Vanishing ideals of parameterized subgroups in a toric variety

Esma BARAN ÖZKAN[*]

Department of Mathematics, Faculty of Sciences, Çankırı Karatekin University, Çankırı, Turkey

Abstract: Let $\mathbb{K}$ be a finite field and X be a complete simplicial toric variety over $\mathbb{K}$ with split torus $T_X \cong (\mathbb{K}^*)^n$. We give an algorithm relying on elimination theory for finding generators of the vanishing ideal of a subgroup Y_Q parameterized by a matrix Q which can be used to study algebraic geometric codes arising from Y_Q. We give a method to compute the lattice L whose ideal I_L is exactly $I(Y_Q)$ under a mild condition. As applications, we give precise descriptions for the lattices corresponding to some special subgroups. We also prove a Nullstellensatz type theorem valid over finite fields, and share `Macaulay2`[*] codes for our algorithms.

Key words: Evaluation code, toric variety, multigraded Hilbert function, vanishing ideal, parameterized code, lattice ideal

1. Introduction

Let X be a split complete simplicial toric variety determined by the fan Σ in $\mathbb{R}^n$ over a finite field $\mathbb{K} = \mathbb{F}_q$ whose class group $\mathrm{Cl}(X)$ is torsion-free. Let $\mathbf{v}_1, \ldots, \mathbf{v}_r \in \mathbb{Z}^n$ denote the primitive generators of the one dimensional cones $\rho_1, \ldots, \rho_r$ in Σ, respectively. Each ρ_i gives T_X-invariant prime divisor $D_{\rho_i} \subseteq X$. Recall from [3, Theorem 4.1.3] that when $\mathbf{v}_1, \ldots, \mathbf{v}_r$ span $\mathbb{R}^n$, the sequence

$$0 \longrightarrow \mathbb{Z}^n \longrightarrow \mathbb{Z}^r \longrightarrow \mathrm{Cl}(X) \longrightarrow 0,$$

is exact, where $\mathbf{m} = (m_1, \ldots, m_n) \in \mathbb{Z}^n$ maps to $(\langle \mathbf{m}, \mathbf{v}_1 \rangle, \ldots, \langle \mathbf{m}, \mathbf{v}_r \rangle) \in \mathbb{Z}^r$ and $\mathbf{a} = (a_1, \ldots, a_r) \in \mathbb{Z}^r$ maps to divisor class $[a_1 D_{\rho_1} + \cdots + a_r D_{\rho_r}] \in \mathrm{Cl}(X)$. Since $\mathrm{Cl}(X)$ has no torsion element, the exact sequence can be written as

$$\mathfrak{P} : 0 \longrightarrow \mathbb{Z}^n \xrightarrow{\ \phi\ } \mathbb{Z}^r \xrightarrow{\ \beta\ } \mathbb{Z}^d \longrightarrow 0 \ , \tag{1.1}$$

where the first map is multiplication by the matrix ϕ whose rows $\mathbf{v}_1, \ldots, \mathbf{v}_r$ and $d = r - n$. The second map is multiplication by a matrix β satisfying the condition $\ker(\beta) = \mathrm{Im}(\phi)$. To simplify notation, we write $\mathbf{t}^{\mathbf{b}} = t_1^{b_1} \cdots t_s^{b_s}$ for any $\mathbf{b} = (b_1, \ldots, b_s) \in \mathbb{Z}^s$. Dualizing the short exact sequence above yields the exact sequence

$$\mathfrak{P}^* : 1 \longrightarrow G \xrightarrow{\ i\ } (\mathbb{K}^*)^r \xrightarrow{\ \pi\ } (\mathbb{K}^*)^n \longrightarrow 1 \ , \tag{1.2}$$

[*]Macaulay2. A software system for research in algebraic geometry. Website http://www.math.uiuc.edu/Macaulay2/ [accessed March 22, 2021].

where π sends $(t_1, \ldots, t_r) \in (\mathbb{K}^*)^r$ to $(\mathbf{t}^{\mathbf{u}_1}, \ldots, \mathbf{t}^{\mathbf{u}_n})$ such that $\mathbf{u}_1, \ldots, \mathbf{u}_n$ are columns of ϕ. It follows that the torus T_X is isomorphic to quotient of $(\mathbb{K}^*)^r$ by the group $G = \ker(\pi)$. Then every element of T_X can be defined as $[p_1 : \cdots : p_r] := G \cdot (p_1, \ldots, p_r)$ for some $(p_1, \ldots, p_r) \in (\mathbb{K}^*)^r$. X has total coordinate ring $S = \mathbb{K}[x_1, \ldots, x_r]$ graded by the group $\mathrm{Cl}(X) \cong \mathbb{Z}^d$. The degree of a monomial $\mathbf{x}^{\mathbf{a}} = x_1^{a_1} \cdots x_r^{a_s}$ is

$$\deg_{\mathbb{Z}^d}(\mathbf{x}^{\mathbf{a}}) := a_1 \deg_{\mathbb{Z}^d}(\mathbf{x}_1) + \cdots + a_r \deg_{\mathbb{Z}^d}(\mathbf{x}_r) = a_1 \beta_1 + \cdots + a_r \beta_r$$

such that $\beta_j := \beta(e_j)$. The grading on S yields a direct sum decomposition $S = \bigoplus_{\alpha \in \mathbb{N}\beta} S_\alpha$ where S_α is vector space whose basis consists of the monomials having degree α and $\mathbb{N}\beta$ is semigroup generated by $\beta_1, \ldots, \beta_r$.

