Finite Fields and Their Applications 17 (2011) 81–104

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Algebraic methods for parameterized codes and invariants of vanishing ideals over finite fields ☆

Carlos Rentería-Márquez [a], Aron Simis [b], Rafael H. Villarreal [c,*]

[a] Departamento de Matemáticas, Escuela Superior de Física y Matemáticas, Instituto Politécnico Nacional, 07300 Mexico City, D.F., Mexico
[b] Departamento de Matemática, Universidade Federal de Pernambuco, 50740-540 Recife, Pe, Brazil
[c] Departamento de Matemáticas, Centro de Investigación y de Estudios Avanzados del IPN, Apartado Postal 14-740, 07000 Mexico City, D.F., Mexico

ARTICLE INFO

Article history:
Received 20 October 2009
Revised 26 July 2010
Accepted 24 September 2010
Available online 6 October 2010
Communicated by W. Cary Huffman

MSC:
primary 13P25
secondary 14G50, 14G15, 11T71, 94B27, 94B05

Keywords:
Evaluation codes
Parameterized codes
Binomial and lattice ideals
Parameters of a code
Gröbner bases
Projective variety
Degree
Index of regularity
Hilbert function
Minimum distance

ABSTRACT

Let $K = \mathbb{F}_q$ be a finite field with q elements and let X be a subset of a projective space $\mathbb{P}^{s-1}$, over the field K, parameterized by Laurent monomials. Let $I(X)$ be the vanishing ideal of X. Some of the main contributions of this paper are in determining the structure of $I(X)$ to compute some of its invariants. It is shown that $I(X)$ is a lattice ideal. We introduce the notion of a parameterized code arising from X and present algebraic methods to compute and study its dimension, length and minimum distance. For a parameterized code, arising from a connected graph, we are able to compute its length and to make our results more precise. If the graph is non-bipartite, we show an upper bound for the minimum distance.

☆ The first author was partially supported by COFAA-IPN and SNI. The second author was partially supported by a grant of CNPq. The third author was partially supported by CONACyT grant 49251-F and SNI.

* Corresponding author.
E-mail addresses: renteri@esfm.ipn.mx (C. Rentería-Márquez), aron@dmat.ufpe.br (A. Simis), vila@math.cinvestav.mx (R.H. Villarreal).

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2010.09.007

1. Introduction

Let $K = \mathbb{F}_q$ be a finite field with q elements and let $y^{v_1}, \ldots, y^{v_s}$ be a finite set of Laurent monomials. Given $v_i = (v_{i1}, \ldots, v_{in}) \in \mathbb{Z}^n$, we set

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

where $y_1, \ldots, y_n$ are the indeterminates of a ring of Laurent polynomials with coefficients in K.

An object of study here is the following set parameterized by these monomials

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

where $K^* = K \setminus \{0\}$ and $\mathbb{P}^{s-1}$ is a projective space over the field K. Following [27] we call X an *algebraic toric set* parameterized by $y^{v_1}, \ldots, y^{v_s}$. We are especially interested in measuring the size of X, in terms of q, n and s, because $|X|$ is the length of the linear codes that we will introduce and examine here.

Let $S = K[t_1, \ldots, t_s] = \bigoplus_{d=0}^{\infty} S_d$ be a polynomial ring over the field K with the standard grading. Another object of study is the graded ideal $I(X) \subset S$ generated by the homogeneous polynomials of S that vanish on X. The ideal $I(X)$ is called the *vanishing ideal* of X.

Some of the main contributions of this paper are in determining the structure of $I(X)$ to compute some of its invariants. The other main contributions are estimates (in certain cases formulas) of the basic parameters of certain linear codes.

The main application we foresee is to algebraic coding theory because our results can be used to study the performance of a new class of evaluation codes that we now introduce. Let $[P_1], \ldots, [P_m]$ be the points of X and let $f_0(t_1, \ldots, t_s) = t_1^d$. The *evaluation map*

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

defines a linear map of K-vector spaces. The image of ev_d, denoted by $C_X(d)$, defines a *linear code* that we call a *parameterized code* of order d. By a *linear code* we mean a linear subspace of $K^{|X|}$. The kernel of ev_d is the homogeneous part $I(X)_d$ of degree d of $I(X)$. Therefore there is an isomorphism of K-vector spaces

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

The *dimension* and the *length* of $C_X(d)$ are given by $\dim_K C_X(d)$ and $|X|$ respectively. We will provide algebraic methods to compute and study the dimension and the length of $C_X(d)$, which are two of the basic parameters of a linear code. A third basic parameter is the *minimum distance* of $C_X(d)$, which is given by $\delta_d = \min\{\|v\| \colon 0 \neq v \in C_X(d)\}$, where $\|v\|$ is the number of non-zero entries of v. The basic parameters of $C_X(d)$ are related by the Singleton bound for the minimum distance:

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

A good parameterized code should have large $|X|$ and with $\dim_K C_X(d)/|X|$ and $\delta_d/|X|$ as large as possible. Evaluation codes associated to a projective torus are called *generalized Reed–Solomon* codes [14]. Parameterized codes are a natural extension of this sort of codes. Some special families of evaluation codes have been extensively studied, including several variations of Reed–Muller codes [5,12,13,15,22,26].

Two of the basic parameters of $C_X(d)$ can be expressed using Hilbert functions of standard graded algebras [31] as we now explain. Recall that the *Hilbert function* of $S/I(X)$ is given by

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

The unique polynomial $h_X(t) \in \mathbb{Z}[t]$ such that $h_X(d) = H_X(d)$ for $d \gg 0$ is called the *Hilbert polynomial* of $S/I(X)$. In our situation $h_X(t)$ is a non-zero constant. Furthermore $h_X(d) = |X|$ for $d \geqslant |X| - 1$, see [19, 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.

The results of this paper will allow to compute the dimension and the length of $C_X(d)$ using Hilbert functions. In certain interesting cases we show a nice formula for the length. For algebraic toric sets arising from combinatorial structures, we are able to estimate the length in terms of n, q, and the rank of a certain subgroup of $\mathbb{Z}^{n+1}$. When $C_X(d)$ arises from a connected non-bipartite graph, we will show an upper bound for the minimum distance and compare this bound with the Singleton bound (see Section 5).

The contents of this paper are as follows. The main theorems in Section 2 are algebraic expressions for $I(X)$, which can be used to extract information about the basic parameters of $C_X(d)$ using Gröbner bases. Before introducing the theorems, recall that an additive subgroup of $\mathbb{Z}^s$ is called a *lattice*. A *lattice ideal* of S is an ideal of the form

$$I(\mathcal{L}) := \big(\big\{t^a - t^b \;\big|\; a, b \in \mathbb{N}^s \text{ with } a - b \in \mathcal{L}\big\}\big) \subset S$$

for some lattice $\mathcal{L} \subset \mathbb{Z}^s$. A polynomial of the form $t^a - t^b$, with $a, b \in \mathbb{N}^s$, is called a *binomial* of S. An ideal generated by binomials is called a *binomial ideal*. The concept of a lattice ideal is a natural generalization of a toric ideal [36, Corollary 7.1.4].

In Theorem 2.1 we show that $I(X)$ is a radical Cohen–Macaulay lattice ideal of dimension 1. Moreover, if $v_i \in \mathbb{N}^n$ for all i, we prove the equality

$$I(X) = \big(t_1 - y^{v_1}z, \ldots, t_s - y^{v_s}z, y_1^{q-1} - 1, \ldots, y_n^{q-1} - 1\big) \cap S,$$

where z is a new indeterminate. A similar statement holds for arbitrary v_i's (see Theorem 2.13). In light of this result, we can compute the reduced Gröbner basis of $I(X)$, with respect to any term order of the monomials of S, using the computer algebra system *Macaulay*2 [6,16]. Thus, we can compute the Hilbert function and the degree of $S/I(X)$, i.e., we can compute the dimension and the length of $C_X(d)$.

We present a different expression for $I(X)$—via a saturation process—valid for a wide class of algebraic toric sets (see Theorem 2.5 and Corollary 2.10). As a consequence, if

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

is a *projective torus*, then $I(\mathbb{T}) = (\{t_i^{q-1} - t_1^{q-1}\}_{i=2}^s)$ (see Corollary 2.8). This equality was first shown in [14]. Then we obtain a family of algebraic toric sets—arising from connected graphs—where $I(X)$ can be computed using a saturation process (see Corollary 2.11).

In Section 3 we focus on the computation of $|X|$, the length of $C_X(d)$. We uncover a direct method, based on integer programming techniques, to compute $|X|$ (see Proposition 3.3). Under certain conditions we prove that $(q-1)^{r-1}$ divides the length of $C_X(d)$, where r is the rank of the subgroup generated by $\{(v_i, 1)\}_{i=1}^s$ (see Theorem 3.5). In some cases—when X comes from a connected graph—we give a formula for the length of $C_X(d)$ (see Corollary 3.8).

The elements of $C_X(d)$ can be interpreted as rational functions on X. For this reason, in Section 4, we study the geometric structure of X. Let $I_{\mathcal{A}}$ be the *toric ideal* of $\mathcal{A} = \{v_1, \ldots, v_s\}$, i.e., $I_{\mathcal{A}}$ is the prime ideal of S of polynomial relations of $y^{v_1}, \ldots, y^{v_s}$. We call $\mathcal{A}$ *homogeneous* if $\mathcal{A}$ lies on an affine hyperplane not containing the origin. We prove that if $\mathcal{A}$ is homogeneous, then the projective

toric variety $V(I_{\mathcal{A}})$ intersected with a projective torus $\mathbb{T} \subset \mathbb{P}^{s-1}$ is always parameterized by Laurent monomials (see Theorem 4.1(i)). This gives a method to produce projective varieties parameterized by Laurent monomials. As a byproduct, letting $V_{\mathcal{A}}$ denote $V(I_{\mathcal{A}}) \cap \mathbb{T}$, our results allow to compute $I(V_{\mathcal{A}})$ using Gröbner bases (see Theorem 4.1(ii)). As we will see, often an algebraic toric set X is in fact a projective variety defined by binomials (see Proposition 4.3). In particular, we obtain the equality $X = V_{\mathcal{A}}$ for any $\mathcal{A}$ arising from the edges of a connected graph. As a consequence, we show a finite Nullstellensatz (see Corollary 4.4).

The dimension of $C_X(d)$ is increasing, as a function of d, until it reaches a constant value [5,11]. We observe that the minimum distance of $C_X(d)$ has the opposite behavior: it is decreasing, as a function of d, until it reaches a constant value (see Proposition 5.2).

Finally, in Section 5, we present an application of our results and techniques to algebraic coding theory. We show upper bounds for the minimum distance of parameterized codes arising from a connected non-bipartite graph (see Theorem 5.3). The geometric perspective of Section 4 plays a role here. A comparison between our bound and the Singleton bound is given (see Remark 5.4 and Example 5.5). We give an explicit formula for the minimum distance of $C_X(d)$ when X is a projective torus in $\mathbb{P}^2$ (see Proposition 5.7). Part of this formula was already known [14]; our contribution here is to use a result of [18] together with the proof of Theorem 5.3 to treat the cases not covered in [14].

For all unexplained terminology and additional information, we refer to [25,33] (for the theory of binomial and toric ideals), [7,35] (for computational commutative algebra), [2] (for graph theory), and [23,32,34] (for the theory of error-correcting codes and linear codes).

2. The ideal of an algebraic toric set parameterized by monomials

We continue to use the notation and definitions used in the introduction. Here we study the structure of the graded ideal $I(X)$ and show algebraic methods to compute a finite set of binomials generating $I(X)$. We begin this section by introducing X^*, the affine companion of X, that shares some of the properties of X, such as being a multiplicative group. Some of our results will admit affine versions for X^* as well. However, as a matter of staying focused, we will deal mostly with X while X^* will play by and large an auxiliary role.

Let $K = \mathbb{F}_q$ be a finite field with q elements and let $K[y_1^{\pm 1}, \ldots, y_n^{\pm 1}]$ be a ring of Laurent polynomials with coefficients in K. Consider a set $y^{v_1}, \ldots, y^{v_s}$ of Laurent monomials with $v_i \in \mathbb{Z}^n$ and $v_i = (v_{i1}, \ldots, v_{in}) \in \mathbb{Z}^n$. The following set is called the *affine algebraic toric set* parameterized by these monomials:

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

This model of parametrization was introduced in [27]. In [21,27] a classification of the affine toric varieties that are parameterized by monomials is given. The set $(K^*)^s$ is called an *affine algebraic torus* of dimension s and is denoted by $\mathbb{T}^*$. The affine torus $\mathbb{T}^*$ is a multiplicative group under the product operation

$$\alpha \cdot \alpha' = (\alpha_1, \ldots, \alpha_s) \cdot \left(\alpha'_1, \ldots, \alpha'_s \right) = \left(\alpha_1 \alpha'_1, \ldots, \alpha_s \alpha'_s \right).$$

Clearly, the set X^* is also a group under componentwise multiplication. We have the inclusions $X^* \subset \mathbb{T}^* \subset \mathbb{A}^s \setminus \{0\}$, where $\mathbb{A}^s$ denotes the affine space K^s.

