mathbf{I}(X_{\mathcal{G}}^*)$, then $f(a_1^2,\ldots,a_{km}^2)=0$ for all $a=(a_1,\ldots,a_{km})\in(\mathbb{F}_q^*)^{km}$.*

Proof. Let $i\in\{0,1,\ldots,m-1\}$ and $\bar{a}=(a_{ik+1}^2,a_{ik+2}^2,\ldots,a_{k(i+1)}^2)$. Let $\alpha_j=a_{ik+j}^2$ for $j=1,\ldots,k$. Let:

$$x_{ik+2}=\alpha_1x_{ik+1}^{-1},$$

$$x_{ik+3}=\alpha_2\alpha_1^{-1}x_{ik+1},$$

$$x_{ik+4}=\alpha_3\alpha_2^{-1}\alpha_1x_{ik+1}^{-1},$$

$$\vdots$$
$$x_{ik+k} = \alpha_{k-1}\alpha_{k-2}^{-1}\cdots\alpha_1 x_{ik+1},$$

where $x_{ik+1} = a_{ik+k}a_{ik+k-1}^{-1}\cdots a_{ik+1}$. It is easy to see that $\bar{a} = (x_{ik+1}x_{ik+2}, x_{ik+2}x_{ik+3}, \ldots, x_{ik+k-1}x_{ik+k}, x_{ik+k}x_{ik+1})$. It follows that $(a_1^2,\ldots,a_{km}^2) \in X_{\mathcal{G}}^*$, then $f(a_1^2,\ldots,a_{km}^2) = 0$. □

Lemma 3.6. *Let* $i \in \{1,\ldots,m\}$ *and* $f = t^a - t^b \in \mathbf{I}(X^*_{C_i^k}) \setminus \{0\}$ *with* $\mathrm{supp}(a) \cap \mathrm{supp}(b) = \emptyset$. *Suppose that* $\deg(f)_{t_i} < q-1$ *for all* i *and* $\emptyset \neq \mathrm{supp}(a) \subsetneq \{(i-1)k+1,\ldots,ik\}$. *Then* $\mathrm{supp}(b) \neq \emptyset$.

Proof. Suppose that $\mathrm{supp}(b) = \emptyset$. Then we get that $f = t^a - 1$. Let $n = |\mathrm{supp}(a)|$. We can write f as:

$$f(t_{\alpha_1},\ldots,t_{\alpha_n}) = t_{\alpha_1}^{a_1}\cdots t_{\alpha_n}^{a_n} - 1,$$

where $t^a = t_{\alpha_1}^{a_1}\cdots t_{\alpha_n}^{a_n}$. First we will prove that $a_i = \frac{q-1}{2}$ for all i. Let $\beta \in \mathbb{F}_q^*$. By the last lemma we get that $f(\beta^2,1,\ldots,1) = (\beta^2)^{a_1} - 1 = 0$. Let $h(t_{\alpha_1}) = t_{\alpha_1}^{a_1} - 1$, Let $S = \{\alpha^2 \mid \alpha \in \mathbb{F}_q^*\}$. It is easy to see that $|S| = \frac{q-1}{2}$, then h vanishes on S. Now we are going to examine the following cases:

- Suppose that $a_1 < \frac{q-1}{2}$. By Combinatorial Nullstellensatz we get that $h = 0$ and this is a contradiction because $a_1 > 0$.
- Suppose that $a_1 > \frac{q-1}{2}$. Let $a_1 = \frac{q-1}{2} + i_1$ where $0 < i_1 < \frac{q-1}{2}$. Let $h'(t_{\alpha_1}) = t_{\alpha_1}^{i_1} - 1$, it is clear that $h' = h$ over S, then h' vanishes on S, by Combinatorial Nullstellensatz we get that $h' = 0$ and this is a contradiction.

Therefore the only possible case is when $a_1 = \frac{q-1}{2}$. In this way we can prove that $a_i = \frac{q-1}{2}$ for all i. Let $\alpha \in \mathbb{F}_q^* \setminus S$. Now we are going to examine the following cases:

1) Suppose that $(i-1)k+1 \in \mathrm{supp}(a)$. If $(i-1)k+2 \notin \mathrm{supp}(a)$, then $(\alpha,\alpha,1,\ldots,1) \in X^*_{C_i^k}$, therefore $f(\alpha,\alpha,1,\ldots,1) = (\alpha)^{\frac{q-1}{2}} - 1 = 0$ and this is a contradiction because $\alpha \notin S$. Suppose that $(i-1)k+2 \in \mathrm{supp}(a)$, if $(i-1)k+3 \notin \mathrm{supp}(a)$, then $(1,\alpha,\alpha,1,\ldots,1) \in X^*_{C_i^k}$, thus $f(1,\alpha,\alpha,1,\ldots,1) = (\alpha)^{\frac{q-1}{2}} - 1 = 0$, and this is a contradiction. If we continue, we get that $(i-1)k+1,\ldots,ik-1 \in \mathrm{supp}(a)$, then $ik \notin \mathrm{supp}(a)$ because supp(a) $\subsetneq \{(i-1)k+1,\ldots,ik\}$, then $(1,\ldots,1,\alpha,\alpha) \in X^*_{C_i^k}$, and $f(1,\ldots,1,\alpha,\alpha) = (\alpha)^{\frac{q-1}{2}} - 1 = 0$ which is a contradiction.

2) Suppose that $(i-1)k+1 \notin \mathrm{supp}(a)$. If $(i-1)k+2 \in \mathrm{supp}(a)$, then $(\alpha,\alpha,1,\ldots,1) \in X^*_{C_i^k}$, then $f(\alpha,\alpha,1,\ldots,1) = (\alpha)^{\frac{q-1}{2}} - 1 = 0$ and this is a contradiction because $\alpha \notin S$. If we continue as in case 1), we get a contradiction.

It follows that $\mathrm{supp}(b) \neq \emptyset$. $\square$

Remark 3.7. Let $i \in \{1,\ldots,m\}$ and $f = t^a - t^b \in \mathbf{I}(X^*_{C_i^k}) \setminus \{0\}$ with $\mathrm{supp}(a) \cap \mathrm{supp}(b) = \emptyset$. Suppose that $\deg(f)_{t_i} < q-1$ for all i. If $\mathrm{supp}(a) = \{(i-1)k+1,\ldots,ik\}$, then $\mathrm{supp}(b) = \emptyset$. If we follow the proof of the last lemma, we can prove that all the coordinates of a are equal to $\frac{q-1}{2}$. Therefore:

$$f = t_{(i-1)k+1}^{\frac{q-1}{2}} \cdots t_{ik}^{\frac{q-1}{2}} - 1.$$

Let $h = t_{(i-1)k+1}^{\frac{q-1}{2}} \cdots t_{ik}^{\frac{q-1}{2}}$ and $h' = t_{(i-1)k+1}^{\frac{q-1}{2}} \cdots t_{(1-1)k+\gamma}^{\frac{q-1}{2}} - t_{(i-1)k+\gamma+1}^{\frac{q-1}{2}} \cdots t_{ik}^{\frac{q-1}{2}}$. h' belongs to $J = \left\langle \left\{ t_i^{q-1} - 1 \right\}_{i=1}^{km} \cup \left(\bigcup_{i=1}^{m} A_i \right) \right\rangle$. On the other hand we have:

$$t_{(i-1)k+\gamma+1}^{\frac{q-1}{2}} \cdots t_{ik}^{\frac{q-1}{2}} h' = h - t_{(i-1)k+\gamma+1}^{q-1} \cdots t_{ik}^{q-1}.$$