For any matrix $Q = [\mathbf{q}_1 \mathbf{q}_2 \cdots \mathbf{q}_r] \in M_{s \times r}(\mathbb{Z})$, the subset $Y_Q = \{[\mathbf{t}^{\mathbf{q}_1} : \cdots : \mathbf{t}^{\mathbf{q}_r}] \mid \mathbf{t} \in (\mathbb{K}^*)^s\}$ of T_X is called the toric set parameterized by Q. The subgroups of T_X are exactly these parametric sets by [11, Theorem 3.2 and Corollary 3.7]. Given a subset $Y \subset X$, the vanishing ideal $I(Y)$ in S is the graded ideal generated by homogenous polynomials in S which vanish at all the elements in Y. Vanishing ideals play an important role in Algebraic Geometry and Coding Theory. Computing the generators of the vanishing ideal $I(Y_Q)$ makes it easy to determine its algebraic and geometric properties and to compute the basic parameters of a linear code obtained by evaluating homogeneous polynomials at the points of Y_Q, see [2, 9, 10, 12].

The aim of this paper is to reveal that some of the results scattered in the literature about the vanishing ideal of Y_Q can be generalised to the more general toric case by carefully adapting and modifying the arguments used. The problem of giving an algorithm computing minimal generators for $I(Y_Q)$ was solved by Villarreal, Simis and Renteria in [9, Theorem 2.1], when X is a projective space. When Y_Q is the torus T_X of a weighted projective space X, Dias and Neves proved in [5] a generalized version of [9, Theorem 2.1]. Our first generalization is Theorem 2.6, which gives an expression for $I(Y_Q)$, leading to a method (see Algorithm 1) via elimination theory for computing a generating set. We provide a `Macaulay2` code for Algorithm 1 in Procedure 2.7.

In [9, Theorem 2.5], the authors prove that $I(Y_Q) = I_L$ for the lattice $L = L_Q + (q-1)L_\beta$ under a mild condition on Q. Applying this result they also proved in [9, Proposition 4.3] that Y_Q is nothing but the zero set in the torus T_X of the lattice ideal I_{L_Q}, and concluded in [9, Corollary 4.4] that $I(V_X(I_L)) = I_L$. We generalize all these in Theorem 3.2 and Theorem 3.10.

Lopez, Villarreal, and Zarate computed in [7] the generators of the vanishing ideal of Y_Q by determining the lattice L for toric sets parameterized by diagonal matrices in projective space. In [11], Şahin not only showed that the vanishing ideal $I(Y_Q)$ is a lattice ideal for more general toric varieties but also generalized this result about diagonal matrices to more general toric varieties. We conclude the paper by giving an alternative proof in Theorem 3.13.

2. Vanishing ideal via elimination theory

In this section, we give a method yielding an algorithm for computing the generators of the vanishing ideal of Y_Q. The following basic theorems will be used to obtain our first main result giving this method.

Lemma 2.1 *[1, Lemma 2.1] Let $\mathbb{K}$ be a field and f be a polynomial in $\mathbb{K}[x_1, \ldots, x_s]$ such that $\deg_{x_i} f \leq k_i$ for all i. Let $\mathbb{K}_i \subseteq \mathbb{K}$ be a finite set with $|\mathbb{K}_i| \geq k_i + 1$ for $1 \leq i \leq s$. If f vanishes on $\mathbb{K}_1 \times \mathbb{K}_2 \times \cdots \times \mathbb{K}_s$, then $f = 0$.*

Theorem 2.2 *[4, Theorem 2, p.87] Let $I \subset \mathbb{K}[x_1, \ldots, x_k]$ be an ideal and let G be a Gröbner basis of I with respect to lex order where $x_1 > x_2 > \cdots > x_k$. Then, for every $0 \le l \le k$ the set*

$$G_l = G \cap \mathbb{K}[x_{l+1}, \ldots, x_k]$$

is a Gröbner basis of the l-th elimination ideal $I_l = I \cap \mathbb{K}[x_{l+1}, \ldots, x_k]$.

When $X = \mathbb{P}^n$, S is graded by $\mathcal{A} = \mathbb{Z}$ via $\deg(x_i) = 1$ for all i. In this case, there is a method to compute the vanishing ideal $I(Y_Q)$, see [9, Theorem 2.1]. Recently, Tochimani and Villarreal [13] generalized this result to subsets of $X = \mathbb{P}^n$ that are parameterized by ratios of Laurent polynomials, whose proof does not generalize to all toric varieties. When $X = \mathbb{P}(w_1, \ldots, w_r)$ is the weighted projective space, S is also $\mathbb{Z}$-graded via $\deg(x_i) = w_i \in \mathbb{N}$ using the degree map $\beta = [w_1 \cdots w_r]$. In [5], Dias and Neves extended the same result to weighted projective spaces if Q is the identity matrix, that is, $Y_Q = T_X$. Our main contribution is to make necessary arrangements needed for a general toric variety to adapt the corresponding proof in [9, Theorem 2.1]. Before we generalize these results to arbitrary toric varieties, let us recall that $\mathbf{m} = \mathbf{m}^+ - \mathbf{m}^-$, where $\mathbf{m}^+, \mathbf{m}^- \in \mathbb{N}^r$, and $\mathbf{x}^{\mathbf{m}}$ denotes the monomial $x_1^{m_1} \cdots x_r^{m_r}$ for any $\mathbf{m} = (m_1, \ldots, m_r) \in \mathbb{Z}^r$.

Theorem 2.3 *Let $R = \mathbb{K}[x_1, \ldots, x_r, y_1, \ldots, y_s, z_1, \ldots, z_d, w]$ be a polynomial ring which is an extension of S. Then $I(Y_Q) = J \cap S$, where*

$$J = \langle \{x_i \mathbf{y}^{\mathbf{q}_i^-} \mathbf{z}^{\beta_i^-} - \mathbf{y}^{\mathbf{q}_i^+} \mathbf{z}^{\beta_i^+}\}_{i=1}^r \cup \{y_i^{q-1} - 1\}_{i=1}^s, w\mathbf{y}^{\mathbf{q}_1^-} \mathbf{z}^{\beta_1^-} \cdots \mathbf{y}^{\mathbf{q}_r^-} \mathbf{z}^{\beta_r^-} - 1 \rangle.$$