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

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

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 $[\alpha]$. By definition, there is a structure map

$$\varphi_s : \mathbb{A}^s \setminus \{0\} \to \mathbb{P}^{s-1}, \quad \alpha \mapsto [\alpha].$$

The image of X^* under φ_s will be denoted by X. The set X is the *algebraic toric set* parameterized by $y^{v_1}, \ldots, y^{v_s}$ that was defined earlier in the introduction:

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

The set X is a multiplicative group with the product operation induced by that of X^*. The group structure of X and X^* will come into play in Section 3.

Let $S = K[t_1, \ldots, t_s]$ be a polynomial ring with coefficients in the field K with the standard grading $S = \bigoplus_{d=0}^{\infty} S_d$ induced by setting $\deg(t_i) = 1$ for all i. We are interested in the radical ideal $I(X)$ generated by the homogeneous polynomials of S that vanish on X.

Recall the following notion from commutative ring theory, which will be used a few times in the exposition. Let D be a commutative ring with unit and let M be a D-module. The set

$$\mathcal{Z}_D(M) := \{ r \in D \mid rm = 0 \text{ for some } 0 \neq m \in M \}$$

is called the set of *zero divisors* of M. If D is the ring of integers, we denote the set of zero divisors of M simply by $\mathcal{Z}(M)$.

We come to one of the main results of this section, a structure theorem allowing—with the help of *Macaulay*2 [6,16]—the computation of the Hilbert function and the degree of $S/I(X)$.

Theorem 2.1. *Let $B = K[t_1, \ldots, t_s, y_1, \ldots, y_n, z]$ be a polynomial ring over the finite field $K = \mathbb{F}_q$. If $v_i \in \mathbb{N}^n$ for all i, then the following holds*:

(a) $I(X) = (\{t_i - y^{v_i} z\}_{i=1}^{s} \cup \{y_i^{q-1} - 1\}_{i=1}^{n}) \cap S$ *and* $I(X)$ *is a binomial ideal.*
(b) $t_i \notin \mathcal{Z}_S(S/I(X))$ *for all* i *and* $I(X)$ *is a radical lattice ideal.*
(c) $S/I(X)$ *is a Cohen–Macaulay ring of dimension* 1.

Proof. (a) We set $I' = (t_1 - y^{v_1} z, \ldots, t_s - y^{v_s} z, y_1^{q-1} - 1, \ldots, y_n^{q-1} - 1) \subset B$. First we show the inclusion $I(X) \subset I' \cap S$. Take a homogeneous polynomial $F = F(t_1, \ldots, t_s)$ of degree d that vanishes on X. We can write

$$F = \lambda_1 t^{m_1} + \cdots + \lambda_r t^{m_r} \quad \left(\lambda_i \in K^*;\ m_i \in \mathbb{N}^s \right), \tag{2.1}$$

where $\deg(t^{m_i}) = d$ for all i. Write $m_i = (m_{i1}, \ldots, m_{is})$ for $1 \leqslant i \leqslant r$. Applying the binomial theorem to expand the right-hand side of the equality

$$t_j^{m_{ij}} = \left[\left(t_j - y^{v_j} z \right) + y^{v_j} z \right]^{m_{ij}}, \quad 1 \leqslant i \leqslant r,\ 1 \leqslant j \leqslant s,$$

and then substituting all the $t_j^{m_{ij}}$ in Eq. (2.1), we obtain that F can be written as:

$$F = \sum_{i=1}^{s} g_i \left(t_i - y^{v_i} z \right) + z^d F\left(y^{v_1}, \ldots, y^{v_s} \right) \tag{2.2}$$

for some $g_1, \ldots, g_s$ in B. By the division algorithm in $K[y_1, \ldots, y_n]$ (see [4, Theorem 3, p. 63]) we can write

$$F\left(y^{v_1}, \ldots, y^{v_s} \right) = \sum_{i=1}^{n} h_i \left(y_i^{q-1} - 1 \right) + G(y_1, \ldots, y_n) \tag{2.3}$$

for some $h_1, \ldots, h_n$ in $K[y_1, \ldots, y_n]$, where the monomials that occur in $G = G(y_1, \ldots, y_n)$ are not divisible by any of the monomials $y_1^{q-1}, \ldots, y_n^{q-1}$, i.e., $\deg_{y_i}(G) < q-1$ for $i = 1, \ldots, n$. Therefore, using Eqs. (2.2) and (2.3), we obtain the equality

$$F = \sum_{i=1}^{s} g_i\big(t_i - y^{v_i} z\big) + \left(\sum_{i=1}^{n} h_i\big(y_i^{q-1} - 1\big) \right) z^d + G(y_1, \ldots, y_n) z^d. \tag{2.4}$$

Thus to show that $F \in I' \cap S$ we need only show that $G = 0$. We claim that G vanishes on $(K^*)^n$. Take an arbitrary sequence $x_1, \ldots, x_n$ of elements of K^*. Making $t_i = x^{v_i}$ for all i in Eq. (2.4) and using that F vanishes on X, we obtain

$$0 = F\big(x^{v_1}, \ldots, x^{v_s}\big) = \sum_{i=1}^{s} g_i'\big(x^{v_i} - y^{v_i} z\big) + \left(\sum_{i=1}^{n} h_i\big(y_i^{q-1} - 1\big) \right) z^d + G(y_1, \ldots, y_n) z^d. \tag{2.5}$$

Since $(K^*, \cdot)$ is a group of order $q-1$, we can then make $y_i = x_i$ for all i and $z = 1$ in Eq. (2.5) to get that G vanishes on $(x_1, \ldots, x_n)$. This completes the proof of the claim. Therefore G vanishes on $(K^*)^n$ and $\deg_{y_i}(G) < q-1$ for all i. By induction on n it follows that $G = 0$. We can also show that $G = 0$ by a direct application of the combinatorial Nullstellensatz [1].

Next we show the inclusion $I(X) \supset I' \cap S$. Let $\mathcal{G}$ be a Gröbner basis of I' with respect to the lexicographic order $y_1 \succ \cdots \succ y_n \succ z \succ t_1 \succ \cdots \succ t_s$. By Buchberger algorithm [4, Theorem 2, p. 89] the set $\mathcal{G}$ consists of binomials and by elimination theory [4, Theorem 2, p. 114] the set $\mathcal{G} \cap S$ is a Gröbner basis of $I' \cap S$. Hence $I' \cap S$ is a binomial ideal. Thus to show the inclusion $I(X) \supset I' \cap S$ it suffices to show that any binomial in $I' \cap S$ is homogeneous and vanishes on X. Take a binomial $f = t^a - t^b$ in $I' \cap S$, where $a = (a_i)$ and $b = (b_i)$ are in $\mathbb{N}^s$. Then we can write

$$f = \sum_{i=1}^{s} g_i\big(t_i - y^{v_i} z\big) + \sum_{i=1}^{n} h_i\big(y_i^{q-1} - 1\big) \tag{2.6}$$

for some polynomials $g_1, \ldots, g_s, h_1, \ldots, h_n$ in B. Making $y_i = 1$ for $i = 1, \ldots, n$ and $t_i = y^{v_i} z$ for $i = 1, \ldots, s$, we get

$$z^{a_1} \cdots z^{a_s} - z^{b_1} \cdots z^{b_s} = 0 \quad \Rightarrow \quad a_1 + \cdots + a_s = b_1 + \cdots + b_s.$$

Hence f is homogeneous. Take a point $[P]$ in X with $P = (x^{v_1}, \ldots, x^{v_s})$. Making $t_i = x^{v_i}$ in Eq. (2.6), we get

$$f\big(x^{v_1}, \ldots, x^{v_s}\big) = \sum_{i=1}^{s} g_i'\big(x^{v_i} - y^{v_i} z\big) + \sum_{i=1}^{n} h_i'\big(y_i^{q-1} - 1\big).$$

Hence making $y_i = x_i$ for all i and $z = 1$, we get that $f(P) = 0$. Thus f vanishes on X.

Thus, we have shown the equality $I(X) = I' \cap S$. The proof of the inclusion $I(X) \supset I' \cap S$ shows that $I' \cap S$ is a binomial ideal. Hence $I(X)$ is a binomial ideal.

(b) Observe that a binomial ideal $J \subset S$ is a lattice ideal if and only if $t_i \notin \mathcal{Z}_S(S/J)$ for all i. This is a consequence of [8, Corollary 2.5]. Thus by part (a) we need only show that t_i is not a zero divisor of $S/I(X)$ for all i. Let $[P]$ be a point in X, with $P = (\alpha_1, \ldots, \alpha_s)$, and let $I_{[P]}$ be the ideal generated by the homogeneous polynomials of S that vanish at $[P]$. Then

$$I_{[P]} = (\alpha_1 t_2 - \alpha_2 t_1, \alpha_1 t_3 - \alpha_3 t_1, \ldots, \alpha_1 t_s - \alpha_s t_1) \quad \text{and} \quad I(X) = \bigcap_{[P] \in X} I_{[P]} \tag{2.7}$$

and the later is the primary decomposition of $I(X)$, because $I_{[P]}$ is a prime ideal of S for any $[P] \in X$. Thus $\operatorname{rad} I(X) = I(X)$, i.e., $I(X)$ is a radical ideal. Since

$$\mathcal{Z}_S\big(S/I(X)\big) = \bigcup_{[P]\in X} I_{[P]}$$

it is seen that t_i is not a zero divisor for any i.

(c) As $I_{[P]}$ has height $s-1$ for any $[P] \in X$, we get that $\dim S/I(X) = 1$. By (b) any variable t_i is an S-regular element of $S/I(X)$. Thus any variable t_i form a homogeneous regular system of parameters of $S/I(X)$, i.e., $S/I(X)$ is a Cohen–Macaulay ring by [36, Proposition 2.2.7]. □

By Theorem 2.1(a), the ideal $I(X)$ is generated by binomials. This fact is surprising, because according to Eq. (2.7) $I(X)$ is a radical ideal and all its minimal primes, except $\mathfrak{p} = (\{t_i - t_1\}_{i=2}^s)$, are non-binomial.

The next notion that we need is that of the saturation of an ideal with respect to a polynomial. We will determine when $I(X)$ can be obtained by a saturation process (see Corollary 2.10).

Definition 2.2. For an ideal $Q \subset S$ and a polynomial $h \in S$, the *saturation* of Q with respect to h is the ideal

$$\big(Q : h^\infty\big) := \big\{ f \in S \;\big|\; f h^m \in Q \text{ for some } m \geqslant 1 \big\}.$$

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

Let $\mathcal{A} = \{v_1, \ldots, v_s\} \subset \mathbb{Z}^n$ and let $I_{\mathcal{A}}$ be its associated *toric ideal*, i.e., $I_{\mathcal{A}}$ is the prime ideal of S given by (see [33]):

$$I_{\mathcal{A}} = \left(t^a - t^b \;\middle|\; a = (a_i),\ b = (b_i) \in \mathbb{N}^s,\ \sum_i a_i v_i = \sum_i b_i v_i \right) \subset S. \tag{2.8}$$

The toric ideal $I_{\mathcal{A}}$ is the kernel of the following epimorphism of K-algebras

$$K[t_1, \ldots, t_s] \to K\big[y^{v_1}, \ldots, y^{v_s}\big]$$

induced by $t_i \mapsto y^{v_i}$. We call $\mathcal{A}$ *homogeneous* if there is a vector $x_0 \in \mathbb{Q}^n$ such that $\langle v_i, x_0 \rangle = 1$ for all i. From Eq. (2.8) it follows that any binomial in $I_{\mathcal{A}}$ vanishes on X. If $\mathcal{A}$ is homogeneous, then any binomial in $I_{\mathcal{A}}$ is homogeneous, in the standard grading of S, hence belongs to $I(X)$. The binomial $t_i^{q-1} - t_1^{q-1}$ vanishes on $(K^*)^s$ because $(K^*, \cdot)$ is a group of order $q-1$. Hence $t_i^{q-1} - t_1^{q-1}$ belongs to $I(X)$ for all i. Thus if $\mathcal{A}$ is homogeneous, then $I(X)$ contains the binomial ideal $Q = I_{\mathcal{A}} + (\{t_i^{q-1} - t_1^{q-1}\}_{i=2}^s)$. For a large class of algebraic toric sets, we show that $I(X)$ is the saturation of Q with respect to $t_1 \cdots t_s$. We also describe when $I(X)$ is the saturation of Q with respect to $t_1 \cdots t_s$.

Let us introduce some more notation. Given $\Gamma \subset \mathbb{Z}^n$, the subgroup of $\mathbb{Z}^n$ generated by Γ is denoted by $\mathbb{Z}\Gamma$.