Note that $t_{(i-1)k+\gamma+1}^{q-1} \cdots t_{ik}^{q-1} = t_{(i-1)k+\gamma+2}^{q-1} \cdots t_{ik}^{q-1}(t_{(i-1)k+\gamma+1}^{q-1} - 1) + t_{(i-1)k+\gamma+2}^{q-1} \cdots t_{ik}^{q-1}$. If we do the same with the term $t_{(i-1)k+\gamma+2}^{q-1} \cdots t_{ik}^{q-1}$ and we continue, we obtain:

$$t_{(i-1)k+\gamma+1}^{q-1} \cdots t_{ik}^{q-1} = g + 1,$$

where $g \in \mathbf{I}(T^{km})$. Therefore $t_{(i-1)k+\gamma+1}^{\frac{q-1}{2}} \cdots t_{ik}^{\frac{q-1}{2}} h' = h - (g+1) = f - g$, then $f = t_{(i-1)k+\gamma+1}^{\frac{q-1}{2}} \cdots\ t_{ik}^{\frac{q-1}{2}} h' + g$. It follows that $f \in J$.

Proposition 3.8. *Let $i \in \{1,\ldots,m\}$ and $f = t^a - t^b \in \mathbf{I}(X^*_{C_i^k}) \setminus \{0\}$ with $\mathrm{supp}(a) \cap \mathrm{supp}(b) = \emptyset$. Suppose that $\deg(f)_{t_i} < q-1$ for all i and $\emptyset \neq \mathrm{supp}(a) \subsetneq \{(i-1)k+1,\ldots,ik\}$. Then all the coordinates of a and b are equal to $\frac{q-1}{2}$.*

Proof. By hypothesis we have that $\mathrm{supp}(a) \neq \emptyset$, let $n = |\mathrm{supp}(a)|$. As $\mathrm{supp}(a) \subsetneq \{(i-1)k+1,\ldots,ik\}$, then $\mathrm{supp}(b) \neq \emptyset$, let $r = |\mathrm{supp}(b)|$. We can write f as:

$$f(t_{\alpha_1},\ldots,t_{\alpha_n},t_{w_1},\ldots,t_{w_r}) = t_{\alpha_1}^{a_1} \cdots t_{\alpha_n}^{a_n} - t_{w_1}^{b_1} \cdots t_{w_r}^{b_r},$$

where $t^a = t_{\alpha_1}^{a_1} \cdots t_{\alpha_n}^{a_n}$ and $t^b = t_{w_1}^{b_1} \cdots t_{\alpha_r}^{b_r}$. Let $(\beta, \mu) \in (\mathbb{F}_q^*)^2$. By Lemma 3.5 we get that $f(\beta^2, 1, \ldots, 1, \mu^2, 1, \ldots, 1) = (\beta^2)^{a_1} - (\mu^2)^{w_1} = 0$. Let $h(t_{\alpha_1}, t_{w_1}) = t_{\alpha_1}^{a_1} - t_{w_1}^{b_1}$, Let $S = \{\alpha^2 \mid \alpha \in \mathbb{F}_q^*\}$. It is easy to see that $|S| = \frac{q-1}{2}$, then h vanishes on S^2. Now we are going to examine the following cases:

- Suppose that $a_1, b_1 < \frac{q-1}{2}$. By Combinatorial Nullstellensatz we get that $h = 0$ and this is a contradiction because $a_1, b_1 > 0$.
- Suppose that $b_1 < \frac{q-1}{2}$ and $a_1 > \frac{q-1}{2}$. Let $a_1 = \frac{q-1}{2} + i_1$ where $0 < i_1 < \frac{q-1}{2}$. Let $h'(t_{\alpha_1}, t_{w_1}) = t_{\alpha_1}^{i_1} - t_{w_1}^{b_1}$, it is clear that $h' = h$ over S^2, then h' vanishes on S^2, by Combinatorial Nullstellensatz we get that $h' = 0$ and this is a contradiction. It is very similar the case $a_1 < \frac{q-1}{2}$ and $b_1 > \frac{q-1}{2}$.
- Suppose that $a_1, b_1 > \frac{q-1}{2}$. Let $a_1 = \frac{q-1}{2} + i_1$ and $b_1 = \frac{q-1}{2} + i_2$ where $0 < i_1, i_2 < \frac{q-1}{2}$. Let $h'(t_{\alpha_1}, t_{w_1}) = t_{\alpha_1}^{i_1} - t_{w_1}^{i_2}$, it is clear that $h' = h$ over S^2, then h' vanishes on S^2, by Combinatorial Nullstellensatz we get that $h' = 0$ and this is a contradiction.
- Suppose that $b_1 < \frac{q-1}{2}$ and $a_1 = \frac{q-1}{2}$. Then $h(t_{\alpha_1}, t_{w_1}) = t_{\alpha_1}^{\frac{q-1}{2}} - t_{w_1}^{b_1}$. Let $h'(t_{w_1}) = 1 - t_{w_1}^{b_1}$, it is clear that $h' = h$ over S^2, then h' vanishes on S, by Combinatorial Nullstellensatz we get that $h' = 0$ and this is a contradiction because $b_1 > 0$. It is very similar the case $0 < a_1 < \frac{q-1}{2}$ and $b_1 = \frac{q-1}{2}$.

As a result, the only possible case is when $b_1 = a_1 = \frac{q-1}{2}$. In this way we can prove that $a_i = \frac{q-1}{2}$ for all i and $b_j = \frac{q-1}{2}$ for all j. □

Proposition 3.9. *Let* $i \in \{1, \ldots, m\}$ *and* $f = t^a - t^b \in \mathbf{I}(X^*_{C_i^k}) \setminus \{0\}$ *with* $\mathrm{supp}(a) \cap \mathrm{supp}(b) = \emptyset$. *Suppose that* $\deg(f)_{t_i} < q-1$ *for all* i. *Then* $\mathrm{supp}(a) \cup \mathrm{supp}(b) = \{(i-1)k+1, \ldots, ik\}$.

Proof. As f is a nonzero polynomial then $\mathrm{supp}(a) \neq \emptyset$ or $\mathrm{supp}(b) \neq \emptyset$, Suppose that $\mathrm{supp}(a) \neq \emptyset$. If $\mathrm{supp}(a) = \{(i-1)k+1, \ldots, ik\}$, then $\mathrm{supp}(b) = \emptyset$, it is clear that $\mathrm{supp}(a) \cup \mathrm{supp}(b) = \{(i-1)k+1, \ldots, ik\}$. Suppose that $\mathrm{supp}(a) \subsetneq \{(i-1)k+1, \ldots, ik\}$, then we know that $\mathrm{supp}(b) \neq \emptyset$ and all the coordinates of a and b are equal to $\frac{q-1}{2}$. Suppose that $H = \mathrm{supp}(a) \cup \mathrm{supp}(b) \subsetneq \{(i-1)k+1, \ldots, ik\}$. Let $S = \{\beta^2 \mid \beta \in K^*\}$ and $\alpha \in K^* \setminus S$. Now we are going to examine the following cases:

1) Suppose that $(i-1)k+1 \in H$. If $(i-1)k+2 \notin H$, then $(\alpha, \alpha, 1, \ldots, 1) \in X^*_{C_i^k}$, therefore $f(\alpha, \alpha, 1, \ldots, 1) = 0$. Then we show $(\alpha)^{\frac{q-1}{2}} = 1$ and this

is a contradiction because $\alpha \notin S$. Suppose that $(i-1)k+2 \in H$, if $(i-1)k+3 \notin H$, then $(1,\alpha,\alpha,1,\ldots,1) \in X^*_{C^k_i}$, therefore $f(1,\alpha,\alpha,1,\ldots,1) = 0$, then we find $(\alpha)^{\frac{q-1}{2}} = 1$ and this is a contradiction. If we continue we get that $(i-1)k+1,\ldots,ik-1 \in H$, then $ik \notin H$ because $H \subsetneq \{(i-1)k+1,\ldots,ik\}$, then $(1,\ldots,1,\alpha,\alpha) \in X^*_{C^k_i}$, and $f(1,\ldots,1,\alpha,\alpha) = 0$ which is a contradiction.