Proof We follow the steps in the proof of [9, Theorem 2.1] making some necessary modifications. $I(Y_Q)$ is generated by homogeneous polynomials, since it is a homogeneous ideal. To show the inclusion $I(Y_Q) \subseteq J \cap S$, pick any generator $f = \sum_{i=1}^k c_i \mathbf{x}^{\mathbf{m}_i}$ of degree $\alpha = \sum_{j=1}^r \beta_j m_{ij}$. We use binomial theorem to write any monomial $\mathbf{x}^{\mathbf{m}_i}$ as

$$
\begin{aligned}
\mathbf{x}^{\mathbf{m}_i} &= x_1^{m_{i1}} \cdots x_r^{m_{ir}} = \left(x_1 - \frac{\mathbf{y}^{\mathbf{q}_1^+} \mathbf{z}^{\beta_1^+}}{\mathbf{y}^{\mathbf{q}_1^-} \mathbf{z}^{\beta_1^-}} + \frac{\mathbf{y}^{\mathbf{q}_1^+} \mathbf{z}^{\beta_1^+}}{\mathbf{y}^{\mathbf{q}_1^-} \mathbf{z}^{\beta_1^-}}\right)^{m_{i1}} \cdots \left(x_r - \frac{\mathbf{y}^{\mathbf{q}_r^+} \mathbf{z}^{\beta_1^+}}{\mathbf{y}^{\mathbf{q}_r^-} \mathbf{z}^{\beta_1^-}} + \frac{\mathbf{y}^{\mathbf{q}_r^+} \mathbf{z}^{\beta_r^+}}{\mathbf{y}^{\mathbf{q}_r^-} \mathbf{z}^{\beta_r^-}}\right)^{m_{ir}} \\
&= \sum_{j=1}^r g_{ij} \frac{x_j \mathbf{y}^{\mathbf{q}_j^-} \mathbf{z}^{\beta_j^-} - \mathbf{y}^{\mathbf{q}_j^+} \mathbf{z}^{\beta_j^+}}{\left(\mathbf{y}^{\mathbf{q}_1^-} \mathbf{z}^{\beta_1^-}\right)^{m_{i1}} \cdots \left(\mathbf{y}^{\mathbf{q}_r^-} \mathbf{z}^{\beta_r^-}\right)^{m_{ir}}} + \mathbf{z}^\alpha \left(\frac{\mathbf{y}^{\mathbf{q}_1^+}}{\mathbf{y}^{\mathbf{q}_1^-}}\right)^{m_{i1}} \cdots \left(\frac{\mathbf{y}^{\mathbf{q}_r^+}}{\mathbf{y}^{\mathbf{q}_r^-}}\right)^{m_{ir}}
\end{aligned}
$$

where $g_{i1}, \ldots, g_{ir} \in R$ for all i. Substituting all the $\mathbf{x}^{\mathbf{m}_i}$ in f, we get

$$f = \sum_{j=1}^r g_j \frac{x_j \mathbf{y}^{\mathbf{q}_j^-} \mathbf{z}^{\beta_j^-} - \mathbf{y}^{\mathbf{q}_j^+} \mathbf{z}^{\beta_j^+}}{\left(\mathbf{y}^{\mathbf{q}_1^-} \mathbf{z}^{\beta_1^-}\right)^{m_1'} \cdots \left(\mathbf{y}^{\mathbf{q}_r^-} \mathbf{z}^{\beta_r^-}\right)^{m_r'}} + \mathbf{z}^\alpha f(\mathbf{y}^{q_1}, \ldots, \mathbf{y}^{q_r}),$$

where $g_j = \sum_{i=1}^k c_j g_{i,j}$ and $m_j' = \sum_{i=1}^k m_{ij}$. Then set $m = \sum_{j=1}^r \sum_{i=1}^k m_{ij}$. We multiply f by h^m to clear all the denominators which yields that

$$fh^m = \sum_{j=1}^r G_j \left(x_j \mathbf{y}^{\mathbf{q}_j^-} \mathbf{z}^{\beta_j^-} - \mathbf{y}^{\mathbf{q}_j^+} \mathbf{z}^{\beta_j^+}\right) + \mathbf{z}^{\alpha'} \left(\mathbf{y}^{\mathbf{q}_1^-} \cdots \mathbf{y}^{\mathbf{q}_r^-}\right)^m f(\mathbf{y}^{q_1}, \ldots, \mathbf{y}^{q_r}),$$

where $h = \mathbf{y}^{\mathbf{q}_1^-}\mathbf{z}^{\beta_1^-}\cdots\mathbf{y}^{\mathbf{q}_r^-}\mathbf{z}^{\beta_r^-}$ and

$$\alpha' = \sum_{j=1}^{r}\left[\beta_j^-(m-m_{ij}) + \beta_j^+ m_{ij}\right] \in \mathbb{N}^n, \quad G_j = g_j\prod_{j=1}^{r}\left(\mathbf{y}^{\mathbf{q}_j^-}\mathbf{z}^{\beta_j^-}\right)^{m-m_j'} \in R.$$

We can apply division algorithm and divide $F = \left(\mathbf{y}^{\mathbf{q}_1^-}\cdots\mathbf{y}^{\mathbf{q}_r^-}\right)^m f(\mathbf{y}^{q_1},\ldots,\mathbf{y}^{q_r})$ by $\{y_i^{q-1}-1\}_{i=1}^s$ which leads to

$$fh^m = \sum_{j=1}^{r}G_i\left(x_j\mathbf{y}^{\mathbf{q}_j^-}\mathbf{z}^{\beta_j^-} - \mathbf{y}^{\mathbf{q}_j^+}\mathbf{z}^{\beta_j^+}\right) + \mathbf{z}^{\alpha'}\left(\sum_{i=1}^{s}H_i(y_i^{q-1}-1) + E(y_1,\ldots,y_s)\right). \quad (2.1)$$

Lemma 2.1 forces that E is the zero polynomial, as $E(\mathbf{t}) = 0$ for all $\mathbf{t} = (t_1,\ldots,t_s) \in (\mathbb{K}^*)^s$.