Lemma 2.3. *If $c = (c_i) \in \mathbb{Z}^s$ and $\sum_i c_i = 0$, then c is in $\mathbb{Z}\{e_2 - e_1, \ldots, e_s - e_1\}$, where e_i is the ith unit vector of $\mathbb{Z}^s$.*

Proof. Notice that $\mathbb{Z}\{e_2 - e_1, \ldots, e_s - e_1\} + \mathbb{Z}e_1 = \mathbb{Z}^s$. Then $c = \lambda_1 e_1 + \sum_{i=2}^s \lambda_i (e_i - e_1)$ for some $\lambda_i \in \mathbb{Z}$. As $\sum_i c_i = 0$, we get $\lambda_1 = 0$. □

Definition 2.4. Given $a \in \mathbb{R}^s$, its *support* is defined as $\operatorname{supp}(a) = \{i \mid a_i \neq 0\}$. Note that a can be uniquely written as $a = a^+ - a^-$, where a^+ and a^- are two non-negative vectors with disjoint support which are called the *positive* and *negative* part of a respectively.

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

Theorem 2.5. *Let $K = \mathbb{F}_q$ be a finite field, let $\mathcal{A} = \{v_1, \ldots, v_s\} \subset \mathbb{Z}^n$, and let $\phi : \mathbb{Z}^n/L \to \mathbb{Z}^n/L$ be the multiplication map $\phi(\bar{a}) = (q-1)\bar{a}$, where $L = \mathbb{Z}\{v_i - v_1\}_{i=2}^s$. If $\mathcal{A}$ is homogeneous, then*

$$\left(I_{\mathcal{A}} + \left(t_2^{q-1} - t_1^{q-1}, \ldots, t_s^{q-1} - t_1^{q-1}\right) : (t_1 \cdots t_s)^{\infty}\right) \subset I(X) \tag{2.9}$$

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

Proof. We set $Q = I_{\mathcal{A}} + (t_2^{q-1} - t_1^{q-1}, \ldots, t_s^{q-1} - t_1^{q-1})$. From the discussion above we have the inclusion $Q \subset I(X)$. By Theorem 2.1(b) each variable t_i is not a zero divisor of $S/I(X)$. It follows readily that $(Q : (t_1 \cdots t_s)^{\infty}) \subset I(X)$.

To prove the second part of the theorem we first need to identify the left-hand side of Eq. (2.9) with a lattice ideal for some specific lattice. Let A be the matrix with column vectors $v_1, \ldots, v_s$ and consider the lattice

$$\mathcal{L} = \ker_{\mathbb{Z}}(A) + \mathbb{Z}\left\{(q-1)(e_i - e_1)\right\}_{i=2}^s \subset \mathbb{Z}^s,$$

where $\ker_{\mathbb{Z}}(A) = \{x \in \mathbb{Z}^s \mid Ax = 0\}$ and e_i denotes the ith unit vector of $\mathbb{R}^s$. It is seen that

$$I(\mathcal{L}) = \left(Q : (t_1 \cdots t_s)^{\infty}\right), \tag{2.10}$$

see [8, Corollary 2.5] or [25, Lemma 7.6]. This equality is valid over any field K.

$\Rightarrow$) Assume that equality holds in Eq. (2.9). Let $\bar{b} = \overline{(b_i)}$ be an element of $\ker(\phi)$. Then we can write

$$(q-1)b = \sum_{i=1}^s a_i v_i \quad \text{with } \sum_{i=1}^s a_i = 0. \tag{2.11}$$

Consider the homogeneous binomial $f = t^{a^+} - t^{a^-}$, where $a = (a_i) = a^+ - a^-$. From Eq. (2.11) we get the equality

$$x_i^{a_1^+ v_{1i} + \cdots + a_s^+ v_{si}} = x_i^{a_1^- v_{1i} + \cdots + a_s^- v_{si}} \quad \text{for any } x_i \in K^*.$$

Consequently $f(x^{v_1}, \ldots, x^{v_s}) = 0$ for any sequence $x_1, \ldots, x_n$ in K^*. Then f vanishes on X and is homogeneous, i.e., $f \in I(X)$. By hypothesis and using Eq. (2.10), we obtain the equality $I(X) = I(\mathcal{L})$. Thus $f = t^{a^+} - t^{a^-}$ belongs to $I(\mathcal{L})$. It is seen that $a = a^+ - a^-$ belongs to $\mathcal{L}$. Then we can write $a = k + c$, where $k \in \ker_{\mathbb{Z}}(A)$ and $c \in \mathbb{Z}\{(q-1)(e_i - e_1)\}_{i=2}^s$. Then from Eq. (2.11) it follows readily that

$$(q-1)b = Aa = Ak + Ac = Ac = (q-1)Ac',$$

for some $c' \in \mathbb{Z}\{(e_i - e_1)\}_{i=2}^s$. Hence $b = Ac'$, i.e., b belongs to L. This means that $\bar{b} = 0$ and we have shown that ϕ is injective, as required.

$\Leftarrow$) Assume that ϕ is injective. We now prove the inclusion $(Q : (t_1 \cdots t_s)^{\infty}) \supset I(X)$. Take a binomial $f = t^a - t^b$ in $I(X)$ with $a = (a_i)$ and $b = (b_i)$ in $\mathbb{N}^s$. By Theorem 2.1(a) it suffices to prove that

f is in $(Q:(t_1\cdots t_s)^\infty)$. Thus by Eq. (2.10) we need only show that $a-b\in\mathcal{L}$. We set $v_i=(v_{i1},\ldots,v_{in})$ for $i=1,\ldots,s$. Since f vanishes on X we get

$$\left[x_1^{v_{11}}\cdots x_n^{v_{1n}}\right]^{a_1}\cdots\left[x_1^{v_{s1}}\cdots x_n^{v_{sn}}\right]^{a_s}=\left[x_1^{v_{11}}\cdots x_n^{v_{1n}}\right]^{b_1}\cdots\left[x_1^{v_{s1}}\cdots x_n^{v_{sn}}\right]^{b_s}\quad\text{for all } x_i\in K^*.$$

Let β be a generator of the cyclic group $(K^*,\cdot)$. Then for any $(\ell_1,\ldots,\ell_n)$ in $[1,q-1]^n\cap\mathbb{N}^n$ we can substitute $x_i=\beta^{\ell_i}$ for $i=1,\ldots,n$ in the equality above to obtain

$$\begin{aligned}&\left[\left(\beta^{\ell_1}\right)^{v_{11}}\cdots\left(\beta^{\ell_n}\right)^{v_{1n}}\right]^{a_1}\cdots\left[\left(\beta^{\ell_1}\right)^{v_{s1}}\cdots\left(\beta^{\ell_n}\right)^{v_{sn}}\right]^{a_s}\\&\quad=\left[\left(\beta^{\ell_1}\right)^{v_{11}}\cdots\left(\beta^{\ell_n}\right)^{v_{1n}}\right]^{b_1}\cdots\left[\left(\beta^{\ell_1}\right)^{v_{s1}}\cdots\left(\beta^{\ell_n}\right)^{v_{sn}}\right]^{b_s}\quad\text{for all } 1\leqslant\ell_i\leqslant q-1,\ \ell_i\in\mathbb{N}.\end{aligned}$$

Therefore for any $\ell=(\ell_1,\ldots,\ell_n)\in[1,q-1]^n\cap\mathbb{N}^n$ we get

$$\beta^{a_1\langle\ell,v_1\rangle}\cdots\beta^{a_s\langle\ell,v_s\rangle}=\beta^{b_1\langle\ell,v_1\rangle}\cdots\beta^{b_s\langle\ell,v_s\rangle}.$$

Since β has order $q-1$ we obtain

$$a_1\langle\ell,v_1\rangle+\cdots+a_s\langle\ell,v_s\rangle\equiv b_1\langle\ell,v_1\rangle+\cdots+b_s\langle\ell,v_s\rangle\mod(q-1).$$

If we set $c_i=a_i-b_i$ for all i and $\delta=(\delta_i):=c_1v_1+\cdots+c_sv_s$, then

$$\langle\ell,\delta\rangle\equiv 0\mod(q-1)\tag{2.12}$$

for any ℓ in $[1,q-1]^n\cap\mathbb{N}^n$. Making $\ell=(q-1,1,\ldots,1)$ and $\ell'=(q-2,1,\ldots,1)$ in Eq. (2.12) we get the equalities

$$\begin{aligned}\langle\ell,\delta\rangle&=(q-1)\delta_1+\delta_2+\cdots+\delta_n\equiv 0\mod(q-1),\\\langle\ell',\delta\rangle&=(q-2)\delta_1+\delta_2+\cdots+\delta_n\equiv 0\mod(q-1).\end{aligned}$$

Consequently, subtracting these equalities, we get that $\delta_1\equiv 0 \bmod (q-1)$. By an appropriate choice of ℓ and ℓ' a similar argument shows that $\delta_i\equiv 0 \bmod (q-1)$ for all i. Therefore we can write $\delta=(q-1)\gamma$ for some $\gamma\in\mathbb{Z}^n$. Notice that $\delta\in L$ because t^a-t^b is homogeneous, i.e., because $\sum_i c_i=0$. Since the map ϕ is injective we obtain that $\gamma\in L\subset\mathbb{Z}\mathcal{A}$. Hence we can write

$$\delta=c_1v_1+\cdots+c_sv_s=(q-1)(d_1v_1+\cdots+d_sv_s)$$

for some d_i's in $\mathbb{Z}$. Setting $c=(c_i)$ and $d=(d_i)$, the vector $k=(k_i)=c-(q-1)d$ is in $\ker_{\mathbb{Z}}(A)$. Notice that $\sum_i k_i=0$, because $\sum_i k_iv_i=0$ and $\mathcal{A}$ is homogeneous. Since $\sum_i c_i=0$, by Lemma 2.3 we get that c and k are in $\mathbb{Z}\{e_i-e_1\}_{i=2}^s$. From the equality $k=c-(q-1)d$ we obtain that $(q-1)d\in\mathbb{Z}\{e_i-e_1\}_{i=2}^s$ and since the quotient group

$$\mathbb{Z}^s/\mathbb{Z}\{e_i-e_1\}_{i=2}^s$$

is torsion-free we get that $d\in\mathbb{Z}\{e_i-e_1\}_{i=2}^s$. Altogether we conclude that $c=k+(q-1)d$, where $k\in\ker_{\mathbb{Z}}(A)$ and $(q-1)d\in\mathbb{Z}\{(q-1)(e_i-e_1)\}_{i=2}^s$, that is, $c\in\mathcal{L}$, as required. □

Remark 2.6. If equality occurs in Eq. (2.9), then X is the projective variety defined by the binomial ideal $I_{\mathcal{A}}+(\{t_i^{q-1}-t_1^{q-1}\}_{i=2}^s)$. This will follow from Lemma 4.2 and the proof of Proposition 4.3.

Remark 2.7. The map ϕ is injective if and only if $q-1$ is not a zero divisor of $\mathbb{Z}^n/L$ if and only if the equality $(L:_{\mathbb{Z}^n}(q-1))=L$ holds, where the left-hand side of the equality is a colon ideal consisting of all $a\in\mathbb{Z}^n$ such that $(q-1)a\in L$.

Corollary 2.8. *(See [14, Theorem 1].) Let $\mathbb{T}^*=(K^*)^s$ be an affine algebraic torus and let $\mathbb{T}$ be its image in $\mathbb{P}^{s-1}$ under the map φ_s. Then $I(\mathbb{T})=(\{t_i^{q-1}-t_1^{q-1}\}_{i=2}^s)$.*

Proof. The set $\mathbb{T}$ is an algebraic toric set parameterized by the monomials $y^{v_1},\ldots,y^{v_s}$, where $v_i=e_i$ for all i. Since $I_{\mathcal{A}}=(0)$ and the group $\mathbb{Z}^s/L=\mathbb{Z}^s/\mathbb{Z}\{e_i-e_1\}_{i=2}^s$ is torsion-free, the equality follows from Theorem 2.5. □

In [14] the evaluation codes associated to $\mathbb{T}$ are called *generalized Reed–Solomon* codes. Thus parameterized codes are a natural extension of this sort of codes.

If D is an integral domain and M is a D-module, then the *torsion sub-module* of M, denoted by $T_D(M)$, is the set of all m in M such that $pm=0$ for some $0\neq p\in D$. We say that M is *torsion-free* if $T_D(M)=(0)$. In what follows D will always be the ring of integers. Thus, we denote the set of zero divisors and the torsion sub-module of M simply by $\mathcal{Z}(M)$ and $T(M)$ respectively.