2) Suppose that $(i-1)k+1 \notin H$. If $(i-1)k+2 \in H$, then $(\alpha,\alpha,1,\ldots,1) \in X^*_{C^k_i}$, hence $f(\alpha,\alpha,1,\ldots,1) = 0$, then we obtain $(\alpha)^{\frac{q-1}{2}} = 1$ and this is a contradiction because $\alpha \notin S$. If we continue as in case 1), we get a contradiction.

Then $H = \{(i-1)k+1,\ldots,ik\}$. The proof is very similar if we suppose that $\operatorname{supp}(b) \neq \emptyset$. □

Theorem 3.10. *Let $\mathcal{G}$ be a graph with m connected components, suppose that each component is a k-cycle with $k = 2\gamma+1$. The vanishing ideal of $X^*_{\mathcal{G}}$ is given by:*

$$\mathbf{I}(X^*_{\mathcal{G}}) = \left\langle \left\{ t_i^{q-1} - 1 \right\}_{i=1}^{km} \cup \left(\bigcup_{i=1}^{m} A_i \right) \right\rangle.$$

Proof. Let $J = \left\langle \left\{ t_i^{q-1} - 1 \right\}_{i=1}^{km} \cup \left(\bigcup_{i=1}^{m} A_i \right) \right\rangle$. By Lemma 3.1 we get that $J \subseteq \mathbf{I}(X^*_{\mathcal{G}})$. Now we will prove the other inclusion. We know that $\mathbf{I}(X^*_{\mathcal{G}})$ is generated by binomials, let $f = t^a - t^b \in \mathbf{I}(X^*_{\mathcal{G}})$ be a binomial; we can suppose that $\operatorname{supp}(a) \cap \operatorname{supp}(b) = \emptyset$. By Proposition 3.2 we can write f as:

$$f = g + f',$$

where $g \in \mathbf{I}(T^{km})$ and $f' = t^{a'} - t^{b'}$ is a binomial such that none of its terms is divisible by any t_i^{q-1} for all i and $\operatorname{supp}(a') \cap \operatorname{supp}(b') = \emptyset$. Therefore $f \in J$ if and only if $f' \in J$. We are going to prove that $f' \in J$. Let:

$$f' = t^{a'_1} \cdots t^{a'_m} - t^{b'_1} \cdots t^{b'_m},$$

where $t^{a'} = t^{a'_1} \cdots t^{a'_m}$ and $t^{b'} = t^{b'_1} \cdots t^{b'_m}$. $t^{a'_i}$ and $t^{b'_i}$ are monomials in $K[t_{(i-1)k+1},\ldots,t_{ik}]$ for all $i = 1,\ldots,m$. Let $i \in \{(i-1)k+1,\ldots,ik\}$. We can write f' as:

$$f' = (t^{a'_i} - t^{b'_i})t^{a'_1} \cdots t^{a'_{i-1}} t^{a'_{i+1}} \cdots t^{a'_m} + t^{b'_i}$$
$$[t^{a'_1} \cdots t^{a'_{i-1}} t^{a'_{i+1}} \cdots t^{a'_m} - t^{b'_1} \cdots t^{b'_{i-1}} t^{b'_{i+1}} \cdots t^{b'_m}].$$

As $f \in \mathbf{I}(X^*_{\mathcal{G}})$, it follows that $f' \in \mathbf{I}(X^*_{\mathcal{G}})$. Let $(x_{(i-1)k+1}, \ldots, x_{ik}) \in (\mathbb{F}^*_q)^k$, then $x = (1, \ldots, 1, x_{(i-1)k+1}x_{(i-1)k+2}, x_{(i-1)k+2}x_{(i-1)k+3}, \ldots, x_{ik-1}x_{ik}, x_{ik}\ x_{(i-1)k+1}\ , 1, \ldots, 1) \in X^*_{\mathcal{G}}$. Let $f_i = t^{a'_i} - t^{b'_i}$. As f' vanishes on x we get that f_i vanishes on $(x_{(i-1)k+1}x_{(i-1)k+2}, x_{(i-1)k+2}\ x_{(i-1)k+3}, \ldots, x_{ik-1}x_{ik}, x_{ik}x_{(i-1)k+1})$, then $f_i \in \mathbf{I}(X^*_{C^k_i})$. It is clear that $\operatorname{supp}(a'_i) \cap \operatorname{supp}(b'_i) = \emptyset$.

Suppose that f_i is a nonzero polynomial and $supp(a'_i) \neq \emptyset$. If $\operatorname{supp}(a'_i) = \{(i-1)k+1, \ldots, ik\}$, then $\operatorname{supp}(b'_i) = \emptyset$. From Remark 3.7 we deduce $f_i \in J$. If $\operatorname{supp}(a'_i) \subsetneq \{(i-1)k+1, \ldots, ik\}$, we know that $\operatorname{supp}(b'_i) \neq \emptyset$ and all the coordinates of a'_i and b'_i are equal to $\frac{q-1}{2}$. From Proposition 3.9 we get that $\operatorname{supp}(a'_i) \cup \operatorname{supp}(b'_i) = \{(i-1)k+1, \ldots, ik\}$ and by Proposition 3.4 we find $f_i \in J$. In any case we obtain $f_i \in J$.

On the other hand we have that:

$$f' = (t^{a'_1} - t^{b'_1})t^{a'_2} \cdots t^{a'_m} + t^{b'_1}\ [t^{a'_2} \cdots t^{a'_m} - t^{b'_2} \cdots t^{b'_m}].$$

If we do the same procedure with the binomial $t^{a'_2} \cdots t^{a'_m} - t^{b'_2} \cdots t^{b'_m}$, we prove $t^{a'_2} \cdots t^{a'_m} - t^{b'_2} \cdots t^{b'_m} = (t^{a'_2} - t^{b'_2})t^{a'_3} \cdots t^{a'_m} + t^{b'_2}\ [t^{a'_3} \cdots t^{a'_m} - t^{b'_3} \cdots t^{b'_m}]$, therefore:

$$f' = f_1 t^{a'_2} \cdots t^{a'_m} + f_2 t^{b'_1} t^{a'_3} \cdots\ t^{a'_m} + t^{b'_1} t^{b'_2} [t^{a'_3} \cdots t^{a'_m} - t^{b'_3} \cdots t^{b'_m}].$$