Multiplying now the equation (2.1) by w^m, we have

$$f(hw)^m = \sum_{j=1}^{r}w^m G_j\left(x_j\mathbf{y}^{\mathbf{q}_j^-}\mathbf{z}^{\beta_j^-} - \mathbf{y}^{\mathbf{q}_j^+}\mathbf{z}^{\beta_j^+}\right) + w^m\mathbf{z}^{\alpha'}\sum_{i=1}^{s}H_i(y_i^{q-1}-1).$$

As $f(hw)^m = f(hw - 1 + 1)^m = f(H(hw-1) + 1) = fH(hw-1) + f$ for some $H \in R$ by binomial theorem, it follows that

$$f = \sum_{j=1}^{r}w^m G_i\left(x_j\mathbf{y}^{\mathbf{q}_j^-}\mathbf{z}^{\beta_j^-} - \mathbf{y}^{\mathbf{q}_j^+}\mathbf{z}^{\beta_j^+}\right) + w^m\mathbf{z}^{\alpha'}\sum_{i=1}^{s}H_i(y_i^{q-1}-1) - fH(hw-1)$$

which establishes the inclusion $I(Y_Q) \subseteq J \cap S$.

As J is generated by binomials, so is $J \cap S$ by Theorem 2.2. Take $f = \mathbf{x}^{\mathbf{a}} - \mathbf{x}^{\mathbf{b}} \in J \cap S$ and write

$$f = \sum_{j=1}^{r}G_j\left(x_j\mathbf{y}^{\mathbf{q}_j^-}\mathbf{z}^{\beta_j^-} - \mathbf{y}^{\mathbf{q}_j^+}\mathbf{z}^{\beta_j^+}\right) + \sum_{i=1}^{s}H_i(y_i^{q-1}-1) + H(hw-1), \quad (2.2)$$

for some polynomials $G_1,\ldots,G_r, H_1,\ldots,H_s, H$ in R. As the last equality is valid also in the ring $R[z_1^{-1},\ldots,z_d^{-1}]$ setting $y_i = 1, x_i = \mathbf{z}^{\beta_i}, w = 1/\mathbf{z}^{\beta_1^-}\cdots\mathbf{z}^{\beta_r^-}$ gives

$$\mathbf{z}^{a_1\beta_1+\cdots+a_r\beta_r} - \mathbf{z}^{b_1\beta_1+\cdots+b_r\beta_r} = 0.$$

Thus, $f = \mathbf{x}^{\mathbf{a}} - \mathbf{x}^{\mathbf{b}}$ is homogeneous. By setting $x_i = \mathbf{t}^{\mathbf{q}_i}, y_j = t_j, z_k = 1$ for all i,j,k and $w = 1/\mathbf{t}^{\mathbf{q}_1^-}\cdots\mathbf{t}^{\mathbf{q}_r^-}$ in (2.2), we obtain $f(\mathbf{t}^{\mathbf{q}_1},\ldots,\mathbf{t}^{\mathbf{q}_r}) = 0$ and so $f \in I(Y_Q)$. Consequently, $J \cap S \subseteq I(Y_Q)$. $\qquad\square$

Remark 2.4 *Given complete simplicial toric variety X, we have the exact sequence $\mathfrak{P}$ in 1.1. Recall that the rows of ϕ are the primitive generators of the rays in the fan of X. There are many alternatives for the matrix β as it can be chosen so that the condition $\ker(\beta) = \operatorname{Im}(\phi)$ is satisfied. However, by [8, Theorem 8.6 and Corollary 8.8], we can choose $\beta_j \in \mathbb{N}^d$, where $\mathbb{N}$ is the set of non-negative integers, since the dimension $\dim_{\mathbb{K}}(S_\alpha)$ is finite for all $\alpha \in \mathbb{N}\beta$ by [3, Proposition 4.3.8].*

Example 2.5 *The matrix β obtained by the following* `Macaulay2` *procedure has negative entries.*

```
i1 : q=11; Phi=matrix{{1,0},{0,1},{-1,2},{0,-1}}; r=numRows Phi;
i2 : n=numColumns Phi; (D,P,K) = smithNormalForm Phi; Beta=P^{n..r-1};
o2 = | -1  2 -1  0 |
     |  0  1  0  1 |
```

Note that multiplying the first row by -1 and then adding twice the second row we get $\beta = \begin{bmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 0 & 1 \end{bmatrix}$ to be a better alternative!

In practice, different matrices Q may give the same subgroup Y_Q of T_X. As we work over the finite field $\mathbb{F}_q$, we note that restricting to matrices Q with non-negative entries strictly smaller than $q-1$, does not harm the generality, since $t^{q-1} \equiv 1 \bmod q$, for any $t \in \mathbb{F}_q^*$. This reduction together with the assumption that $\beta_j \in \mathbb{N}^d$ will decrease the complexity of the algorithm for finding a generating set for $I(Y_Q)$ which will be based on the following result whose proof is skipped.

Theorem 2.6 *Let $R = \mathbb{K}[x_1,\ldots,x_r,y_1,\ldots,y_s,z_1,\ldots,z_d]$ be a polynomial ring which is an extension of S. Then $I(Y_Q) = J \cap S$, where*

$$J = \langle \{x_i - \mathbf{y}^{\mathbf{q}_i} \mathbf{z}^{\beta_i}\}_{i=1}^r \cup \{y_i^{q-1} - 1\}_{i=1}^s \rangle.$$

Theorem 2.6 gives rise to Algorithm 1 for computing the binomial generators of the ideal $I(Y_Q)$ in the ring $\mathbb{F}_q[x_1,\ldots,x_r]$ from the given matrices Q and β with entries from the set $\mathbb{N}$ of non-negative integers, for every prime power q.

Algorithm 1 Computing the generators of vanishing ideal $I(Y_Q)$.

Input The matrices $Q \in M_{s \times r}(\mathbb{N})$, $\beta \in M_{d \times r}(\mathbb{N})$ and a prime power q.
Output The generators of $I(Y_Q)$.

1: Write the ideal J of R using Theorem 2.6.
2: Find the Gröbner basis G of J wrt. lex order $z_1 > \cdots > z_d > y_1 > \cdots > y_s > x_1 > \cdots > x_r$.
3: Find $G \cap S$ so that $I(Y_Q) = \langle G \cap S \rangle$.