Lemma 2.9. *Let $\mathcal{A}=\{v_1,\ldots,v_s\}\subset\mathbb{Z}^n$, let $L=\mathbb{Z}\{v_i-v_1\}_{i=2}^s$ and let $\mathcal{B}=\{(v_i,1)\}_{i=1}^s$. Then*

(i_1) *there is an isomorphism of groups $\tau: T(\mathbb{Z}^n/L)\to T(\mathbb{Z}^{n+1}/\mathbb{Z}\mathcal{B})$, given by $\tau(\bar{a})=\overline{(a,0)}$,*
(i_2) *$\mathcal{Z}(\mathbb{Z}^n/L)=\mathcal{Z}(\mathbb{Z}^{n+1}/\mathbb{Z}\mathcal{B})$,*
(i_3) *if $\mathcal{A}$ is homogeneous, then $I_{\mathcal{A}}=I_{\mathcal{B}}$.*

Proof. (i_1): The map τ is clearly a well-defined one-to-one homomorphism of groups. To prove that τ is onto let $\overline{(a,b)}\in T(\mathbb{Z}^{n+1}/\mathbb{Z}\mathcal{B})$ with $a\in\mathbb{Z}^n$, $b\in\mathbb{Z}$. There is $0\neq p\in\mathbb{N}$ such that

$$p(a,b)=\lambda_1(v_1,1)+\cdots+\lambda_s(v_s,1)\quad(\lambda_i\in\mathbb{Z}).$$

Then $pa=\lambda_1v_1+\cdots+\lambda_sv_s$ and $pb=\lambda_1+\cdots+\lambda_s$. Hence we obtain the equality

$$p(a-bv_1)=\lambda_2(v_2-v_1)+\cdots+\lambda_s(v_s-v_1).$$

This means that $\overline{a-bv_1}$ is an element of $T(\mathbb{Z}^n/L)$. It follows readily that $\tau(\overline{a-bv_1})=\overline{(a,b)}$. Thus τ is onto. (i_2): This is not hard to prove. It follows using that the map τ is an isomorphism. (i_3): This follows by a direct application of [36, Corollary 7.2.42]. □

Using this lemma we will prove the next generalized version of Theorem 2.5, valid for any $\mathcal{A}$. The trick to show the next result is to lift $\mathcal{A}$ to a homogeneous set $\mathcal{B}$ in $\mathbb{Z}^{n+1}$.

Corollary 2.10. *Let $\mathcal{A}=\{v_1,\ldots,v_s\}\subset\mathbb{Z}^n$ and let $\mathcal{B}=\{(v_1,1),\ldots,(v_s,1)\}$. Then*

(a) $(I_{\mathcal{B}}+(t_2^{q-1}-t_1^{q-1},\ldots,t_s^{q-1}-t_1^{q-1}):(t_1\cdots t_s)^{\infty})\subset I(X)$.
(b) *Equality in* (a) *holds if and only if $q-1\notin\mathcal{Z}(\mathbb{Z}^{n+1}/\mathbb{Z}\mathcal{B})$.*
(c) *Let $p_1,\ldots,p_m$ be the prime numbers (if any) that occur in the factorizations of the invariant factors of the $\mathbb{Z}$-module $\mathbb{Z}^{n+1}/\mathbb{Z}\mathcal{B}$. Equality in* (a) *holds if and only if either $\mathbb{Z}^{n+1}/\mathbb{Z}\mathcal{B}$ is torsion-free or $q\not\equiv 1 \bmod p_i$ for all i.*

Proof. Let w be a new parameter and let X^w be the image under the map φ_s of the set

$$\left(X^*\right)^w=\left\{\left(x_1^{v_{11}}\cdots x_n^{v_{1n}}w,\ldots,x_1^{v_{s1}}\cdots x_n^{v_{sn}}w\right)\;\middle|\;x_i\in K^*\text{ for all }i,\ w\in K^*\right\}.$$

Clearly $\mathcal{B}$ is homogeneous because if we set $x_0 = e_{n+1}$, we get $\langle x_0, (v_i, 1)\rangle = 1$ for all i. By Lemma 2.9 we have $\mathcal{Z}(\mathbb{Z}^n/L) = \mathcal{Z}(\mathbb{Z}^{n+1}/\mathbb{Z}\mathcal{B})$, where $L = \mathbb{Z}\{v_i - v_1\}_{i=2}^s$. Therefore (a) and (b) follow at once from Theorem 2.5 and Remark 2.7 because $X = X^w$.

We now prove (c). If $\mathbb{Z}^{n+1}/\mathbb{Z}\mathcal{B}$ is torsion-free, then equality holds in (a) by part (b). Hence we may assume that this module has torsion. By the fundamental structure theorem of finitely generated abelian groups (see [20, pp. 187–188]) we have

$$\mathbb{Z}^{n+1}/\mathbb{Z}\mathcal{B} \simeq \mathbb{Z}^{r_0} \times \mathbb{Z}_{q_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{q_r^{\alpha_r}}, \tag{2.13}$$

where $q_i \in \{p_1, \ldots, p_m\}$ and $r_0 = n + 1 - \operatorname{rank}(\mathbb{Z}\mathcal{B})$. From Eq. (2.13) it is seen that one has the equality $\mathcal{Z}(\mathbb{Z}^{n+1}/\mathbb{Z}\mathcal{B}) = \bigcup_{i=1}^m (p_i)$. Therefore, by (b), equality holds in (a) if and only if $q - 1 \notin \bigcup_{i=1}^m (p_i)$ if and only if $q \not\equiv 1 \mod p_i$ for all i. □

Corollary 2.11. *Let G be a simple graph with vertex set $V_G = \{y_1, \ldots, y_n\}$, edge set E_G, and let $\mathcal{A}$ be the set of all $e_i + e_j$ such that $\{y_i, y_j\} \in E_G$. If c_1 is the number of non-bipartite connected components of G, then the equality*

$$\left(I_{\mathcal{A}} + \left(t_2^{q-1} - t_1^{q-1}, \ldots, t_s^{q-1} - t_1^{q-1}\right) : (t_1 \cdots t_s)^{\infty}\right) = I(X) \tag{2.14}$$

holds if and only if either $0 \leqslant c_1 \leqslant 1$ or $c_1 \geqslant 2$ and $\operatorname{char}(K) = 2$. In particular equality holds for any finite field K if G is connected or if G is bipartite.

Proof. Let $\mathcal{A} = \{v_1, \ldots, v_s\}$ and let $\mathcal{B} = \{(v_1, 1), \ldots, (v_s, 1)\}$ be a lifting of $\mathcal{A}$. Notice that $I_{\mathcal{A}} = I_{\mathcal{B}}$ because $\mathcal{A}$ is homogeneous, see Lemma 2.9(i_3). We denote the matrix whose columns are the vectors in $\mathcal{A}$ (resp. $\mathcal{B}$) by A (resp. B). The matrices A and B have the same rank r. We denote the greatest common divisor of all the non-zero $r \times r$ sub-determinants of A (resp. B) by $\Delta_r(A)$ (resp. $\Delta_r(B)$).

We claim that $\Delta_r(B) = 2^{c_1 - 1}$ if $c_1 \geqslant 1$ and $\Delta_r(B) = 1$ if $c_1 = 0$. If $c_1 = 0$, then G is bipartite. Thus $\Delta_r(B) = 1$ because in this case A is totally unimodular [29, p. 273], i.e., any sub-determinant of A is equal to 0 or ± 1. Assume that $c_1 \geqslant 1$, i.e., G is not bipartite. There is an exact sequence of groups

$$0 \to T\left(\mathbb{Z}^{n+1}/\mathbb{Z}\mathcal{B}\right) \xrightarrow{\vartheta} T\left(\mathbb{Z}^n/\mathbb{Z}\mathcal{A}\right) \xrightarrow{\psi} \mathbb{Z}_2 \to 0, \tag{2.15}$$

where the homomorphisms are defined as follows. For $a = (a_1, \ldots, a_n) \in \mathbb{Z}^n$ and $b \in \mathbb{Z}$, we set

$$\vartheta(\overline{a, b}) = \bar{a} \quad \text{and} \quad \psi(\bar{a}) = \overline{a_1 + \cdots + a_n}.$$

It is not hard to verify that ϑ is injective, ψ is onto, and $\operatorname{im}(\vartheta) = \ker(\psi)$. The exact sequence of Eq. (2.15) is a particular case of [30, Eq. (∗), p. 2044]. It is well known [20, pp. 187–188] that the orders of the groups $T(\mathbb{Z}^n/\mathbb{Z}\mathcal{A})$ and $T(\mathbb{Z}^{n+1}/\mathbb{Z}\mathcal{B})$ are $\Delta_r(A)$ and $\Delta_r(B)$ respectively. Therefore, using the exact sequence above, we get $\Delta_r(A) = 2\Delta_r(B)$. By a result of [17] we have

$$\mathbb{Z}^n/\mathbb{Z}\mathcal{A} \simeq \mathbb{Z}^{n-r} \times \mathbb{Z}_2^{c_1} = \mathbb{Z}^{c_0} \times \mathbb{Z}_2^{c_1} \tag{2.16}$$

and $r = n - c_0$, where c_0 is the number of bipartite components of G. Hence $\Delta_r(A) = 2^{c_1}$, and consequently $\Delta_r(B) = 2^{c_1 - 1}$ as claimed. This means that $\mathbb{Z}^{n+1}/\mathbb{Z}\mathcal{B}$ is torsion-free if and only if $c_1 = 1$. It also means that $p_1 = 2$ is the only prime factor that can occur in the factorizations of the invariant factors of $\mathbb{Z}^{n+1}/\mathbb{Z}\mathcal{B}$. The number of elements of K is equal to $q = p^u$ for some prime number p and some $u \geqslant 1$, where p is the characteristic of the field K. Altogether, by Corollary 2.10(c), we get that equality holds in Eq. (2.14) if and only if $0 \leqslant c_1 \leqslant 1$ or $c_1 \geqslant 2$ and $p^u \not\equiv 1 \mod 2$ if and only if $0 \leqslant c_1 \leqslant 1$ or $c_1 \geqslant 2$ and $p = 2$. □

Example 2.12. Let $\mathcal{A}$ be the point configuration consisting of the following points in $\mathbb{Z}^6$:

$$v_1 = (1,1,0,0,0,0), \quad v_2 = (0,1,1,0,0,0), \quad v_3 = (1,0,1,0,0,0),$$
$$v_4 = (0,0,0,1,1,0), \quad v_5 = (0,0,0,0,1,1), \quad v_6 = (0,0,0,1,0,1).$$

In this case we have $\mathbb{Z}^6/\mathbb{Z}\mathcal{A} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}^7/\mathbb{Z}\mathcal{B} \simeq \mathbb{Z} \times \mathbb{Z}_2$. If K is a finite field with $q = 2^m$ elements, then $q \not\equiv 1 \bmod 2$ and $I_{\mathcal{A}} = I_{\mathcal{B}} = 0$. Thus using Corollary 2.10(c) we get the equality $I(X) = (\{t_i^{q-1} - t_1^{q-1}\}_{i=2}^6)$. If K is a field with 3 elements, then using *Macaulay*2 [16] together with Theorem 2.1 it is seen that $I(X)$ is minimally generated by 15 binomials. In this case we do not have equality in Corollary 2.10(a).

The next result can be shown using the argument in the proof of Theorem 2.1.

Theorem 2.13. *Let $B = K[t_1, \ldots, t_s, y_0, y_1, \ldots, y_n, z]$ be a polynomial ring over a finite field $K = \mathbb{F}_q$ and let $v_i \in \mathbb{Z}^n$ for all i. The following holds*:

(a) $I(X) = (y^{v_1^-} t_1 - y^{v_1^+} z, \ldots, y^{v_s^-} t_s - y^{v_s^+} z, y_1^{q-1} - 1, \ldots, y_n^{q-1} - 1, y_0 y_1 \cdots y_n - 1) \cap S$.
(b) *$I(X)$ is a Cohen–Macaulay lattice ideal and* $\dim S/I(X) = 1$.

3. The length of parameterized codes and the degree of $S/I(X)$

We continue using the definitions and terms from the introduction and from Section 2. Let $\mathcal{A} = \{v_1, \ldots, v_s\} \subset \mathbb{Z}^n$ and let X be an algebraic toric set parameterized by the Laurent monomials $y^{v_1}, \ldots, y^{v_s}$. In this section we study $|X|$, the degree of $S/I(X)$. The motivation to study $|X|$ comes from coding theory because this number represents the length of $C_X(d)$, the parameterized code of order d.

As before, we denote the Hilbert polynomial of $S/I(X)$ by $h_X(t)$. The *index of regularity* of $S/I(X)$, denoted by $\operatorname{reg}(S/I(X))$, is the least integer $p \geqslant 0$ such that $h_X(d) = H_X(d)$ for $d \geqslant p$. 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

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

where $h_0, \ldots, h_r$ are positive integers. Indeed $h_i = \dim_K(S/(I(X), t_s))_i$. This follows from the fact that $I(X)$ is a Cohen–Macaulay lattice ideal. 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 [31] or [36, Corollary 4.1.12]).

Although Theorems 2.1 and 2.13 provide an effective method to compute the degree with *Macaulay*2 [16], we seek other methods that can lead to explicit formulas for $|X|$ for certain families of point configurations, especially for these arising from finite graphs.