If we proceed like before with the binomial $t^{a'_3} \cdots t^{a'_m} - t^{b'_3} \cdots t^{b'_m}$ and we continue, we get:

$$f' = \sum_{j=1}^{m} f_j h_j,$$

where $h_j \in K[t_1, \ldots, t_{km}]$ for all j. As $f_j \in J$ for all j we show $f' \in J$. □

Let $\mathcal{G}_i$ be a graph with m_i connected components and each component is a k_i-cycle, where $1 \leq i \leq r$. Suppose that $k_i = 2\gamma_i + 1$ and $C^{k_i}_{i1} = x^i_1 \cdots x^i_{k_i} x^i_1$, $C^{k_i}_{i2} = x^i_{k_i+1} \cdots x^i_{2k_i} x^i_{k_i+1}, \ldots, C^{k_i}_{im_i} = x^i_{(m_i-1)k_i+1} \cdots x^i_{m_i k_i} x^i_{(m_i-1)k_i+1}$ are all the components of $\mathcal{G}_i$. Let $\mathcal{G} = \bigcup_{i=1}^{r} \mathcal{G}_i$. In this case we will work with the polynomial ring $K[t^1_1, \ldots, t^1_{k_1 m_1}, \ldots, t^r_1, \ldots, t^r_{k_r m_r}]$.

For each $1 \leq i \leq r$, let:

$$F_1^i = \{A \subseteq \{1, \ldots, k_i\} \mid |A| = \gamma_i\},$$
$$F_2^i = \{A \subseteq \{k_i+1, \ldots, 2k_i\} \mid |A| = \gamma_i\},$$
$$\vdots$$
$$F_{m_i}^i = \{A \subseteq \{(m_i-1)k_i+1, \ldots, m_ik_i\} \mid |A| = \gamma_i\}.$$

Let $A_j^i = \{(t_{\alpha_1}^i)^{\frac{q-1}{2}} \cdots (t_{\alpha_{\gamma_i}}^i)^{\frac{q-1}{2}} - (t_{w_1}^i)^{\frac{q-1}{2}} \cdots (t_{w_{\gamma_i+1}}^i)^{\frac{q-1}{2}} \mid \{\alpha_1, \ldots, \alpha_{\gamma_i}\} \in F_j^i$ and $\{w_1, \ldots, w_{\gamma_i+1}\} = \{(j-1)k_i+1, \ldots, jk_i\} - \{\alpha_1, \ldots, \alpha_{\gamma_i}\}\}$. Note that $\bigcup_{j=1}^{m_i} A_j^i \subseteq K[t_1^i, \ldots, t_{k_im_i}^i]$. The following theorem is a generalization of Theorem 3.10.

Theorem 3.11. *Let $\mathcal{G} = \bigcup_{i=1}^r \mathcal{G}_i$. Then the vanishing ideal of $X_{\mathcal{G}}^*$ is given by:*

$$\mathbf{I}(X_{\mathcal{G}}^*) = \left\langle \bigcup_{i=1}^{r} \{(t_j^i)^{q-1} - 1\}_{j=1}^{k_im_i} \bigcup \left(\bigcup_{i=1}^{r} \bigcup_{j=1}^{m_i} A_j^i \right) \right\rangle.$$

Proof. Let $J = \left\langle \bigcup_{i=1}^{r} \{(t_j^i)^{q-1} - 1\}_{j=1}^{k_im_i} \bigcup \left(\bigcup_{i=1}^{r} \bigcup_{j=1}^{m_i} A_j^i \right) \right\rangle$. The proof is similar to the proof of Theorem 3.10. It follows from Lemma 3.1 that $J \subseteq \mathbf{I}(X_{\mathcal{G}}^*)$. Now we will prove the other inclusion. We know that $\mathbf{I}(X_{\mathcal{G}}^*)$ is generated by binomials, let:

$$f = t^{a_1} \cdots t^{a_r} - t^{b_1} \cdots t^{b_r} \in \mathbf{I}(X_{\mathcal{G}}^*),$$

where t^{a_i} and t^{b_i} are monomials in $K[t_1^i, \ldots, t_{k_im_i}^i]$ for all i. Note that we can write f as:

$$f = (t^{a_i} - t^{b_i})t^{a_1} \cdots t^{a_{i-1}}t^{a_{i+1}} \cdots t^{a_r} + t^{b_i}[t^{a_1} \cdots t^{a_{i-1}}t^{a_{i+1}} - t^{b_1} \cdots t^{b_{i-1}}t^{b_{i+1}} \cdots t^{b_r}].$$

Let $f_i = t^{a_i} - t^{b_i}$. As $f \in \mathbf{I}(X_{\mathcal{G}}^*)$, it follows that $f_i \in \mathbf{I}(X_{\mathcal{G}_i}^*)$, from Theorem 3.10 we deduce $f_i \in J$. It is easy to see that we can write f as:

$$f = \sum_{i=1}^{r} f_ih_i,$$

where $h_i \in K[t_1^1, \ldots, t_{k_1m_1}^1, \ldots, t_1^r, \ldots, t_{k_rm_r}^r]$ for all i, therefore $f \in J$. □

4 The Regularity Of The Vanishing Ideal Of Odd Cycles

We continue with the notation and definitions used in the introduction and in the preliminaries. Let $\mathcal{G}_i$ be a graph with m_i connected components, suppose that each component is a k_i-cycle with $k_i = 2\gamma_i + 1$ and $1 \leq i \leq r$. The following proposition is easy to prove.

Proposition 4.1. *Let $\mathcal{G} = \bigcup_{i=1}^{r} \mathcal{G}_i$. Using the same notation of Theorem 3.11, let:*

$$G = \bigcup_{i=1}^{r} \{(t_j^i)^{q-1} - 1\}_{j=1}^{k_i m_i} \bigcup \left(\bigcup_{i=1}^{r} \bigcup_{j=1}^{m_i} A_j^i \right).$$

Then G is a Gröbner basis for $\mathbf{I}(X_{\mathcal{G}}^*)$ with respect to grlex order.

Theorem 4.2. *Let $\mathcal{G}$ be a graph with m connected components and each component is a k-cycle. Suppose that $k = 2\gamma + 1$ and let $S = K[t_1, \ldots, t_{km}]$, then:*

$$\operatorname{reg}(S/\mathbf{I}(X_{\mathcal{G}}^*)) = m(k+\gamma)\left(\frac{q-1}{2}\right) - km.$$