Using the function `toBinomial` creating a binomial from a list of integers (see [6]), we write a `Macaulay2` code which implements this algorithm.

Procedure 2.7 *Given a particular input q, Q, β, the following procedure finds the generators of $I(Y_Q)$.*

```
i2 : toBinomial = (b,R) -> (top := 1_R; bottom := 1_R;
scan(#b, i -> if b_i > 0 then top = top * R_i^(b_i)
else if b_i < 0 then bottom = bottom * R_i^(-b_i)); top - bottom);
i3 : r=numColumns Q;s=numRows Q; d=numRows Beta; F=ZZ/q;
i4 : C=(id_(ZZ^r)| -transpose Q | -transpose Beta);
i5 : R=F[x_1..x_r,y_1..y_s,z_1..z_d];
i6 : J = ideal apply(entries C, b -> toBinomial(b,R))+ideal apply (s,i->R_(r+i) ^(q-1)-1)
i7 : IYQ=eliminate (J,for i from r to r+s+d-1 list R_i)
```

Example 2.8 *Let* $X = \mathcal{H}_2$ *be the Hirzebruch surface over* $\mathbb{K} = \mathbb{F}_1 1$. *The fan for* X *has primitive ray generators* $\mathbf{v}_1 = (1,0)$, $\mathbf{v}_2 = (0,1)$, $\mathbf{v}_3 = (-1,2)$, $\mathbf{v}_4 = (0,-1)$ *and its coordinate ring* $S = \mathbb{K}[x_1, x_2, x_3, x_4]$. *Then for* X, *the matrices* ϕ *and* β *in 1.1 are given by*

$$\phi = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ -1 & 2 \\ 0 & -1 \end{bmatrix}, \ \beta = \begin{bmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 0 & 1 \end{bmatrix}.$$

This shows that $S = \mathbb{K}[x_1, x_2, x_3, x_4]$ *is graded by letting*

$$\deg_{\mathbb{Z}^2}(x_1) = \deg_{\mathbb{Z}^2}(x_3) = (1,0), \quad \deg_{\mathbb{Z}^2}(x_2) = (0,1), \quad \deg_{\mathbb{Z}^2}(x_4) = (2,1).$$

Since the map π *in 1.2 is defined by* $\pi : \mathbf{t} \mapsto (t_1 t_3^{-1}, t_2 t_3^2 t_4^{-1})$ *for* X,

$$G = \ker(\pi) = \{(t_1, t_2, t_1, t_1^2 t_2) \mid t_1, t_2 \in \mathbb{K}^*\} \cong (\mathbb{K}^*)^2.$$

Thus the torus of $X = X_\Sigma$ *has quotient representation* $T_X \cong (\mathbb{K}^*)^2 \cong (\mathbb{K}^*)^4/G$. *Consider the set parameterized by* $Q = [1 \ 2 \ 3 \ 4]$, *that is,* $Y_Q = \{[t : t^2 : t^3 : t^4] \ \mid \ t \in \mathbb{K}^*\}$. *In order to compute the generators of* $I(Y_Q)$ *in* Macaulay2 *it suffices to supply* q *together with* Q *and* β:

```
i1 : q=11; Beta=matrix {{1,0,1,2},{0,1,0,1}}; Q=matrix {{1,2,3,4}};
```

and we obtain $I(Y_Q) = \langle x_1^2 x_2 - x_4, x_1^5 - x_3^5 \rangle$ *by using Procedure 2.7. The vanishing ideal* $I(Y_Q)$ *is also evaluated in [2, Example 3.7] by computing the lattice* L *asociated* $I(Y_Q)$.

3. Conceptual descriptions of the lattice of a vanishing ideal

A subgroup $L \subseteq \mathbb{Z}^r$ is called a lattice. For any lattice L, the lattice ideal corresponding to L, denoted I_L, is the ideal generated by binomials $\mathbf{x}^\mathbf{a} - \mathbf{x}^\mathbf{b}$ for all $\mathbf{a}, \mathbf{b} \in \mathbb{N}^r$ such that $\mathbf{a} - \mathbf{b} \in L$.

The vanishing ideal $I(Y_Q)$ is a lattice ideal, see [11]. Then the lattice associated with $I(Y_Q)$ is identified in the following lemma.

Lemma 3.1 *[2, Lemma 3.2] The ideal* $I(Y_Q)$ *is equal to* I_L *where* $L = \{\mathbf{m} \in L_\beta : Q\mathbf{m} \equiv 0 \ mod \ (q-1)\}$.

This description is not very useful in practice, for it requires some operations. In this section, we give a handier description of the lattice of the ideal $I(Y_Q)$, in terms of Q and β, under a condition on the lattice $\mathcal{L} = QL_\beta = \{Q\mathbf{m} | \mathbf{m} \in L_\beta\}$ using Lemma 3.1. Before stating it, let us remind that $\mathcal{L} : (q-1) = \{\mathbf{m} \in \mathbb{Z}^s | (q-1)\mathbf{m} \in \mathcal{L}\}$ and the colon module $\mathcal{L} : (q-1)\mathbb{Z}^s$ are the same. Given any matrix Q, $\ker_\mathbb{Z} Q$ is a lattice, denoted L_Q.

Theorem 3.2 *Let* $L = (L_Q \cap L_\beta) + (q-1)L_\beta$. *Then* $I_L \subseteq I(Y_Q)$. *The equality holds if and only if* $\mathcal{L} = \mathcal{L} : (q-1)$.