At the other end, the number of elements of X^*, the affine counterpart of X, can alternatively be obtained by using linear algebra methods over the ring $\mathbb{Z}/(q-1)\mathbb{Z}$, i.e., by solving linear systems over this ring. This may then be used to estimate $|X|$. As mentioned before, some of the results of this paper have an affine version. We can think of this linear algebra approach to compute $|X^*|$ as the analog of Proposition 3.3, which is a device that enables to use linear programming methods. The multiplicity of approaches is a hint of the mathematical richness embodied in the parametrization models dealt with in this work.

We begin by presenting a direct method, based on integer programming [29], to compute the degree of $S/I(X)$. A key element here is the fact that X is a multiplicative group as explained in Section 2. Let $\mathbb{T}^* = (K^*)^n$ be an affine algebraic torus of dimension n. There is a surjective homomorphism of multiplicative groups

$$\theta : \mathbb{T}^* \to X; \quad (x_1, \ldots, x_n) \overset{\theta}{\longmapsto} \left[\left(x^{v_1}, \ldots, x^{v_s}\right)\right].$$

Therefore $\mathbb{T}^*/\ker(\theta) \simeq X$ and $|\mathbb{T}^*| = (q-1)^n = |X||\ker(\theta)|$. Thus computing $|X|$ amounts to computing $|\ker(\theta)|$.

Lemma 3.1. *Let $(x_i) = (\beta^{\ell_1}, \ldots, \beta^{\ell_n}) \in \mathbb{T}^*$ with β a generator of $(K^*, \cdot)$ and $0 \leqslant \ell_i \leqslant q-2$ for all i. Then $(x_i) \in \ker(\theta)$ if and only if there are unique integers $\lambda_1, \ldots, \lambda_s, \mu$ such that*

$$\ell A = (q-1)\lambda + \mu \mathbf{1}; \quad 0 \leqslant \mu \leqslant q-2; \ \ell = (\ell_i); \ \lambda = (\lambda_i); \ \mathbf{1} = (1, \ldots, 1).$$

Proof. Assume that $(x_i) \in \ker(\theta)$. Then $[(x^{v_1}, \ldots, x^{v_s})] = [\mathbf{1}]$. This means that there is an integer μ such that $0 \leqslant \mu \leqslant q-2$ and

$$\beta^{\langle v_i, \ell \rangle} = \beta^{\mu} \quad \text{for all } i.$$

Hence there are integers $\lambda_1, \ldots, \lambda_s$ such that

$$\langle v_i, \ell \rangle - \mu = (q-1)\lambda_i \quad \text{for all } i \quad \Rightarrow \quad \ell A = (q-1)\lambda + \mu \mathbf{1},$$

as required. To show the uniqueness assume that $\langle v_i, \ell \rangle - \mu = (q-1)\lambda_i$ and $\langle v_i, \ell \rangle - \mu' = (q-1)\lambda_i'$ for some i. Then $(q-1)(\lambda_i - \lambda_i') = \mu' - \mu$. Since $|\mu' - \mu|$ is at most $q-2$, we get $\lambda_i = \lambda_i'$ and $\mu' = \mu$. The converse follows readily by direct substitution of $x_i = \beta^{\ell_i}$ into $[(x^{v_1}, \ldots, x^{v_s})]$. □

Remark 3.2. If $v_i \in \mathbb{N}^n$, then $\lambda_i \geqslant 0$. This follows by dividing $\langle v_i, \ell \rangle$ by $(q-1)$.

Proposition 3.3. *The map $\beta^{\ell} \mapsto (\ell, \lambda, \mu)$ gives a bijection between $\ker(\theta)$ and the integral vectors of the polytope*

$$\mathcal{P} = \left\{(\ell, \lambda, \mu) \;\middle|\; \ell = (\ell_i); \ \lambda = (\lambda_i); \ \ell A = (q-1)\lambda + \mu \mathbf{1}; \ 0 \leqslant \ell_i \leqslant q-2 \text{ for all } i; \ 0 \leqslant \mu \leqslant q-2\right\}.$$

In particular the number of integral vectors of $\mathcal{P}$ equals $|\ker(\theta)|$.

Proof. By Lemma 3.1 the map $\beta^{\ell} \mapsto (\ell, \lambda, \mu)$ is well defined and bijective. □

Example 3.4. Let A be the matrix with column vectors $v_1 = (1,1,0,0)$, $v_2 = (0,1,1,0)$, $v_3 = (0,0,1,1)$, $v_4 = (1,0,0,1)$. Let K be a field with $q = 5$ elements. The integral points of $\mathcal{P}$ and the elements of $\ker(\theta)$ can be found directly using *Porta* [3]. A computation with this program shows that $\mathcal{P} \cap \mathbb{Z}^{n+s+1}$ has 16 points and that $\ker(\theta)$ is equal to

$$\begin{array}{llll}
\left(\beta^0, \beta^0, \beta^0, \beta^0\right), & \left(\beta^0, \beta^1, \beta^0, \beta^1\right), & \left(\beta^0, \beta^2, \beta^0, \beta^2\right), & \left(\beta^0, \beta^3, \beta^0, \beta^3\right), \\
\left(\beta^1, \beta^0, \beta^1, \beta^0\right), & \left(\beta^1, \beta^1, \beta^1, \beta^1\right), & \left(\beta^1, \beta^2, \beta^1, \beta^2\right), & \left(\beta^1, \beta^3, \beta^1, \beta^3\right), \\
\left(\beta^2, \beta^0, \beta^2, \beta^0\right), & \left(\beta^2, \beta^1, \beta^2, \beta^1\right), & \left(\beta^2, \beta^2, \beta^2, \beta^2\right), & \left(\beta^2, \beta^3, \beta^2, \beta^3\right), \\
\left(\beta^3, \beta^0, \beta^3, \beta^0\right), & \left(\beta^3, \beta^1, \beta^3, \beta^1\right), & \left(\beta^3, \beta^2, \beta^3, \beta^2\right), & \left(\beta^3, \beta^3, \beta^3, \beta^3\right).
\end{array}$$

Hence in this case one has $4^4 = (q-1)^n = |X||\ker(\theta)| = |X|16$. Then $|X| = 16$.

Before we state our next result, recall that a subset $\mathcal{B} \subset \mathbb{Z}^{n+1}$ is called a *Hilbert basis* if $\mathbb{N}\mathcal{B} = \mathbb{R}_+\mathcal{B} \cap \mathbb{Z}^{n+1}$, where $\mathbb{N}\mathcal{B}$ is the semigroup generated by $\mathcal{B}$, and $\mathbb{R}_+\mathcal{B}$ is the *polyhedral cone* generated by $\mathcal{B}$ consisting of the linear combinations of $\mathcal{B}$ with non-negative coefficients. A polyhedral cone containing no lines is called *pointed*. The subgroup of $\mathbb{Z}^{n+1}$ generated by $\mathcal{B}$ is denoted by $\mathbb{Z}\mathcal{B}$. The ideal $I(X)$ is called a *complete intersection* if it can be generated by $s-1$ homogeneous polynomials of S.

Theorem 3.5. *Let $\mathcal{B} = \{(v_1, 1), \ldots, (v_s, 1)\}$ and let $r = \operatorname{rank}(\mathbb{Z}\mathcal{B})$. If the polyhedral cone $\mathbb{R}_+\mathcal{B}$ is pointed and $\mathcal{B}$ is a Hilbert basis, then $(q-1)^{r-1}$ divides $|X|$.*

Proof. By [10], after permutation of the $(v_i, 1)$'s, we may assume that $\mathcal{B}' = \{(v_1, 1), \ldots, (v_r, 1)\}$ is a Hilbert basis and a linearly independent set. It is a fact that $\mathcal{B}$ is a Hilbert basis if and only if $\mathbb{R}_+\mathcal{B} \cap \mathbb{Z}\mathcal{B} = \mathbb{N}\mathcal{B}$ and $\mathbb{Z}^{n+1}/\mathbb{Z}\mathcal{B}$ is a torsion-free group. This fact can be shown using lattice theory. In Lemma 3.7 we show the part of this fact that we really need, namely that $\mathcal{B}'$ is a Hilbert basis if and only if the group $\mathbb{Z}^{n+1}/\mathbb{Z}\mathcal{B}'$ is torsion-free.

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

$$X_1 = \left\{ \left[\left(x^{v_1}, \ldots, x^{v_r} \right) \right] \mid x_i \in K^* \text{ for all } i \right\} \subset \mathbb{P}^{r-1}.$$

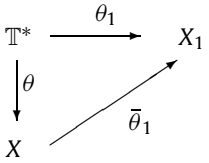
Since $I_{\mathcal{B}'} = (0)$ and $\mathbb{Z}^{n+1}/\mathbb{Z}\mathcal{B}'$ is torsion-free, by Corollary 2.10(b) we obtain the equality

$$I(X_1) = \left(\left\{ t_i^{q-1} - t_1^{q-1} \right\}_{i=2}^{r} \right).$$

Thus $I(X_1)$ is a complete intersection generated by $r-1$ forms of degree $q-1$. For complete intersections there is an explicit formula for the Hilbert series [36, p. 104]. Hence using this formula we get that the degree of $K[t_1, \ldots, t_r]/I(X_1)$ is equal to $(q-1)^{r-1}$, i.e., $|X_1| = (q-1)^{r-1}$. To complete the proof consider the epimorphism

$$\theta_1 : \mathbb{T}^* \to X_1; \quad (x_1, \ldots, x_n) \overset{\theta_1}{\longmapsto} \left[\left(x^{v_1}, \ldots, x^{v_r} \right) \right],$$

where $\mathbb{T}^* = (K^*)^n$ is an affine algebraic torus. Since $\ker(\theta) \subset \ker(\theta_1)$, there is an epimorphism $\bar{\theta}_1 : X \to X_1$ such that the diagram



is commutative. Therefore $|X_1| = (q-1)^{r-1}$ divides $|X|$. □

Definition 3.6. Let $\mathcal{P} \subset \mathbb{R}^n$ be a lattice polytope, i.e., $\mathcal{P}$ is the convex hull of a finite set of integral points in $\mathbb{R}^n$. The *relative volume* of $\mathcal{P}$, denoted by $\operatorname{vol}(\mathcal{P})$, is given by

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

where $d = \dim(\mathcal{P})$, $i \in \mathbb{N}$, $i\mathcal{P} = \{ix \mid x \in \mathcal{P}\}$.

Lemma 3.7. *Let $\mathcal{B}' = \{u_1, \ldots, u_r\} \subset \mathbb{Z}^{n+1}$ be a set of linearly independent vectors. Then $\mathcal{B}'$ is a Hilbert basis if and only if $\mathbb{Z}^{n+1}/\mathbb{Z}\mathcal{B}'$ is torsion-free.*

Proof. Let B' be the matrix with column vectors $u_1, \ldots, u_r$ and let $\Delta_r(B')$ be the greatest common divisor of all the non-zero $r \times r$ sub-determinants of B'. Assume that $\mathcal{B}'$ is a Hilbert basis. Since $|T(\mathbb{Z}^{n+1}/\mathbb{Z}\mathcal{B}')|$ is equal to $\Delta_r(B')$, we need only show $\Delta_r(B') = 1$. According to [9, Lemma 2.1] there are vectors $\gamma_1, \ldots, \gamma_r$ in $\mathbb{Z}^{n+1}$ such that

$$\mathbb{R}\mathcal{B}' \cap \mathbb{Z}^{n+1} = \mathbb{Z}\gamma_1 \oplus \cdots \oplus \mathbb{Z}\gamma_r,$$

where $\mathbb{R}\mathcal{B}'$ is the vector space spanned by $\mathcal{B}'$. Then we can write

$$u_i = c_{i1}\gamma_1 + \cdots + c_{ir}\gamma_r \quad (i = 1, \ldots, r)$$

where $C = (c_{ij})$ is an integral matrix. By [9, Remark 2.2], we have

$$\Delta_r\big(B'\big) = r!\,\mathrm{vol}\big(\mathrm{conv}(0, u_1, \ldots, u_r)\big) = \big|\det(C)\big|.$$

To complete the proof it suffices to show that $|\det(C)| = 1$. Let $c_1, \ldots, c_r$ be the rows of C. As $\mathcal{B}'$ is a Hilbert basis, it is seen that the rows of C form a Hilbert basis. Let $\mathcal{Q} = [0, 1]^r$ and let $\mathcal{P}$ be the parallelotope

$$\mathcal{P} = \{\lambda_1 c_1 + \cdots + \lambda_r c_r \mid 0 \leqslant \lambda_i \leqslant 1\}.$$

Recall that $\mathrm{vol}(\mathcal{P}) = |\det(C)|$. As $c_1, \ldots, c_r$ are linearly independent and form a Hilbert basis, we have

$$(k+1)^r = \big|k\mathcal{Q} \cap \mathbb{Z}^r\big| = \big|k\mathcal{P} \cap \mathbb{Z}^r\big| \quad \text{for all } k \in \mathbb{N}.$$