Proof. Let $\mathbb{Y}_{\mathcal{G}}^*$ be the projective closure of $X_{\mathcal{G}}^*$. We know that for each $d \geq 1$ the codes $C_{X_{\mathcal{G}}^*}(d)$ and $C_{\mathbb{Y}_{\mathcal{G}}^*}(d)$ have the same basic parameters (see [15, Theorem 2.4]). From Proposition 4.1 we know that:

$$G = \left\{ t_i^{q-1} - 1 \right\}_{i=1}^{km} \bigcup \left(\bigcup_{i=1}^{m} A_i \right),$$

is a Gröbner basis for $\mathbf{I}(X_{\mathcal{G}}^*)$. On the other hand we know that $\mathbf{I}(\mathbb{Y}_{\mathcal{G}}^*) = \mathbf{I}(X_{\mathcal{G}}^*)^h$, where $\mathbf{I}(X_{\mathcal{G}}^*)^h$ is the homogenization of $\mathbf{I}(X_{\mathcal{G}}^*)$. We are going to homogenize with respect to the variable u, since G is a Gröbner basis for $\mathbf{I}(X_{\mathcal{G}}^*)$ with respect to the grlex order, it follows that G^h is a Gröbner basis for $\mathbf{I}(X_{\mathcal{G}}^*)^h \subseteq S[u]$, where $S[u] = K[t_1, \ldots, t_{km}, u]$, regarding the order:

$$t^\delta u^a >_h t^\beta u^b \Leftrightarrow t^\delta >_{grlex} t^\beta \text{ or } t^\delta = t^\beta \text{ and } a > b,$$

where t^δ and t^β are monomials in S. Denote by R the graded ring $S[u]/\mathbf{I}(X_{\mathcal{G}}^*)^h$. Consider $u \in S[u]$, let $\overline{u} = \mathbf{I}(X_{\mathcal{G}}^*)^h + u$. $\overline{u}$ is regular on R, then we have the following exact sequence of graded $S[u]$-modules:

$$0 \to R[-1] \xrightarrow{\overline{u}} R \to R/\langle \overline{u} \rangle \to 0,$$

where $R[-1]$ is the graded $S[u]$-module obtained by a shift in the graduation, in other words $R[-1]_i = R_{i-1}$. Since $S[u]/\mathbf{I}(X^*_{\mathcal{G}})^h$ is a 1-dimensional ring, the regularity of $S[u]/\mathbf{I}(X^*_{\mathcal{G}})^h$ is the least integer r for which $H_{\mathbb{Y}^*_{\mathcal{G}}}(d)$ is equal to some constant for all $d \geq r$. From the last exact sequence we have $H_{\mathbb{Y}^*_{\mathcal{G}}}(d) - H_{\mathbb{Y}^*_{\mathcal{G}}}(d-1) = \dim_K(R/\langle \overline{u}\rangle)_d$. For $d \geq 1$, we define:

$$h_d := \dim_K(R/\langle \overline{u}\rangle)_d = H_{\mathbb{Y}^*_{\mathcal{G}}}(d) - H_{\mathbb{Y}^*_{\mathcal{G}}}(d-1).$$

First we will prove that $\operatorname{reg}(S[u]/\mathbf{I}(X^*_{\mathcal{G}})^h) \leq m(k+\gamma)\left(\frac{q-1}{2}\right) - km$. Let $\alpha = m(k+\gamma)\left(\frac{q-1}{2}\right) - km$. If we show that $h_d = 0$ for $d \geq \alpha+1$, then $H_{\mathbb{Y}^*_{\mathcal{G}}}(d-1) = H_{\mathbb{Y}^*_{\mathcal{G}}}(d)$ for $d-1 \geq \alpha$, and our result follows. Let $d \geq \alpha+1$. To show that $h_d = 0$ for $d \geq \alpha+1$, it is enough to prove that if $g \in S[u]_d$ is a monomial, then:

$$\langle \overline{u}\rangle + (\mathbf{I}(X^*_{\mathcal{G}})^h + g) = \langle \overline{u}\rangle + (\mathbf{I}(X^*_{\mathcal{G}})^h). \tag{3}$$

Let $g = t^{a_1}\cdots t^{a_m}u^{a_0} \in S[u]_d$, where t^{a_i} is a monomial in $K[t_{(i-1)k+1},\ldots, t_{ik}]$ for $i = 1,\ldots,m$. If $a_0 > 0$, it is clear that 3 follows, therefore we will suppose that $a_0 = 0$. For $i \in \{1,\ldots,m\}$, let $g_i = t^{a_1}\cdots t^{a_{i-1}}t^{a_{i+1}}\cdots t^{a_m}$.

Let $i \in \{1,\ldots,m\}$, suppose that there is $w \in \{(i-1)k+1,\ldots,ik\}$ such that $t_w^{q-1} \mid t^{a_i}$, then $t^{a_i} = t_w^{q-1}t^c$, where t^c is a monomial in $K[t_{(i-1)k+1},\ldots,t_{ik}]$. Therefore we can write g as:

$$g = t^{a_1}\cdots t^{a_{i-1}}t_w^{q-1}t^c t^{a_{i+1}}\cdots t^{a_m} = g_i t^c[t_w^{q-1} - u^{q-1}] + u^{q-1}g_i t^c,$$

it is clear that 3 follows, then we will suppose that all the coordinates of each a_i are less or equal than $q-2$. Now we will suppose that for each $i \in \{1,\ldots,m\}$, the monomial t^{a_i} is not divisible by any $LT(f)$, for all $f \in A_i^h$. Then we can write t^{a_i} as:

$$t^{a_i} = (t_{w_{i1}}^{a_{i1}}\cdots t_{w_{i\gamma+1}}^{a_{i\gamma+1}})t_{w_{i\gamma+2}}^{a_{i\gamma+2}}\cdots t_{w_{ik}}^{a_{ik}},$$

where $0 \leq a_{ij} \leq \frac{q-1}{2} - 1$ for all $(i,j) \in \{1,\ldots,m\}\times\{1,\ldots,\gamma+1\}$ and $|\{w_{i1},\ldots,w_{ik}\}| = k$. On the other hand we have that:

$$\deg(g) = \sum_{i=1}^{m}\sum_{j=1}^{\gamma+1} a_{ij} + \sum_{i=1}^{m}\sum_{j=\gamma+2}^{k} a_{ij},$$

it follows that $\deg(g) \leq m(\gamma+1)(\frac{q-1}{2}-1) + m\gamma(q-2)$, therefore:

$$\alpha+1=m(k+\gamma)\left(\frac{q-1}{2}\right)-km+1\leq m(\gamma+1)\left(\frac{q-1}{2}-1\right)+m\gamma(q-2),$$

we deduce that:

$$\begin{aligned} mk\left(\frac{q-1}{2}\right)-km+1 &\leq m\left(\frac{q-1}{2}\right)-m(\gamma+1)+m\gamma(q-2),\\ m\left(\frac{q-1}{2}\right)(k-1)+1 &\leq m[k-(\gamma+1)]+m\gamma(q-2),\\ m\gamma(q-1)+1 &\leq m\gamma+m\gamma(q-2),\\ m\gamma(q-1)+1 &\leq m\gamma(q-1),\\ 1 &\leq 0, \end{aligned}$$

this is a contradiction, therefore there is $i\in\{1,\dots,m\}$ such that t^{a_i} is divisible by $LT(f)$ for some $f=t_{\alpha_1}^{\frac{q-1}{2}}\cdots t_{\alpha_\gamma}^{\frac{q-1}{2}}u^{\frac{q-1}{2}}-t_{w_1}^{\frac{q-1}{2}}\cdots t_{w_{\gamma+1}}^{\frac{q-1}{2}}\in A_i^h$. Then $t^{a_i}=(t_{w_1}^{\frac{q-1}{2}}\cdots t_{w_{\gamma+1}}^{\frac{q-1}{2}})t^c$, where t^c is a monomial in $K[t_{(i-1)k+1},\dots,t_{ik}]$ and all the coordinates of c are between 0 and $q-2$. We can write g as:

$$g=-g_it^cf+g_it^c(t_{\alpha_1}^{\frac{q-1}{2}}\cdots t_{\alpha_\gamma}^{\frac{q-1}{2}}u^{\frac{q-1}{2}}),$$

then we show 3 follows, thus we have proved that $\operatorname{reg}(S[u]/\mathbf{I}(X_{\mathcal{G}}^*)^h)\leq\alpha$.