Proof We start with the proof of the inclusion $I_L \subseteq I(Y_Q)$. By the virtue of Lemma 3.1, it suffices to prove that $L \subseteq L_1 = \{\mathbf{m} \in L_\beta : Q\mathbf{m} \equiv 0 \mod (q-1)\}$, as $I(Y_Q) = I_{L_1}$. Take $\mathbf{m} \in L$. Since $L = (L_Q \cap L_\beta) + (q-1)L_\beta \subseteq L_\beta$, we have $\mathbf{m} \in L_\beta$. On the other hand, we can write $\mathbf{m} = \mathbf{m}' + (q-1)\mathbf{m}''$ for

some $\mathbf{m}' \in L_Q \cap L_\beta$ and $\mathbf{m}'' \in L_\beta$. Since $Q\mathbf{m} = (q-1)Q\mathbf{m}''$, it follows that $\mathbf{m} \in L_1$, completing the proof of the inclusion.

Now, in order to show that $I(Y_Q) \subseteq I_L$ iff $\mathcal{L} = \mathcal{L} : (q-1)$, it is enough to prove that $L_1 \subseteq L$ iff $\mathcal{L} : (q-1) \subseteq \mathcal{L}$. Assume first that $L_1 \subseteq L$ and take $\mathbf{z} \in \mathcal{L} : (q-1)$. This means that there exist $\mathbf{m} \in L_\beta$ such that $(q-1)\mathbf{z} = Q\mathbf{m}$. So, $\mathbf{m} \in L_1 \subseteq L$ and we have $\mathbf{m} = \mathbf{m}' + (q-1)\mathbf{m}''$ for some $\mathbf{m}' \in L_Q \cap L_\beta$ and $\mathbf{m}'' \in L_\beta$. Thus, $(q-1)\mathbf{z} = Q\mathbf{m} = (q-1)Q\mathbf{m}''$, and we have $\mathbf{z} = Q\mathbf{m}'' \in \mathcal{L}$. Therefore, $\mathcal{L} : (q-1) \subseteq \mathcal{L}$.

Suppose now that $\mathcal{L} : (q-1) \subseteq \mathcal{L}$ and let $\mathbf{m} \in L_1$. Then $\mathbf{m} \in L_\beta$ and $Q\mathbf{m} = (q-1)\mathbf{z}$ for some $\mathbf{z} \in \mathbb{Z}^s$. So, $\mathbf{z} \in \mathcal{L} : (q-1) \subseteq \mathcal{L}$ yielding $\mathbf{z} = Q\mathbf{m}'$ for some $\mathbf{m}' \in L_\beta$. Hence $Q(\mathbf{m} - (q-1)\mathbf{m}') = 0$ and so, $\mathbf{m} - (q-1)\mathbf{m}' \in L_Q \cap L_\beta$. This implies that $\mathbf{m} = (\mathbf{m} - (q-1)\mathbf{m}') + (q-1)\mathbf{m}' \in L$. Hence, $L_1 \subseteq L$. □

We can check if the condition above is satisfied and in the affirmative case, we can compute the generators of the lattice using the following code in `Macaulay2`.

Procedure 3.3 *Check if the condition $\mathcal{L} = \mathcal{L} : (q-1)$ holds and produces a basis for L.*

```
i2: s=numRows Q;
i3: LL=image (Q*Phi);
i4: if LL:(q-1)*(ZZ^s)==LL then print yes else print no;
i5: ML=mingens ((q-1)*(image Phi)+intersect(ker Q,image Phi));
```

Example 3.4 *Consider the Hirzebruch surface $X = \mathcal{H}_2$ over the field $\mathbb{F}_2$ and take $Q = [1\ 2\ 3\ 4]$. The input is as follows:*

```
i1 : q=2;Phi=matrix{{1,0},{0,1},{-1,2},{0,-1}};Q=matrix {{1,2,3,4}};
```

and then Procedure 3.3 tells us that the condition is satisfied and gives $L = \langle(-1,0,1,0),(-2,-1,0,1)\rangle$.

Definition 3.5 *Q is called homogeneous, if there is a matrix $A \in M_{d\times s}(\mathbb{Q})$ such that $AQ = \beta$.*

Lemma 3.6 *Let $Q = [\mathbf{q}_1 \cdots \mathbf{q}_r] \in M_{s\times r}(\mathbb{Z})$. Q is homogeneous iff $L_Q \subseteq L_\beta$.*

Proof Suppose that Q is homogeneous. So, $AQ = \beta$ for some matrix $A \in M_{d\times s}(\mathbb{Q})$. Take an element $\mathbf{m}$ of L_Q. Since $Q\mathbf{m} = 0$, we have $\beta\mathbf{m} = AQ\mathbf{m} = 0$. Hence, $\mathbf{m} \in L_\beta$ and thus $L_Q \subseteq L_\beta$. Conversely, assume that $L_Q \subseteq L_\beta$. Denote by Q' the $(s+d) \times r$ matrix $[Q\ \beta]^T$. Then $L_{Q'} = L_Q \cap L_\beta = L_Q$ which implies that the rows of β belong to the row space of Q. So, a row of β can be expressed as a $\mathbb{Q}$-linear combination of the rows of Q. Let the following be the i-th row of β:

$$a_{i1}[q_{11} \cdots q_{1r}] + \cdots + a_{is}[q_{s1} \cdots q_{sr}] = [(a_{i1}q_{11} + \cdots + a_{is}q_{s1}) \quad \cdots \quad (a_{i1}q_{1r} + \cdots + a_{is}q_{sr})]$$
$$= [([a_{i1} \cdots a_{is}]\mathbf{q}_1) \quad \cdots \quad ([a_{i1} \cdots a_{is}]\mathbf{q}_r)].$$

So, for $A = (a_{ij}) \in M_{d\times s}(\mathbb{Q})$ we have $AQ = \beta$. □

The next corollary is a generalization of Theorem 2.5 in [9] studying the case $X = \mathbb{P}^n$.

Corollary 3.7 *Let $Q = [\mathbf{q}_1 \cdots \mathbf{q}_r] \in M_{s\times r}(\mathbb{Z})$ be a homogeneous matrix and $L = L_Q + (q-1)L_\beta$. Then $I_L \subseteq I(Y_Q)$. The equality holds if and only if $\mathcal{L} = \mathcal{L} : (q-1)$.*

Proof Since Q is homogeneous, $L_Q \subseteq L_\beta$ shows that $L = L_Q \cap L_\beta + (q-1)L_\beta = L_Q + (q-1)L_\beta$. Therefore, $I(Y_Q) = I_L$ from Theorem 3.2. □

Using Theorem 3.2, we give other proofs of the following facts proven for the first time in [11].