Therefore

$$1 = \lim_{k\to\infty} \frac{(k+1)^r}{k^r} = \lim_{k\to\infty} \frac{|k\mathcal{Q} \cap \mathbb{Z}^r|}{k^r} = \lim_{k\to\infty} \frac{|k\mathcal{P} \cap \mathbb{Z}^r|}{k^r} = \mathrm{vol}(\mathcal{P}).$$

Thus we have shown $1 = \mathrm{vol}(\mathcal{P}) = |\det(C)|$, as required. The converse follows readily. □

Corollary 3.8. *Let G be a connected graph with vertex set $V_G = \{y_1, \ldots, y_n\}$, edge set E_G, and let $\mathcal{A} = \{v_1, \ldots, v_s\}$ be the set of all $e_i + e_j \in \mathbb{R}^n$ such that $\{y_i, y_j\} \in E_G$. Then $|X| = (q-1)^{n-1}$ if G is non-bipartite and $|X| = (q-1)^{n-2}$ if G is bipartite.*

Proof. Assume that G is non-bipartite. Then G has a connected subgraph H with the same vertex set and with a unique cycle of odd length. We may assume that $\{v_1, \ldots, v_n\}$ is the set of all $e_i + e_j$ such that $\{y_i, y_j\}$ is an edge of H. Let B' be the matrix whose columns are the vectors in $\mathcal{B}' = \{(v_1, 1), \ldots, (v_n, 1)\}$. Then $\Delta_n(B') = 1$, see the proof of Corollary 2.11. As $|T(\mathbb{Z}^{n+1}/\mathbb{Z}\mathcal{B}')|$ equals $\Delta_n(B')$, we obtain that $\mathbb{Z}^{n+1}/\mathbb{Z}\mathcal{B}'$ is torsion-free. Therefore, by Lemma 3.7, the set $\mathcal{B}'$ is a Hilbert basis and generates a group of rank n. Hence by Theorem 3.5 we get that $(q-1)^{n-1}$ divides X_1, where

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

There is a well-defined epimorphism

$$\bar{\theta}_1 : X \to X_1; \quad \big[\big(x^{v_1}, \ldots, x^{v_s}\big)\big] \overset{\bar{\theta}_1}{\longmapsto} \big[\big(x^{v_1}, \ldots, x^{v_n}\big)\big]$$

induced by the projection map $[(\alpha_1,\ldots,\alpha_s)]\mapsto[(\alpha_1,\ldots,\alpha_n)]$. Thus $|X_1|$ divides $|X|$. Hence $(q-1)^{n-1}$ divides $|X|$. On the other hand the kernel of the map

$$\theta:\mathbb{T}^*\to X;\quad (x_1,\ldots,x_n)\overset{\theta}{\longmapsto}\left[\left(x^{v_1},\ldots,x^{v_s}\right)\right]$$

contains the diagonal subgroup $\mathcal{D}^*=\{(\lambda,\ldots,\lambda)\mid\lambda\in K^*\}$. Thus $|X|$ divides $(q-1)^{n-1}$. Putting altogether we get $|X|=(q-1)^{n-1}$.

Assume that G is bipartite. We may assume that $V_1=\{y_1,\ldots,y_p\}$, $V_2=\{y_{p+1},\ldots,y_n\}$ is the bipartition of G. The graph G has a spanning tree H with the same vertex set. We may assume that $\{v_1,\ldots,v_{n-1}\}$ is the set of all e_i+e_j such that $\{y_i,y_j\}$ is an edge of H. Let B' be the matrix whose columns are the vectors in $\mathcal{B}'=\{(v_1,1),\ldots,(v_{n-1},1)\}$. Then $\Delta_{n-1}(B')=1$, see the proof of Corollary 2.11. Therefore, by Lemma 3.7, the set $\mathcal{B}'$ is a Hilbert basis and generates a group of rank $n-1$. Hence by Theorem 3.5 we get that $(q-1)^{n-2}$ divides $|X_1|$, where

$$X_1=\left\{\left[\left(x^{v_1},\ldots,x^{v_{n-1}}\right)\right]\;\middle|\;x_i\in K^*\text{ for all }i\right\}\subset\mathbb{P}^{n-2}.$$

There is an epimorphism $\bar{\theta}_1:X\to X_1$. Thus $|X_1|$ divides $|X|$ and consequently $(q-1)^{n-2}$ divides $|X|$. On the other hand the kernel of the map $\theta:\mathbb{T}^*\to X$ contains the set Γ of all vectors of the form

$$\underbrace{(\beta^a,\ldots,\beta^a}_{p\text{-entries}},\underbrace{\beta^b,\ldots,\beta^b)}_{(n-p)\text{-entries}}$$

with $0\leqslant a,b\leqslant q-2$. Indeed any of these vector maps to $[(\beta^{a+b},\ldots,\beta^{a+b})]=[\mathbf{1}]$ under the map θ. Since $|\Gamma|=(q-1)^2$ we obtain that $|X|\leqslant(q-1)^{n-2}$. Altogether $|X|=(q-1)^{n-2}$. □

Parameterized codes arising from complete bipartite graphs have been studied in [13]. In [13] one can find formulas for some of its basic parameters. As an application we recover a formula for the length of these codes.

Corollary 3.9. *(See [13, Theorem 5.1].) If G is a complete bipartite graph with n vertices, then the length of the parameterized code $C_X(d)$ is equal to $(q-1)^{n-2}$.*

The hypothesis that G is connected is essential in Corollary 3.8:

Example 3.10. Let $K=\mathbb{F}_7$ and let X be the algebraic toric set parameterized by the monomials $y_1y_2, y_2y_3, y_1y_3, y_4y_5, y_5y_6, y_4y_6$. Using Theorem 2.1 and *Macaulay*2 [16] we get:

$$|X|=\deg S/I(X)=(q-1)^{n-1}/2=3888,\qquad \operatorname{reg}S/I(X)=16,$$

the ideal $I(X)$ is generated by 15 binomials, and the Hilbert function of $S/I(X)$ is given by

$$H_X(0)=1,\quad H_X(1)=6,\quad H_X(2)=21,\quad H_X(3)=56,\quad H_X(4)=126,$$
$$H_X(5)=252,\quad H_X(6)=457,\quad H_X(7)=762,\quad H_X(8)=1182,\quad H_X(9)=1712,$$
$$H_X(10)=2313,\quad H_X(11)=2898,\quad H_X(12)=3373,\quad H_X(13)=3678,$$
$$H_X(14)=3828,\quad H_X(15)=3878,\quad H_X(16)=3888.$$

Thus the length of the parameterized code $C_X(d)$ of order d is 3888 and its dimension is $H_X(d)$. Then the Singleton bound gives that the minimum distance of $C_X(15)$ is at most 11.

4. The vanishing ideal of certain projective binomial varieties

Let $K = \mathbb{F}_q$ be a finite field and let $\mathcal{A} = \{v_1, \ldots, v_s\} \subset \mathbb{Z}^n$ be a point configuration. In this section we study the geometric structure of X, the algebraic toric set parameterized by $y^{v_1}, \ldots, y^{v_s}$. A sufficient condition is given for X to be a projective variety defined by binomials and a finite Nullstellensatz is brought up in this connection. We prove that certain projective binomial varieties are parameterized by Laurent monomials.

Let $V(I_{\mathcal{A}}) = \{[\alpha] \in \mathbb{P}^{s-1} \mid f(\alpha) = 0 \text{ for all } f \in I_{\mathcal{A}} \text{ with } f \text{ homogeneous}\}$ be the projective toric variety defined by the toric ideal $I_{\mathcal{A}}$. We shall be interested in the following projective binomial variety $V_{\mathcal{A}}$ and in its corresponding ideal $I(V_{\mathcal{A}})$:

$$V_{\mathcal{A}} := V(I_{\mathcal{A}}) \cap \mathbb{T} = V\big(I_{\mathcal{A}} + \big(\{t_i^{q-1} - t_1^{q-1}\}_{i=2}^{s}\big)\big),$$

where $\mathbb{T} = V(\{t_i^{q-1} - t_1^{q-1}\}_{i=2}^{s}) = \{[(\alpha_i)] \in \mathbb{P}^{s-1} \mid \alpha_i \in K^* \text{ for all } i\}$ is a projective torus.

First we prove that $V_{\mathcal{A}}$ is parameterized by Laurent monomials provided that $\mathcal{A}$ is homogeneous. As in previous sections, let A be the matrix with column vectors $v_1, \ldots, v_s$. Recall that $\ker_{\mathbb{Z}}(A)$ is a free abelian group of finite rank. Let $c_1, \ldots, c_m$ be a set of generators of $\ker_{\mathbb{Z}}(A)$. Write $c_i = (c_{i1}, \ldots, c_{is})$ for $1 \leqslant i \leqslant m$. Consider the linear system

$$\begin{aligned} c_{11}x_1 + \cdots + c_{1s}x_s - (q-1)x_{s+1} &= 0 \\ \vdots \qquad\quad \vdots \qquad\quad \vdots \qquad\quad &\vdots \\ c_{m1}x_1 + \cdots + c_{ms}x_s - (q-1)x_{s+m} &= 0. \end{aligned} \tag{4.1}$$

The integral solutions of this system form a free abelian group of finite rank. Let

$$\begin{aligned} \gamma_1 &= (\alpha_{11}, \ldots, \alpha_{s1}, \alpha_{(s+1)1}, \ldots, \alpha_{(s+m)1}) \\ \vdots \quad \vdots \quad \vdots \quad \vdots \quad &\vdots \\ \gamma_k &= (\alpha_{1k}, \ldots, \alpha_{sk}, \alpha_{(s+1)k}, \ldots, \alpha_{(s+m)k}) \end{aligned} \tag{4.2}$$

be a set of generators for this group and let $\alpha_1 = (\alpha_{11}, \ldots, \alpha_{1k}), \ldots, \alpha_s = (\alpha_{s1}, \ldots, \alpha_{sk})$.

Theorem 4.1. *Let $Z = \{[(z_1^{\alpha_{11}} \cdots z_k^{\alpha_{1k}}, \ldots, z_1^{\alpha_{s1}} \cdots z_k^{\alpha_{sk}})] \mid z_i \in K^* \text{ for all } i\} \subset \mathbb{P}^{s-1}$ be the algebraic toric set parameterized by $y^{\alpha_1}, \ldots, y^{\alpha_s}$. If $\mathcal{A} = \{v_1, \ldots, v_s\}$ is homogeneous, then*

(i) $Z = V_{\mathcal{A}}$.
(ii) $I(V_{\mathcal{A}}) = (y^{\alpha_1^-}t_1 - y^{\alpha_1^+}z, \ldots, y^{\alpha_s^-}t_s - y^{\alpha_s^+}z, y_1^{q-1} - 1, \ldots, y_k^{q-1} - 1, y_0y_1\cdots y_k - 1) \cap S$.

Proof. (i) First we prove the inclusion "$\subset$": Take $[w] \in Z$. Let $f = t^a - t^b$ be a binomial in $I_{\mathcal{A}}$ with $a = (a_i)$ and $b = (b_i)$ in $\mathbb{N}^s$. Notice that f is homogeneous because so is $\mathcal{A}$. By Theorem 2.1 the ideal $I_{\mathcal{A}}$ is a binomial ideal. Thus we need only show that $f(w) = 0$. We can write

$$w = (w_i) = \big(z_1^{\alpha_{11}} \cdots z_k^{\alpha_{1k}}, \ldots, z_1^{\alpha_{s1}} \cdots z_k^{\alpha_{sk}}\big)$$

for some $z_1, \ldots, z_k$ in K^*. Let β be a generator of the cyclic group $(K^*, \cdot)$. Each z_i can be written as $z_i = \beta^{\ell_i}$ for some $0 \leqslant \ell_i \leqslant q-2$. Hence

$$f(w) = \left(z_1^{\alpha_{11}} \cdots z_k^{\alpha_{1k}}\right)^{a_1} \cdots \left(z_1^{\alpha_{s1}} \cdots z_k^{\alpha_{sk}}\right)^{a_s} - \left(z_1^{\alpha_{11}} \cdots z_k^{\alpha_{1k}}\right)^{b_1} \cdots \left(z_1^{\alpha_{s1}} \cdots z_k^{\alpha_{sk}}\right)^{b_s}$$
$$= \beta^{p_1} - \beta^{p_2}, \quad \text{where} \tag{4.3}$$

$$p_1 - p_2 = \ell_1\langle a-b, (\alpha_{11}, \ldots, \alpha_{s1})\rangle + \cdots + \ell_k\langle a-b, (\alpha_{1k}, \ldots, \alpha_{sk})\rangle. \tag{4.4}$$

From Eqs. (4.1) and (4.2) we have

$$\langle (c_{j1}, \ldots, c_{js}), (\alpha_{1i}, \ldots, \alpha_{si})\rangle \equiv 0 \mod (q-1) \tag{4.5}$$

for all i, j. The difference $a-b$ is in the kernel of A. Thus we can write

$$a - b = \eta_1(c_{11}, \ldots, c_{1s}) + \cdots + \eta_m(c_{m1}, \ldots, c_{ms}) \tag{4.6}$$

for some η_i in $\mathbb{Z}$. If we substitute the right-hand side of Eq. (4.6) into Eq. (4.4), and then use Eq. (4.5), we obtain that $p_1 - p_2 \equiv 0 \mod (q-1)$. Thus $\beta^{p_1} = \beta^{p_2}$ and $f(w) = 0$.