Now we will show that $\alpha\leq\operatorname{reg}(S[u]/\mathbf{I}(X_{\mathcal{G}}^*)^h)$. If we show that $h_d>0$ for $d=\alpha$, then $H_{\mathbb{Y}_{\mathcal{G}}^*}(d-1)<H_{\mathbb{Y}_{\mathcal{G}}^*}(d)$, for $d=\alpha$, and our result follows. It suffices to find a monomial $M\in S[u]_d$ such that:

$$\langle\overline{u}\rangle+(\mathbf{I}(X_{\mathcal{G}}^*)^h+M)\neq\langle\overline{u}\rangle+(\mathbf{I}(X_{\mathcal{G}}^*)^h). \tag{4}$$

For $i\in\{1,\dots,m\}$, let $M_i=t_{(i-1)k+1}^{q-2}\cdots t_{(i-1)k+\gamma}^{q-2}t_{(i-1)k+\gamma+1}^{\frac{q-1}{2}-1}\cdots t_{ik}^{\frac{q-1}{2}-1}$. Note that $\deg(M_i)=(k+\gamma)(\frac{q-1}{2})-k$ and M_i is not divisible by any $LT(f)$ for all $f\in G_i^h$, where $G_i=\{t_j^{q-1}-1\}_{j=(i-1)k+1}^{ik}\cup A_i$. Let:

$$M=\prod_{i=1}^{m}M_i.$$

It is clear that $M\in S[u]_d$. Suppose that:

$$\langle\overline{u}\rangle+(\mathbf{I}(X_{\mathcal{G}}^*)^h+M)=\langle\overline{u}\rangle+(\mathbf{I}(X_{\mathcal{G}}^*)^h),$$

then we get that $\mathbf{I}(X_{\mathcal{G}}^*)^h+M\in\langle\overline{u}\rangle$, therefore $\mathbf{I}(X_{\mathcal{G}}^*)^h+M=\mathbf{I}(X_{\mathcal{G}}^*)^h+\tilde{g}u$, where $\tilde{g}\in S[u]$, thus we deduce that $M-\tilde{g}u\in\mathbf{I}(X_{\mathcal{G}}^*)^h$, then we can write M as:

$$M = g' + \tilde{g}u,$$

where $g' \in \mathbf{I}(X^*_{\mathcal{G}})^h$, making $u = 0$ in the previous equation we obtain:

$$M \in \big\langle \{LT(f) \mid f \in G^h\} \big\rangle,$$

it follows that M is divisible by $LT(f)$ for some $f \in G^h$, and this is a contradiction, thus 4 follows. □

Theorem 4.3. *Let $\mathcal{G}_i$ be a graph with m_i connected components, suppose that each component is a k_i-cycle with $k_i = 2\gamma_i+1$ and $1 \leq i \leq l$. We will work with the polynomial ring $\tilde{S} = K[t^1_1, \ldots, t^1_{k_1 m_1}, \ldots, t^l_1, \ldots, t^l_{k_l m_l}]$. Let $\mathcal{G} = \bigcup_{i=1}^{l} \mathcal{G}_i$, then:*

$$\operatorname{reg}(\tilde{S}/\mathbf{I}(X^*_{\mathcal{G}})) = \sum_{i=1}^{l} m_i(k_i + \gamma_i)\left(\frac{q-1}{2}\right) - k_i m_i.$$

Proof. We will proceed by induction on l. If $l = 1$ there is nothing else to do. We are going to suppose that our result follows for $l = r$ and we will prove the formula for $l = r + 1$. Let $\mathcal{G}' = \bigcup_{i=1}^{r} \mathcal{G}_i$ and $\mathbb{Y}'$ be the projective closure of $X^*_{\mathcal{G}'}$. Let $S' = K[t^1_1, \ldots, t^1_{k_1 m_1}, \ldots, t^r_1, \ldots, t^r_{k_r m_r}]$, in the projective space we will work with the ring $S'[u]$. We know that the the Hilbert series of $S'[u]/\mathbf{I}(\mathbb{Y}')$ is given by:

$$F_{\mathbb{Y}'}(t) = \frac{f(t)}{1-t},$$

where $\deg(f) = \operatorname{reg}(S'[u]/\mathbf{I}(\mathbb{Y}'))$ and $F(S'[u]/(u, \mathbf{I}(\mathbb{Y}')), t) = f(t)$. Let $\mathbb{Y}''$ be the projective closure of $X^*_{\mathcal{G}_{r+1}}$ and $S'' = K[t^{r+1}_1, \ldots, t^{r+1}_{k_{r+1} m_{r+1}}]$. We know that the Hilbert series of $S''[u]/\mathbf{I}(\mathbb{Y}'')$ is given by:

$$F_{\mathbb{Y}''}(t) = \frac{g(t)}{1-t},$$

where $\deg(g) = \operatorname{reg}(S''[u]/\mathbf{I}(\mathbb{Y}''))$ and $F(S''[u]/(u, \mathbf{I}(\mathbb{Y}'')), t) = g(t)$. According to [22, Proposition 2.2.20, p.42], we have an isomorphism:

$$S'[u]/(u, \mathbf{I}(\mathbb{Y}')) \otimes_K S''[u]/(u, \mathbf{I}(\mathbb{Y}'')) \cong S[u]/(u, \mathbf{I}(\mathbb{Y})),$$

where $S = K[t^1_1, \ldots, t^1_{k_1 m_1}, \ldots, t^{r+1}_1, \ldots, t^{r+1}_{k_{r+1} m_{r+1}}]$ and $\mathbb{Y}$ is the projective closure of $X^*_{\mathcal{G}}$ with $\mathcal{G} = \bigcup_{i=1}^{r+1} \mathcal{G}_i$. On the other hand we have that $F(S'[u]/(u, \mathbf{I}(\mathbb{Y}')) \otimes_K S''[u]/(u, \mathbf{I}(\mathbb{Y}'')), t) = F(S[u]/(u, \mathbf{I}(\mathbb{Y})), t)$, thus:

$$F(S[u]/(u, \mathbf{I}(\mathbb{Y})), t) = F(S'[u]/(u, \mathbf{I}(\mathbb{Y}')), t)F(S''[u]/(u, \mathbf{I}(\mathbb{Y}'')), t),$$

(see [22, p.102]) therefore $F(S[u]/(u,\mathbf{I}(\mathbb{Y})),t) = f(f)g(t)$, it follows that $\mathrm{reg}(S[u]/\mathbf{I}(\mathbb{Y})) = \mathrm{reg}(S'[u]/\mathbf{I}(\mathbb{Y}')) + \mathrm{reg}(S''[u]/\mathbf{I}(\mathbb{Y}''))$. If we apply inductive hypothesis, our result follows. □

5 Dimension Of Parameterized affine Codes by Odd Cycles

Let $\mathcal{G}$ be a k-cycle and $S = K[t_1,\ldots,t_k]$, suppose that $k = 2\gamma+1$. Let $F = \{A \subseteq \{1,\ldots,k\} \mid |A| = \gamma\}$ and $d \geq 1$. For $H = \{h_1,\ldots,h_\gamma\} \in F$, let:

$$A_H(d) = \{t_{h_1}^{a_{h_1}} \cdots t_{h_\gamma}^{a_{h_\gamma}} t_{w_1}^{a_{w_1}} \cdots t_{w_{\gamma+1}}^{a_{w_{\gamma+1}}} \mid \{w_1,\ldots,w_{\gamma+1}\} = \{1,\ldots,k\} - H,$$
$$a_{h_i} < q-1 \text{ for all } i,\ a_{w_j} < \tfrac{q-1}{2} \text{ for all } j \text{ and } \textstyle\sum_{i=1}^{\gamma} a_{h_i} + \sum_{j=1}^{\gamma+1} a_{w_j} \leq d\}.$$

Let $r = |F| = \binom{k}{\gamma}$ and $F = \{H_1,\ldots,H_r\}$. The Hilbert function of $\mathbf{I}(X_{\mathcal{G}}^*)$ can be obtained from the following result.