Corollary 3.8 $I(T_X) = I_{(q-1)L_\beta}$

Proof T_X is the toric set parameterized by the identity matrix $Q = I_r$. It is clear that $L_Q = \ker_{\mathbb{Z}} I_r = \{0\}$. Notice also that $\mathcal{L} = QL_\beta = \{I_r \mathbf{m} | \mathbf{m} \in L_\beta\} = L_\beta$. Since L_β is torsion free, the condition $\mathcal{L} = \mathcal{L} : (q-1)$ is satisfied. As $L = (q-1)L_\beta$, we have that $I(T_X) = I_{(q-1)L_\beta}$ by Theorem 3.2. □

Corollary 3.9 *The vanishing ideal of the point* $[1 : \cdots : 1]$ *is the toric ideal* I_{L_β}.

Proof Take $Q = \beta$. Then $Y_Q = \{[1 : \cdots : 1]\}$ and $L_Q = L_\beta$. So, $\mathcal{L} = QL_\beta = \{Q\mathbf{m} | \mathbf{m} \in L_Q\} = 0$. Thus, $L = L_\beta + (q-1)L_\beta = L_\beta$. This gives $I([1 : \cdots : 1]) = I_{L_\beta}$ by Theorem 3.2. □

Before giving another consequence of Theorem 3.2, let us introduce more notation. For a homogeneous ideal J, we define its zero locus in X to be the following:

$$V_X(J) := \{[P] \in X : F(P) = 0, \text{for all homogeneous } F \in J\}.$$

It follows from Lemma 3.6 and [11, Proposition 2.3] that Q is homogeneous if and only if the toric ideal I_{L_Q} is homogeneous. Assuming Q to be homogeneous, the zero locus $V_Q := V_X(I_{L_Q}) \cap T_X$ in T_X of the toric ideal I_{L_Q} is a subgroup, by [11, Corollary 2.4] since we study over a finite field. The following consequence of Theorem 3.2 ensures that it coincides with the subgroup Y_Q if the condition $\mathcal{L} = \mathcal{L} : (q-1)$ holds, generalizing [9, Proposition 4.3] and [9, Corollary 4.4].

Theorem 3.10 (Finite Nullstellensatz) *If Q is homogeneous and $L = L_Q + (q-1)L_\beta$, then we have the following*

1. $V_Q = V_X(I_L)$,

2. $V_Q = Y_Q$, *if the condition* $\mathcal{L} = \mathcal{L} : (q-1)$ *holds,*

3. $I(V_X(I_L)) = I_L$, *if the condition* $\mathcal{L} = \mathcal{L} : (q-1)$ *holds.*

Proof Notice that $\mathbf{m} \in L \iff \mathbf{m} = \mathbf{m}_1 + \mathbf{m}_2$, for $\mathbf{m}_1 \in L_Q$ and $\mathbf{m}_2 \in (q-1)L_\beta$. It follows that

$$\mathbf{m} \in L \iff \mathbf{m}^+ = \mathbf{m}_1^+ + \mathbf{m}_2^+ + \mathbf{c} \text{ and } \mathbf{m}^- = \mathbf{m}_1^- + \mathbf{m}_2^- + \mathbf{c}, \text{ for some } \mathbf{c} \in \mathbb{N}^r.$$

Turning these vectors into monomials, we get the following relation

$$\mathbf{x}^{\mathbf{m}^+} - \mathbf{x}^{\mathbf{m}^-} = \mathbf{x}^{\mathbf{c}}[\mathbf{x}^{\mathbf{m}_2^+}(\mathbf{x}^{\mathbf{m}_1^+} - \mathbf{x}^{\mathbf{m}_1^-}) + \mathbf{x}^{\mathbf{m}_1^-}(\mathbf{x}^{\mathbf{m}_2^+} - \mathbf{x}^{\mathbf{m}_2^-})].$$

Hence, the ideal $I_L = I_{L_Q} + I_{(q-1)L_\beta}$. By Corollary 3.8, we also have $I_L = I_{L_Q} + I(T_X)$ so that $V_Q = V_X(I_L)$ establishing (1).

Take a point $[P] = [\mathbf{t}^{\mathbf{q}_1} : \cdots : \mathbf{t}^{\mathbf{q}_r}] \in Y_Q$. We have $(\mathbf{x}^{\mathbf{m}^+} - \mathbf{x}^{\mathbf{m}^-})(P) = \mathbf{t}^{Q\mathbf{m}^+} - \mathbf{t}^{Q\mathbf{m}^-} = 0$ whenever $\mathbf{m} \in L_Q$. So, we observe that $Y_Q \subseteq V_X(I_{L_Q})$. As Y_Q is a subgroup of T_X, it follows that $Y_Q \subseteq V_Q$. Taking ideals of both sides yields $I(V_Q) \subseteq I(Y_Q)$. As $V_Q = V_X(I_L)$ by (1) above, we finally have $I_L \subseteq I(V_Q) \subseteq I(Y_Q)$. Under the assumptions, $I(Y_Q) = I_L$ by Theorem 3.2, so the three ideals coincide in the last containment, verifying (3). By [11, Lemma 2.8], $\bar{Y}_Q = V_X(I(Y_Q))$ and $\bar{V}_Q = V_X(I(V_Q))$. As we work over a finite field, any set is closed with respect to Zariski topology and thus $Y_Q = V_Q$ proving (2). $\qquad\square$

There are examples for which $Y_Q \neq V_Q$, when the condition $\mathcal{L} = \mathcal{L} : (q-1)$ is broken.