"$\supset$": Take $[w] \in V_{\mathcal{A}}$. We can write $w = (\beta^{h_1}, \ldots, \beta^{h_s})$, where β is a generator of the cyclic group K^*. Since $\mathcal{A}$ is homogeneous and $Ac_i = 0$, we get that $f = t_i^{c_i^+} - t^{c_i^-}$ is a homogeneous binomial in $I_{\mathcal{A}}$. Thus the evaluation of f at w is zero. This means that $\beta^{\langle h, c_i\rangle} = 1$ for all i, where $h = (h_i)$. Hence $\langle h, c_i\rangle \equiv 0 \mod (q-1)$ for all i. Hence using Eq. (4.1) and the choice of the α_i's we obtain

$$h = \lambda_1(\alpha_{11}, \ldots, \alpha_{s1}) + \cdots + \lambda_k(\alpha_{1k}, \ldots, \alpha_{sk}), \quad \lambda_i \in \mathbb{Z}.$$

Making $z_i = \beta^{\lambda_i}$ we have $w = (\beta^{h_1}, \ldots, \beta^{h_s}) = (z_1^{\alpha_{11}} \cdots z_k^{\alpha_{1k}}, \ldots, z_1^{\alpha_{s1}} \cdots z_k^{\alpha_{sk}})$. Thus $[w] \in Z$. Part (ii) follows from (i) and Theorem 2.13. □

Lemma 4.2. *If $X \subset Y \subset \mathbb{T}$ and $I(X) = I(Y)$, then $X = Y$.*

Proof. Let $[\alpha] = [(\alpha_i)]$ be a point in Y. The ideal $\mathfrak{p} = (\{\alpha_1 t_i - \alpha_i t_1\}_{i=2}^s)$ is a minimal prime of $I(Y)$, then $\mathfrak{p}$ is a minimal prime of $I(X)$. Thus $\mathfrak{p} = (\{\gamma_1 t_i - \gamma_i t_1\}_{i=2}^s)$ for some $[(\gamma_i)] \in X$. Notice that $\mathcal{G}_1 = \{t_i - (\alpha_i/\alpha_1)t_1\}_{i=2}^s$ and $\mathcal{G}_2 = \{t_i - (\gamma_i/\gamma_1)t_1\}_{i=2}^s$ are both reduced Gröbner basis of $\mathfrak{p}$ with respect to the lex ordering $t_s \succ \cdots \succ t_1$. Then by the uniqueness of such basis [4] we obtain $\mathcal{G}_1 = \mathcal{G}_2$. Hence $\alpha_i/\alpha_1 = \gamma_i/\gamma_1$ for $i = 1, \ldots, s$ and $(\alpha_i) = (\alpha_1/\gamma_1)(\gamma_i)$, i.e., $[(\alpha_i)] = [(\gamma_i)]$. This proves that $[(\alpha_i)] \in X$, as required. □

Proposition 4.3. *If $\mathcal{A}$ is homogeneous and $\mathbb{Z}^n/\mathbb{Z}\{v_i - v_1\}_{i=2}^s$ is torsion-free, then $X = V_{\mathcal{A}}$. In particular we have equality for any $\mathcal{A}$ arising from a connected or bipartite graph.*

Proof. The inclusion $X \subset V_{\mathcal{A}}$ is easy to see. The ideal $I(V_{\mathcal{A}})$ is a graded radical ideal such that t_i is not a zero divisor of $S/I(V_{\mathcal{A}})$ for all i. This follows by observing the equality

$$I(V_{\mathcal{A}}) = \bigcap_{[P] \in V_{\mathcal{A}}} I_{[P]}$$

where $I_{[P]} = (\alpha_1 t_2 - \alpha_2 t_1, \alpha_1 t_3 - \alpha_3 t_1, \ldots, \alpha_1 t_s - \alpha_s t_1)$ is the prime ideal generated by the homogeneous polynomials of S that vanish on $[P] = [(\alpha_i)]$. Hence it is seen that

$$\left(I_{\mathcal{A}} + \left(t_2^{q-1} - t_1^{q-1}, \ldots, t_s^{q-1} - t_1^{q-1}\right) : (t_1 \cdots t_s)^{\infty}\right) \subset I(V_{\mathcal{A}}) \subset I(X).$$

By Theorem 2.5 equality holds everywhere. Thus $I(V_{\mathcal{A}}) = I(X)$. Then by Lemma 4.2 we get $V_{\mathcal{A}} = X$. □

Combining this result with Theorem 2.5 we obtain:

Corollary 4.4 *(Finite Nullstellensatz). If $\mathcal{A}$ is homogeneous and $\mathbb{Z}^n/\mathbb{Z}\{v_i - v_1\}_{i=2}^s$ is torsion-free, then*

$$\big(I_{\mathcal{A}} + \big(\{t_i^{q-1} - t_1^{q-1}\}_{i=2}^s\big) : (t_1 \cdots t_s)^\infty\big) = I\big(V\big(I_{\mathcal{A}} + \big(\{t_i^{q-1} - t_1^{q-1}\}_{i=2}^s\big)\big)\big).$$

In particular this equality holds for any $\mathcal{A}$ arising from a connected or bipartite graph.

5. Minimum distance in parameterized codes

As an application of our results, in this section we present an upper bound for the minimum distance of a parameterized code arising from a connected non-bipartite graph. A comparison between our bound and the Singleton bound will be given. The geometric perspective of Section 4 plays a role here. We will give an explicit formula for the minimum distance of $C_X(d)$ when X is a projective torus in $\mathbb{P}^2$.

We begin with a general fact about parameterized linear codes. The dimension of $C_X(d)$ is increasing, as a function of d, until it reaches a constant value. This behavior was pointed out in [5] (resp. [11]) for finite (resp. infinite) fields.

Proposition 5.1. *(See [5,11].) Let $H_X(d)$ be the dimension of the parameterized linear code $C_X(d)$ and let r be the regularity index of $S/I(X)$. Then*

$$1 = H_X(0) < H_X(1) < \cdots < H_X(r-1) < H_X(d) = |X| \quad \text{for } d \geqslant r.$$

The minimum distance of $C_X(d)$ has the opposite behavior. It is decreasing, as a function of d, until it reaches a constant value.

Proposition 5.2. *If $\delta_d > 1$ (resp. $\delta_d = 1$), then $\delta_d > \delta_{d+1}$ (resp. $\delta_{d+1} = 1$).*

Proof. To show the first assertion assume that $\delta_d > 1$. For any homogeneous polynomial F in S we set $Z_X(F) = \{[P] \in X \mid F(P) = 0\}$. By definition of δ_d it suffices to show that

$$\max\big\{\big|Z_X(F)\big|\colon F \in S_d;\ \mathrm{ev}_d(F) \neq 0\big\} < \max\big\{\big|Z_X(F)\big|\colon F \in S_{d+1};\ \mathrm{ev}_{d+1}(F) \neq 0\big\}.$$

Let F be a polynomial in S_d such that $\mathrm{ev}_d(F) \neq 0$ and with $|Z_X(F)|$ as large as possible. As $\delta_d > 1$, there are $[P_1] \neq [P_2]$ in X with $P_1 = (1, a_2, \ldots, a_s)$ and $P_2 = (1, b_2, \ldots, b_s)$ such that $F(P_i) \neq 0$ for $i = 1, 2$. Then $a_k \neq b_k$ for some k. Let $G = F(a_k t_1 - t_k)$. Thus $G \in S_{d+1}$, G does not vanish on X because $G(P_2) \neq 0$ and G has more zeros than F. This proves the inequality above. The second assertion is also easy to show. □

The method of proof of the next result can also be applied to other families of parameterized codes, e.g., to parameterized codes arising from Ehrhart clutters [24] or from bipartite graphs.

We come to our main application.

Theorem 5.3. *Let G be a connected non-bipartite graph with s edges, let $V_G = \{y_1, \ldots, y_n\}$ be its vertex set, and let X be the algebraic toric set parameterized by the set of monomials $y_i y_j$ such that $\{y_i, y_j\}$ is an edge of G. If δ_d is the minimum distance of $C_X(d)$ and $d \geqslant 1$, then*

$$\delta_d \leqslant \begin{cases} (q-1)^{n-(k+2)}(q-1-\ell) & \text{if } d \leqslant (q-2)(n-1) - 1, \\ 1 & \text{if } d \geqslant (q-2)(n-1), \end{cases}$$

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

Proof. Let $v_1, \ldots, v_s$ be the set of all $e_i + e_j \in \mathbb{R}^n$ such that $\{y_i, y_j\}$ is an edge of G. Thus X is the algebraic toric set parameterized by $y^{v_1}, \ldots, y^{v_s}$. As G is a connected non-bipartite graph, there is a connected subgraph H of G with the same vertex set as G and with a unique cycle of odd length. Thus H is connected non-bipartite has n vertices and n edges. We may assume that $\{v_1, \ldots, v_n\}$ is the set of all $e_i + e_j \in \mathbb{R}^n$ such that $\{y_i, y_j\}$ is an edge of H.

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

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

We claim that $I(X_1) = (\{t_i^{q-1} - t_n^{q-1}\}_{i=1}^{n-1})$. Let B' be the matrix whose columns are the vectors in $\mathcal{B}' = \{(v_1, 1), \ldots, (v_n, 1)\}$. From the proof of Corollary 3.8, we obtain that the group $\mathbb{Z}^{n+1}/\mathbb{Z}\mathcal{B}'$ is torsion-free, and since $\mathcal{B}'$ is linearly independent, using Corollary 2.10(b) we obtain

$$\begin{aligned} \left(\left\{ t_i^{q-1} - t_n^{q-1} \right\}_{i=1}^{n-1} \right) &= \left(\left(\left\{ t_i^{q-1} - t_n^{q-1} \right\}_{i=1}^{n-1} \right) : (t_1 \cdots t_n)^{\infty} \right) \\ &= \left(I_{\mathcal{B}'} + \left(\left\{ t_i^{q-1} - t_n^{q-1} \right\}_{i=1}^{n-1} \right) : (t_1 \cdots t_n)^{\infty} \right) \\ &= I(X_1). \end{aligned}$$

This completes the proof of the claim. Let $\mathbb{T} = \{[(x_1, \ldots, x_n)] \mid x_i \in K^* \ \forall i\}$ be a projective torus in $\mathbb{P}^{n-1}$. By Corollary 2.8, we have $I(\mathbb{T}) = I(X_1)$. Consequently by Lemma 4.2, we conclude the equality $\mathbb{T} = X_1$.

Let δ_d' be the minimum distance of $C_{X_1}(d)$. Next we show that $\delta_d \leqslant \delta_d'$. By Corollary 3.8 one has $|X| = |X_1| = (q-1)^{n-1}$. Therefore the projection map

$$\overline{\theta}_1 : X \to X_1, \quad \left[(\alpha_1, \ldots, \alpha_s) \right] \mapsto \left[(\alpha_1, \ldots, \alpha_n) \right]$$

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

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

Therefore we have the inequality

$$\max\left\{ \left| Z_X(F) \right| : \ F \in S_d; \ \mathrm{ev}_d(F) \neq 0 \right\} \geqslant \max\left\{ \left| Z_{X_1}(F_1) \right| : \ F_1 \in S_d'; \ \mathrm{ev}_d(F_1) \neq 0 \right\}.$$

Consequently $\delta_d \leqslant \delta_d'$.