Theorem 5.1. *Let $\mathcal{G}$ be a k-cycle and $S = K[t_1,\ldots,t_k]$, suppose that $k = 2\gamma+1$. Using the above notation, we have that:*

$$H_{X_{\mathcal{G}}^*}(d) = \left|\bigcup_{i=1}^{r} A_{H_i}(d)\right|.$$

Proof. Let $A = \{t_{w_1}^{\frac{q-1}{2}} \cdots t_{w_{\gamma+1}}^{\frac{q-1}{2}} - t_{\alpha_1}^{\frac{q-1}{2}} \cdots t_{\alpha_\gamma}^{\frac{q-1}{2}} \mid \{\alpha_1,\ldots,\alpha_\gamma\} \in F$ and $\{w_1,\ldots, w_{\gamma+1}\} = \{1,\ldots,k\} \setminus \{\alpha_1,\ldots,\alpha_\gamma\}\}$. We know that the vanishing ideal of $X_{\mathcal{G}}^*$ is given by:

$$\mathbf{I}(X_{\mathcal{G}}^*) = \left\langle \{t_i^{q-1}-1\}_{i=1}^{k} \cup A \right\rangle.$$

Let $G = \{t_i^{q-1}-1\}_{i=1}^{k} \cup A$, by Proposition 4.1, G is a Gröbner basis for $\mathbf{I}(X_{\mathcal{G}}^*)$ with respect to grlex order. Let $d \geq 1$, we know that $H_{X_{\mathcal{G}}^*}(d)$ is the number of standard monomials of degree less or equal to d. Let:

$$\Delta_{\mathbf{I}(X_{\mathcal{G}}^*)}(d) = \{m \in \Delta_{>_{grlex}}(\mathbf{I}(X_{\mathcal{G}}^*)) \mid \deg(m) \leq d\},$$

we are going to prove that:

$$\Delta_{\mathbf{I}(X_{\mathcal{G}}^*)}(d) = \bigcup_{i=1}^{r} A_{H_i}(d).$$

Let $m \in \Delta_{\mathbf{I}(X^*_{\mathcal{G}})}(d)$, then $m \in \Delta_{>_{grlex}}(\mathbf{I}(X^*_{\mathcal{G}}))$ and $\deg(m) \leq d$. As $m \in \Delta_{>_{grlex}}(\mathbf{I}(X^*_{\mathcal{G}}))$, it follows that $m \notin \langle LT(\mathbf{I}(X^*_{\mathcal{G}}))\rangle$. On the other hand G is a Gröbner basis, then m is not divisible by any leader monomial of any element of G. Therefore, there is $H = \{\alpha_1, \dots, \alpha_\gamma\} \in F$ such that:

$$m = t_{\alpha_1}^{a_{\alpha_1}} \cdots t_{\alpha_\gamma}^{a_{\alpha_\gamma}} t_{w_1}^{a_{w_1}} \cdots t_{w_{\gamma+1}}^{a_{w_{\gamma+1}}},$$

where $\{w_1, \dots, w_{\gamma+1}\} = \{1, \dots, k\} \setminus H$, $a_{\alpha_i} < q-1$ for all i and $a_{w_j} < \frac{q-1}{2}$ for all j. It follows that $m \in A_H(d)$, thus:

$$\Delta_{\mathbf{I}(X^*_{\mathcal{G}})}(d) \subseteq \bigcup_{i=1}^{r} A_{H_i}(d).$$

The other inclusion is clear. □

For $d \geq 1$ we define the following sets:

$A_\gamma(d) = \{t_1^{a_1} \cdots t_\gamma^{a_\gamma} t_{\gamma+1}^{a_{\gamma+1}} \cdots t_k^{a_k} \mid 0 \leq a_i < q-1$ for all $i = 1, \dots, \gamma$, $0 \leq a_j < \frac{q-1}{2}$ for all $j = \gamma+1, \dots, k$ and $\sum_{i=1}^k a_i \leq d\}$,

$A_{\gamma-1}(d) = \{t_1^{a_1} \cdots t_{\gamma-1}^{a_{\gamma-1}} t_\gamma^{a_\gamma} \cdots t_k^{a_k} \mid 0 \leq a_i < q-1$ for all $i = 1, \dots, \gamma-1$, $0 \leq a_j < \frac{q-1}{2}$ for all $j = \gamma, \dots, k$ and $\sum_{i=1}^k a_i \leq d\}$,

$$\vdots$$

$A_1(d) = \{t_1^{a_1} t_2^{a_2} \cdots t_k^{a_k} \mid 0 \leq a_1 < q-1$, $0 \leq a_j < \frac{q-1}{2}$ for all $j = 2, \dots, k$ and $\sum_{i=1}^k a_i \leq d\}$,

$A_0(d) = \{t_1^{a_1} \cdots t_k^{a_k} \mid 0 \leq a_i < \frac{q-1}{2}$ for all $i = 1, \dots, k$ and $\sum_{i=1}^k a_i \leq d\}$.

Remark 5.2. Let $1 \leq l \leq r$ and $1 \leq i_1 < \cdots < i_l \leq r$. It is easy to see that:

$$\left| A_{H_{i_1}}(d) \cap \cdots \cap A_{H_{i_l}}(d) \right| \in \{|A_\gamma(d)|, \dots, |A_1(d)|, |A_0(d)|\}.$$

Therefore if we use Theorem 5.1, we can write $H_{X^*_{\mathcal{G}}}(d)$ as:

$$H_{X^*_{\mathcal{G}}}(d) = \beta_0 |A_0(d)| + \beta_1 |A_1(d)| + \cdots + \beta_\gamma |A_\gamma(d)|,$$

where $\beta_0, \dots, \beta_\gamma$ are integers independent of d and q.

Proposition 5.3. *Let $0 < i \leq \gamma$ and $S = K[t_1, \dots, t_k]$. Let $X^*_i = \{(x_1, \dots, x_i, x^2_{i+1}, \dots, x^2_k) \mid x_j \in K^*$ for all $j\}$ and $X^*_0 = \{(x^2_1, \dots, x^2_k) \mid x_i \in K^*$ for all $i\}$. Then:*

(i) $H_{X_i^*}(d) = |A_i(d)|$.

(ii) $H_{X_0^*}(d) = |A_0(d)|$.