Example 3.11 *Let $X = \mathcal{H}_2$ be the Hirzebruch surface over $\mathbb{F}_{11}$ and $Q = [1\ 2\ 3\ 4]$. Although Q is not homogeneous, we can remedy this by adjoining β and obtaining the homogeneous matrix $Q' = [Q\ \beta]^T$. Notice that $Y_Q = Y_{Q'}$ and so $I(Y_{Q'}) = \langle x_1^2 x_2 - x_4, x_1^5 - x_3^5 \rangle$, see Example 2.8 .*

By Theorem 3.10, we have $V_{Q'} = V_X(I_L)$ for the lattice $L = L_{Q'} + (q-1)L_\beta$. Since $L_{Q'} = \langle (2,1,0,-1) \rangle$ and $L_\beta = \langle (2,1,0,-1), (1,0,-1,0) \rangle$ we have $L = \langle (2,1,0,-1), (10,0,-10,0) \rangle$ and hence the ideal $I_L = \langle x_1^2 x_2 - x_4, x_1^{10} - x_3^{10} \rangle$. Applying [11, Algorithm 1], we obtain the matrix A below whose subgroup Y_A is precisely the zero locus $V_X(I_L)$ of the lattice ideal I_L:

$$A = \begin{bmatrix} -1 & 2 & -1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 10 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

We now apply one of the algorithms developed in the previous sections to conclude that

$$I(V_{Q'}) = I(V_X(I_L)) = I(Y_A) = I_L.$$

Therefore, $V_{Q'} \neq Y_{Q'}$ as otherwise, they would have the same vanishing ideals.

We close this section by discussing another special case where Q is diagonal.

Definition 3.12 *The toric set parameterized by a diagonal matrix is called a degenerate torus.*

Let η be a generator of the cyclic group $\mathbb{K}^*$, then for all $t_i \in \mathbb{K}^*$ we can write $t_i = \eta^{h_i}$ for some $0 \leq h_i \leq q - 2$. The following is the generalized version of the corresponding result in [7] valid for $X = \mathbb{P}^n$. The first proof is given in [11] and we give another here using Lemma 3.1.

Theorem 3.13 *Let $Q = diag(q_1, \ldots, q_r) \in M_{r \times r}(\mathbb{Z})$ and $D = diag(d_1, \ldots, d_r)$ where $d_i = |\eta^{q_i}|$. Then $I(Y_Q) = I_L$ for $L = D(L_{\beta D})$.*

Proof By Lemma 3.1, it is enough to show that $L = L_1$ where $L_1 = \{\mathbf{m} \in L_\beta : Q\mathbf{m} \equiv 0 \bmod (q-1)\}$. Let $\mathbf{m}$ be any element in L. Then $\mathbf{m} = D\mathbf{z}$ for some $\mathbf{z} \in \mathbb{Z}^r$ and $\mathbf{m} \in L_\beta$. Since $d_i = (q-1)/\gcd(q-1, q_i)$, $q_i d_i \equiv 0 \bmod (q-1)$ for all d_i. Therefore, $Q\mathbf{m} = QD\mathbf{z} \equiv 0 \bmod (q-1)$ and so, $\mathbf{m} \in L_1$.

Take $\mathbf{m} \in L_1$. Then $Q\mathbf{m} \equiv 0 \bmod (q-1)$, that is, for every $1 \leq i \leq r$ there exist $z_i \in \mathbb{Z}$ such that $q_i m_i = (q-1)z_i$. Hence,

$$\frac{q_i}{\gcd(q-1, q_i)} m_i = \frac{q-1}{\gcd(q-1, q_i)} z_i = d_i z_i.$$

Since $q_i/\gcd(q-1,q_i)$ and $q-1/\gcd(q-1,q_i)$ are coprime, it follows that d_i divides m_i. Therefore, $m_i = d_i z'_i$ for some $z'_i \in \mathbb{Z}$ and so, $\mathbf{m} = D\mathbf{z}'$ for $\mathbf{z}' = (z'_1, \ldots, z'_r)$. Hence, $\mathbf{m} \in L$. $\qquad\qquad\square$

Acknowledgment

References

[1] Alon N. Combinatorial Nullstellensatz. Combinatorics, Probability and Computing 1999; 8 (1-2): 7-29.

[2] Baran E, Şahin M. On parameterized toric codes. Applicable Algebra in Engineering, Communication and Computing 2021. doi: 10.1007/s00200-021-00513-8

[3] Cox DA, Little J, Schenck H. Toric Varieties. Graduate Studies in Mathematics, 124, Providence, RI, USA: American Mathematical Society, 2011.

[4] Cox DA, Little J, O'Shea D. Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra. New York, NY, USA: Springer Verlag, 1997.

[5] Dias E, Neves J. Codes over a weighted torus. Finite Fields and Their Applications 2015; 33: 66-79.

[6] Eisenbud D, Grayson DR, Stillman M, Sturmfels B. Computations in Algebraic Geometry with Macaulay 2. Algorithms and Computation in Mathematics, 8, Berlin, Germany: Springer Verlag, 2002.

[7] Lopez HH, Villarreal RH, Zarate L. Complete Intersection Vanishing Ideals on Degenerate Tori over Finite Fields. Arabian Journal of Mathematics 2013; 2 (2): 189-197.

[8] Miller E, Sturmfels B. Combinatorial commutative algebra, Graduate Texts in Mathematics, 227, New York, NY, USA: Springer-Verlag, 2005.

[9] Renteria C, Simis A, Villarreal RH. Algebraic methods for parameterized codes and invariants of vanishing ideals over finite fields. Finite Fields and Their Applications 2011; 17 (1): 81-104.

[10] Sarmiento E, Vaz-Pinto M, Villarreal RH. On the Vanishing ideal of an algebraic toric set and its parameterized linear codes. Journal of Algebra and its Applications 2012; 11 (4): 1250072.

[11] Şahin M. Toric codes and lattice ideals. Finite Fields and Their Applications 2018; 52: 243-260.

[12] Şahin M, Soprunov I. Multigraded Hilbert functions and toric complete intersection codes. Journal of Algebra 2016; 459: 446-467.

[13] Tochimani A, Villarreal RH. Vanishing ideals over finite fields. Mathematical Notes 2019; 105 (3): 429-438.