Case (I): First we consider the case $1 \leqslant d \leqslant (q-2)(n-1) - 1$. Let

$$\begin{aligned} M &= \max\left\{ \left| Z_{X_1}(F_1) \right| : \ F_1 \in S_d'; \ \mathrm{ev}_d(F_1) \neq 0 \right\}, \\ M_1 &= (q-1)^{n-k-2}\big((q-1)^{k+1} - (q-1) + \ell \big). \end{aligned}$$

Next we show that $M \geqslant M_1$. It suffices to exhibit a homogeneous polynomial F_1 in S' of degree d with exactly M_1 roots in $X_1 = \mathbb{T}$. Let β be a generator of the cyclic group $(K^*, \cdot)$. Consider the polynomial $F_1 = f_1 f_2 \cdots f_k g_\ell$, where $f_1, \ldots, f_k, g_\ell$ are given by

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

Now, the roots of F_1 in X_1 are in one-to-one correspondence with the union of the following sets:

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

Therefore the number of zeros of F_1 in X_1 is given by

$$
\begin{aligned}
\big|Z_{X_1}(F_1)\big| &= (q-2)\big[(q-1)^{n-2}+(q-1)^{n-3}+\cdots+(q-1)^{n-(k+1)}\big]+\ell(q-1)^{n-(k+2)}\\
&= (q-1)^{n-(k+2)}\big[(q-1)^{k+1}-(q-1)+\ell\big]=M_1,
\end{aligned}
$$

as required. Thus $M\geqslant M_1$. Altogether we get

$$
\begin{aligned}
\delta_d\leqslant\delta_d' &= \min\big\{\big\|\mathrm{ev}_d(F_1)\big\|\colon \mathrm{ev}_d(F_1)\neq 0;\ F_1\in S_d'\big\}\\
&= |X_1|-\max\big\{\big|Z_{X_1}(F_1)\big|\colon F_1\in S_d';\ \mathrm{ev}_d(F_1)\neq 0\big\}\\
&\leqslant (q-1)^{n-1}-\big((q-1)^{n-k-2}\big((q-1)^{k+1}-(q-1)+\ell\big)\big)\\
&= (q-1)^{n-k-2}\big((q-1)-\ell\big),
\end{aligned}
$$

where $\|\mathrm{ev}_d(F_1)\|$ is the number of non-zero entries of $\mathrm{ev}_d(F_1)$. This completes the proof of the case $1\leqslant d\leqslant(q-2)(n-1)-1$.

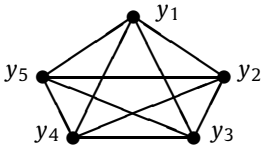
Case (II): Next we consider the case $d\geqslant(q-2)(n-1)$. Since $I(X_1)=(\{t_i^{q-1}-t_1^{q-1}\}_{i=2}^n)$, the Hilbert series of $S'/I(X_1)$ is given by $F_{X_1}(t)=(1-t^{q-1})^{n-1}/(1-t)^n$. Hence the regularity index of $S'/I(X_1)$ equals $(n-1)(q-2)$. Thus $\dim_K C_{X_1}(d)=|X_1|$ for $d\geqslant(n-1)(q-2)$. By the Singleton bound we get

$$
1\leqslant\delta_d\leqslant\delta_d'\leqslant|X_1|-\dim_K C_{X_1}(d)+1=1
$$

for $d\geqslant(n-1)(q-2)$. Thus $\delta_d=1$ for $d\geqslant(n-1)(q-2)$. □

Remark 5.4. If G is an odd cycle of length $n\geqslant 3$ and X is the algebraic toric set parameterized by the edges of G, then the minimum distance of $C_X(d)$ equals δ_d' [28]. This means that for any odd cycle the bound of Theorem 5.3 is sharper that the Singleton bound for any $d\geqslant 1$. For connected non-bipartite graphs which are not cycles, our bound is sharper than the Singleton bound within a certain range (see Example 5.5).

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



Let $C_X(d)$ be the parameterized code of order d over the field $K = \mathbb{F}_7$ and let b_d (resp. δ'_d) be the Singleton bound (resp. the bound of Theorem 5.3). Then the minimum distance of $C_X(d)$ is bounded by $\min\{b_d, \delta'_d\}$. Using *Macaulay*2 [16], together with Theorem 2.1, we obtain:

d	1	2	3	4	5	6	7	8	9	10	11	12	13
b_d	1287	1252	1162	977	646	316	127	36	6	1	1	1	1
δ'_d	1080	864	648	432	216	180	144	108	72	36	30	24	18

d	14	15	16	17	18	19	20
δ'_d	12	6	5	4	3	2	1

Thus our bound is better than the Singleton bound for $d = 1, \ldots, 6$. For $d > 7$ is the other way around. If $\mathbb{T}$ is a projective torus in $\mathbb{P}^4$, it is seen that the minimum distance of $C_{\mathbb{T}}(d)$ is exactly δ'_d, i.e., the upper bound δ'_d is the minimum distance of a linear code.

A linear code is called *maximum distance separable* (MDS for short) if equality holds in the Singleton bound. Reed–Solomon codes are MDS [32, p. 42]. The next result is not hard to show. It follows by adapting the argument of [32, p. 42].

Proposition 5.6. *Let $\mathbb{T} = \{[(x_1, x_2)] \mid x_i \in K^* \text{ for } i = 1, 2\}$ be a projective torus in $\mathbb{P}^1$. Then the minimum distance δ_d of the parameterized code $C_{\mathbb{T}}(d)$ is given by*

$$\delta_d = \begin{cases} q - 1 - d & \text{if } 1 \leqslant d \leqslant q - 3, \\ 1 & \text{if } d \geqslant q - 2, \end{cases}$$

and $C_{\mathbb{T}}(d)$ is an MDS code.

Finally we compute the minimum distance for the parameterized code defined by a projective torus in $\mathbb{P}^2$.

Proposition 5.7. *Let $\mathbb{T} = \{[(x_1, x_2, x_3)] \mid x_i \in K^* \text{ for all } i\}$ be a projective torus in $\mathbb{P}^2$. Then the minimum distance δ_d of the parameterized code $C_{\mathbb{T}}(d)$ is given by*

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

Proof. The case $1 \leqslant d \leqslant q - 2$ was shown in [14, Theorem 2]. To show the second case assume that $q - 1 \leqslant d \leqslant 2q - 5$. By Corollary 2.8, the vanishing ideal $I(\mathbb{T})$ is a complete intersection generated by $t_2^{q-1} - t_1^{q-1}$ and $t_3^{q-1} - t_1^{q-1}$. Therefore the inequality $\delta_d \geqslant 2q - d - 3$ is a direct consequence of [18, Theorem 4.4]. Next, we write $d = (q - 2) + \ell$ where $1 \leqslant \ell \leqslant q - 3$. Let β be a generator of $(K^*, \cdot)$. The homogeneous polynomial

$$F = (\beta t_1 - t_2)\cdots\left(\beta^{(q-2)}t_1 - t_2\right)(\beta t_1 - t_3)\cdots\left(\beta^{\ell}t_1 - t_3\right)$$

has degree d and the zero set $Z_{\mathbb{T}}(F)$ of F in $\mathbb{T}$ is the set:

$$\left(\{1\}\times\left\{\beta^i\right\}_{i=1}^{q-2}\times K^*\right)\cup\left(\{1\}\times\{1\}\times\left\{\beta^i\right\}_{i=1}^{\ell}\right).$$

Therefore the number of zeros of F in $\mathbb{T}$ is given by

$$\left|Z_{\mathbb{T}}(F)\right| = (q-2)(q-1)+\ell.$$

This implies that

$$\delta_d \leqslant (q-1)^2 - \left((q-2)(q-1)+\ell\right) = 2q-d-3.$$

Thus $\delta_d = 2q-d-3$. Finally, since the vanishing ideal of $\mathbb{T}$ is a complete intersection, the regularity index of $K[t_1,t_2,t_3]/I(\mathbb{T})$ is equal to $2(q-2)$. Thus by the Singleton bound we get that $\delta_d = 1$ for $d \geqslant 2q-4$. □

The lower bound of Hansen [18, Theorem 4.4]—for the minimum distance of evaluation codes on complete intersections—that we used in the proof above has been nicely generalized in [12, Theorem 3.2].

References

[1] N. Alon, Combinatorial Nullstellensatz, in: Recent Trends in Combinatorics, Maŕaháza, 1995, Combin. Probab. Comput. 8 (1–2) (1999) 7–29.
[2] B. Bollobás, Modern Graph Theory, Grad. Texts in Math., vol. 184, Springer-Verlag, New York, 1998.
[3] T. Christof, PORTA: A Polyhedron Representation Transformation Algorithm, http://www.zib.de/Optimization/Software/Porta, 1997, revised by A. Löbel and M. Stoer.
[4] D. Cox, J. Little, D. O'Shea, Ideals, Varieties, and Algorithms, Springer-Verlag, 1992.
[5] I.M. Duursma, C. Rentería, H. Tapia-Recillas, Reed–Muller codes on complete intersections, Appl. Algebra Engrg. Comm. Comput. 11 (6) (2001) 455–462.
[6] D. Eisenbud, D.R. Grayson, M. Stillman (Eds.), Computations in Algebraic Geometry with Macaulay 2, Algorithms Comput. Math., vol. 8, Springer-Verlag, Berlin, 2002.
[7] D. Eisenbud, Commutative Algebra with a View Toward Algebraic Geometry, Grad. Texts in Math., vol. 150, Springer-Verlag, 1995.
[8] D. Eisenbud, B. Sturmfels, Binomial ideals, Duke Math. J. 84 (1996) 1–45.
[9] C. Escobar, J. Martínez-Bernal, R.H. Villarreal, Relative volumes and minors in monomial subrings, Linear Algebra Appl. 374 (2003) 275–290.
[10] A.M.H. Gerards, A. Sebö, Total dual integrality implies local strong unimodularity, Math. Program. 38 (1) (1987) 69–73.
[11] A.V. Geramita, M. Kreuzer, L. Robbiano, Cayley–Bacharach schemes and their canonical modules, Trans. Amer. Math. Soc. 339 (1) (1993) 163–189.
[12] L. Gold, J. Little, H. Schenck, Cayley–Bacharach and evaluation codes on complete intersections, J. Pure Appl. Algebra 196 (1) (2005) 91–99.
[13] M. González-Sarabia, C. Rentería, Evaluation codes associated to complete bipartite graphs, Int. J. Algebra 2 (1–4) (2008) 163–170.
[14] M. González-Sarabia, C. Rentería, M. Hernández de la Torre, Minimum distance and second generalized Hamming weight of two particular linear codes, Congr. Numer. 161 (2003) 105–116.
[15] M. González-Sarabia, C. Rentería, H. Tapia-Recillas, Reed–Muller-type codes over the Segre variety, Finite Fields Appl. 8 (4) (2002) 511–518.
[16] D. Grayson, M. Stillman, Macaulay2, 1996, available via anonymous ftp from math.uiuc.edu.
[17] J. Grossman, D.M. Kulkarni, I. Schochetman, On the minors of an incidence matrix and its Smith normal form, Linear Algebra Appl. 218 (1995) 213–224.
[18] J. Hansen, Linkage and codes on complete intersections, Appl. Algebra Engrg. Comm. Comput. 14 (3) (2003) 175–185.
[19] J. Harris, Algebraic Geometry. A First Course, Grad. Texts in Math., vol. 133, Springer-Verlag, New York, 1992.
[20] N. Jacobson, Basic Algebra I, second edition, W.H. Freeman and Company, New York, 1996.
[21] A. Katsabekis, A. Thoma, Parametrizations of toric varieties over any field, J. Algebra 308 (2) (2007) 751–763.
[22] G. Lachaud, The parameters of projective Reed–Muller codes, Discrete Math. 81 (2) (1990) 217–221.
[23] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, 1977.

[24] J. Martínez-Bernal, E. O'Shea, R.H. Villarreal, Ehrhart clutters: regularity and max-flow min-cut, Electron. J. Combin. 17 (1) (2010) R52.
[25] E. Miller, B. Sturmfels, Combinatorial Commutative Algebra, Grad. Texts in Math., vol. 227, Springer-Verlag, 2004.
[26] C. Rentería, H. Tapia-Recillas, Linear codes associated to the ideal of points in $\mathbf{P}^d$ and its canonical module, Comm. Algebra 24 (3) (1996) 1083–1090.
[27] E. Reyes, R.H. Villarreal, L. Zárate, A note on affine toric varieties, Linear Algebra Appl. 318 (2000) 173–179.
[28] E. Sarmiento, M. Vaz Pinto, R.H. Villarreal, The minimum distance of parameterized codes of complete intersection vanishing ideals over finite fields, preprint.
[29] A. Schrijver, Theory of Linear and Integer Programming, John Wiley & Sons, New York, 1986.
[30] A. Simis, R.H. Villarreal, Constraints for the normality of monomial subrings and birationality, Proc. Amer. Math. Soc. 131 (2003) 2043–2048.
[31] R. Stanley, Hilbert functions of graded algebras, Adv. Math. 28 (1978) 57–83.
[32] H. Stichtenoth, Algebraic Function Fields and Codes, Universitext, Springer-Verlag, Berlin, 1993.
[33] B. Sturmfels, Gröbner Bases and Convex Polytopes, Univ. Lecture Ser., vol. 8, American Mathematical Society, Providence, RI, 1996.
[34] M. Tsfasman, S. Vladut, D. Nogin, Algebraic Geometric Codes: Basic Notions, Math. Surveys Monogr., vol. 139, American Mathematical Society, Providence, RI, 2007.
[35] W.V. Vasconcelos, Computational Methods in Commutative Algebra and Algebraic Geometry, Springer-Verlag, 1998.
[36] R.H. Villarreal, Monomial Algebras, Monogr. Textb. Pure Appl. Math., vol. 238, Marcel Dekker, New York, 2001.