Proof. We are going to prove (i). First, we are going to prove that:

$$\mathbf{I}(X_i^*) = \left\langle t_1^{q-1} - 1, \ldots, t_i^{q-1} - 1, t_{i+1}^{\frac{q-1}{2}} - 1, \ldots, t_k^{\frac{q-1}{2}} - 1 \right\rangle.$$

Let $>_{grlex}$ be the grlex order on S and let $f \in \mathbf{I}(X_i^*)$. By the division algorithm (see [3, Theorem 3,p. 64]) we can write f as:

$$f = \sum_{j=1}^{i} h_j(t_j^{q-1} - 1) + \sum_{j=i+1}^{k} h_j(t_j^{\frac{q-1}{2}} - 1) + G(t_1, \ldots, t_k),$$

where $h_j \in S$ for all j and none term of G is divisible by any $t_1^{q-1}, \ldots, t_i^{q-1}, t_{i+1}^{\frac{q-1}{2}}, \ldots, t_k^{\frac{q-1}{2}}$. By Combinatorial-Nullstellensatz, taking $S_j = K^*$ for all $j = 1, \ldots, i$ and $S_j = \{a^2 \mid a \in K^*\}$ for all $j = i+1, \ldots, k$, we obtain $G = 0$. Therefore:

$$\mathbf{I}(X_i^*) \subseteq \left\langle t_1^{q-1} - 1, \ldots, t_i^{q-1} - 1, t_{i+1}^{\frac{q-1}{2}} - 1, \ldots, t_k^{\frac{q-1}{2}} - 1 \right\rangle.$$

The other inclusion is clear. Let $G = \{t_1^{q-1} - 1, \ldots, t_i^{q-1} - 1, t_{i+1}^{\frac{q-1}{2}} - 1, \ldots, t_k^{\frac{q-1}{2}} - 1\}$, by [3, Theorem 6,p. 85], it follows that G is a Gröbner basis for $\mathbf{I}(X_i^*)$ with respect to grlex order. For $d \geq 1$ we know that $H_{X_i^*}(d)$ is the number of standard monomials of degree less or equal to d, thus (i) follows. The proof of (ii) is similar. □

The sets $X_0^*, \ldots, X_\gamma^*$ in Proposition 5.3 are degenerate torus (see [14, Section 4]). From Remark 5.2 and Proposition 5.3 we get that the Hilbert function of $\mathbf{I}(X_\mathcal{G}^*)$ can be written as:

$$H_{X_\mathcal{G}^*}(d) = \beta_0 H_{X_0^*}(d) + \cdots + \beta_\gamma H_{X_\gamma^*}(d),$$

where $\beta_0, \ldots, \beta_\gamma$ are integers independent of d and q. In other words, we can write $H_{X_\mathcal{G}^*}(d)$ as linear combination of Hilbert functions of degenerate torus. For each $i \in \{0, \ldots, \gamma\}$ we can find an explicit formula for $H_{X_i^*}(d)$ in [14, Section 4]; therefore if we want to find an explicit formula for $H_{X_\mathcal{G}^*}(d)$, we just need to find the values of $\beta_0, \ldots, \beta_\gamma$.

Example 5.4. Let $K = \mathbb{F}_5$ and $S = K[t_1, t_2, t_3, t_4, t_5]$. Let:

$$X_\mathcal{G}^* = \{(x_1x_2, x_2x_3, x_3x_4, x_4x_5, x_5x_1) \mid x_i \in \mathbb{F}_5^*\}.$$

Let X_0^*, X_1^*, X_2^* be the sets defined in Proposition 5.3. Using Macaulay 2.0, we obtain:

d	$H_{X_2^*}(d)$	$H_{X_1^*}(d)$	$H_{X_0^*}(d)$	$H_{X_9^*}(d)$
1	6	6	6	6
2	18	17	16	21
9	128	64	32	512

Note that $\operatorname{reg}(S/\mathbf{I}(X_9^*)) = 9$. Then we have the following system of equations:

$$6 = 6\beta_2 + 6\beta_1 + 6\beta_0$$
$$21 = 18\beta_2 + 17\beta_1 + 16\beta_0$$
$$512 = 128\beta_2 + 64\beta_1 + 32\beta_0$$

Resolving the previous system, we obtain $\beta_2 = 10$, $\beta_1 = -15$ and $\beta_0 = 6$. Using Macaulay 2.0 we can verify that for $d \geq 1$ it follows the following equality:

$$H_{X_9^*}(d) = 10H_{X_2^*}(d) - 15H_{X_1^*}(d) + 6H_{X_0^*}(d).$$

If we change the field K, then the last equality will remain true.

References

[1] N. Alon, Combinatorial Nullstellensatz, Recent trends in combinatorics (Mátraháza, 1995), *Combin. Probab. Comput.* **8** (1999), no. 1-2, 7–29.

[2] W. W. Adams and P. Loustaunau, *An Introduction to Gröbner Bases*, GSM **3**, American Mathematical Society, 1994.

[3] D. Cox, J. Little and D. O'Shea, *Ideals, Varieties, and Algorithms*, Springer-Verlag, 1992.

[4] P. Delsarte, J. M. Goethals and F. J. MacWilliams, On generalized Reed-Muller codes and their relatives, *Information and Control* **16** (1970), 403–442.

[5] 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.

[6] 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.

[7] D. Eisenbud and B. Sturmfels, Binomial ideals, *Duke Math. J.* **84** (1996), 1–45.

[8] A. V. Geramita, M. Kreuzer and L. Robbiano, Cayley-Bacharach schemesand their canonical modules, *Trans. Amer. Math. Soc.* **339** (1993), no. 1, 163-189.

[9] 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.

[10] 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.

[11] M. González-Sarabia and C. Rentería, Evaluation codes associated to complete bipartite graphs, *Int. J. Algebra* **2** (2008), no. 1-4, 163–170.

[12] M. González-Sarabia, J. Nava, C. Rentería and E. Sarmiento, Parameterized codes over cycles, *An. St. Univ. Ovidius Constanta* **21** (2013), no. 3, 241–255.

[13] J. Harris, *Algebraic Geometry. A first course*, Graduate Texts in Mathematics **133**, Springer-Verlag, New York, 1992.

[14] H. H. López, C. Rentería and R. H. Villarreal, Affine cartesian codes, Des. Codes Cryptography. **71** (2014), no. 1, 5–19.

[15] H. H. López, E. Sarmiento, M. Vaz Pinto and R. H. Villarreal, Parameterized affine codes, *Studia Sci. Math. Hungar.* **49** (2012), no. 3, 406–418.

[16] J. Neves, M. Vaz Pinto and R. H. Villarreal, Vanishing ideals over graphs and even cycles, *Comm. Algebra* **43** (2015), no. 3, 1050–1075.

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

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

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

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

[22] R. H. Villarreal, *Monomial Algebras*, Monographs and Textbooks in Pure and Applied Mathematics **238**, Marcel Dekker, New York, 2001.

M. Eduardo Uribe-Paczka,
Department of Mathematics,
Escuela Superior de Física y Matemáticas,
Instituto Politécnico Nacional, 07300 Mexico City.
Email: muribep1700@alumno.ipn.mx

Eliseo Sarmiento,
Department of Mathematics,
Escuela Superior de Física y Matemáticas,
Instituto Politécnico Nacional, 07300 Mexico City.
Email:eliseo@esfm.ipn.mx

Carlos Rentería Márquez,
Department of Mathematics,
Escuela Superior de Física y Matemáticas,
Instituto Politécnico Nacional, 07300 Mexico City.
Email:renteri@esfm.ipn.mx