RATIONAL POINTS OF LATTICE IDEALS ON A TORIC VARIETY AND TORIC CODES

MESUT S¸AH˙IN

Abstract. We show that the number of rational points of a subgroup inside a toric variety over a finite field defined by a homogeneous lattice ideal can be computed via Smith normal form of the matrix whose columns constitute a basis of the lattice. This generalizes and yields a concise toric geometric proof of the same fact proven purely algebraically by Lopez and Villarreal for the case of a projective space and a standard homogeneous lattice ideal of dimension one. We also prove a Nullstellensatz type theorem over a finite field establishing a one to one correspondence between subgroups of the dense split torus and certain homogeneous lattice ideals. As application, we compute the main parameters of generalized toric codes on subgroups of the torus of Hirzebruch surfaces, generalizing the existing literature.

1. Introduction

Let $\Sigma$ be a complete simplicial fan with rays generated by the lattice vectors $v_1, \ldots, v_r \in \mathbb{Z}^n$. Each cone $\sigma \in \Sigma$ defines an affine toric variety $U_{\sigma}$ over a field $K$ whose ring of regular functions is the semigroup ring $K[\sigma \cap \mathbb{Z}^n]$. Gluing these affine pieces in a standard way, we obtain the split toric variety $X_\Sigma$ as an abstract variety over $K$. The Cox ring $S = K[x_1, \ldots, x_r]$ of $X_\Sigma$ is graded naturally by the group $\text{Cl} X_\Sigma$, i.e. we have the decomposition $S = \bigoplus_{\alpha \in \text{Cl} X_\Sigma} S_\alpha$, where $S_\alpha$ is the $K$-vector space spanned by the monomials of degree $\alpha$.

By a celebrated result due to Cox in [6], $K$-rational points of a toric variety $X := X_\Sigma$ over an algebraic closure $\overline{K}$ of $K$, is identified with the orbits in the Geometric Invariant Theory quotient $[\overline{K} \setminus V(B)]/G$, see Section 2 for details. It follows that the $K$-rational points $X(\overline{K})$ of $X$ can have representatives with coordinates in $\overline{K}$. Thus, we can study $K$-rational points of a subvariety of $X$ cut out by a $\text{Cl} X_\Sigma$-graded (or simply homogeneous) ideal $J$ using this correspondence:

$$V_{X(\overline{K})}(J) = \{ [P] \in [\overline{K}^r \setminus V(B)]/G : F(P) = 0, \text{ for any homogeneous } F \in J \}.$$ 

Our main motivation comes from immediate applications to error-correcting codes defined on toric varieties over a finite field $K = \mathbb{F}_q$. In this regard, we assume that the class group $\text{Cl} X_\Sigma$ is free throughout, which does not harm the generality, as the codes on a singular toric variety survive when the singularity is resolved and smooth complete toric varieties have a torsion-free class group, by [7, Proposition 4.2.5].

2020 Mathematics Subject Classification. Primary 14M25; 14G05 ; Secondary 94B27 ; 11T71.

The author is supported by TUBITAK Project No:119F177.
For any $\alpha$ and any subset $Y = \{[P_1], \ldots, [P_N]\}$ consisting of some $\mathbb{F}_q$-rational points of $X$, we have the following evaluation map for $K = \mathbb{F}_q$:

\begin{equation}
\text{ev}_Y : S_\alpha \to \mathbb{K}^N, \quad F \mapsto (F(P_1), \ldots, F(P_N)).
\end{equation}

The image $C_{\alpha,Y} = \text{ev}_Y(S_\alpha)$ is a linear code, called a generalized toric code. The three basic parameters of $C_{\alpha,Y}$ are block-length which is $N$, the dimension which is $K = \dim_{\mathbb{F}_q}(C_{\alpha,Y})$, and the minimum distance $\delta = \delta(C_{\alpha,Y})$ which is the minimum of the numbers of nonzero components of nonzero vectors in $C_{\alpha,Y}$.

When $Y = T_X(\mathbb{F}_q)$ is the $\mathbb{F}_q$-rational points of the maximal torus of $X$ we get the classical toric code examined for the first time by Hansen in [12] and studied further in e.g. [16, 26, 3, 27, 18, 5] showcasing some champion codes. Although the block-length of $C_{\alpha,Y}$ equals $N = (q - 1)^n$ in this classical case, its computation depends on the way $Y$ is presented in the general case. For instance, if $Y = Y_Q$ is parameterised by the monomials whose power is a column of an integer matrix $Q$, then some algorithms are given for computing the length $N = |Y|$, see [25, 1]. The vanishing ideal $I(Y) \subseteq S$ of $Y$, which is generated by homogeneous polynomials vanishing on $Y$, is relevant in the computation of the other parameters as well.

Namely, the kernel of $\text{ev}_Y$ is just the subspace $I_q(Y) := I(Y) \cap S_\alpha$, and hence the dimension $K = \dim_{\mathbb{F}_q}(C_{\alpha,Y})$ is the value $H_Y(\alpha) := \dim_{\mathbb{F}_q} S_\alpha - \dim_{\mathbb{F}_q} I_q(Y)$ of the multigraded Hilbert function $H_Y$ of $Y$, see [29]. The minimum distance function of $I(Y)$ is introduced and is related to the minimum distance of $C_{\alpha,Y}$ in [21] for the case of the projective space $X = \mathbb{P}^n$. The ideal $I(Y_Q)$ is a lattice ideal $I_L$ for a unique lattice $L \subseteq \mathbb{Z}^r$ of rank $r$ as shown in [25, 8, 1]. Moreover, every subgroup of $T_X(\mathbb{F}_q)$ is not only of the form $Y_Q$ but also is the common zeroes $V_{X(\mathbb{F}_q)}(I_L)$ of binomials generating a lattice ideal $I_L$, see [28, Section 3].

The present paper aims mainly to develop methods for computing parameters of generalized toric codes $C_{\alpha,Y}$ from subgroups $Y = V_{X(\mathbb{F}_q)}(I_L)$ of $T_X$. Before we state our main results, we need to introduce a little more notation.

Let $B$ be an $r \times n$ matrix whose columns constitute a basis for $L$; let $A$ and $C$ be unimodular matrices of sizes $r$ and $n$, respectively, so that

$$D = ABC = [d_1e_1| \cdots | d_ne_n]$$

is the Smith-Normal form of $B$, where $e_1, \ldots, e_n \in \mathbb{Z}^r$. These $d_i$’s are known as the invariant factors having the property that $d_i$ divides $d_{i+1}$ for each $i \in [n - 1] := \{1, \ldots, n - 1\}$ and that the order of the torsion part $T(\mathbb{Z}^r/L)$ of the group $\mathbb{Z}^r/L$ is $d_1 \cdots d_n$, by the fundamental structure theorem for finitely generated abelian groups, see [14, pp. 187—188].

We first observe in Proposition 3.3 that the common solutions $V_{X(\mathbb{K})}(I_L)$ of polynomials in $I_L$ lie in the torus $T_X$, for any field $\mathbb{K}$.

Then, we count characters to see the number of $\mathbb{K}$-rational points is finite: $|V_{X(\mathbb{K})}(I_L)| \leq d_1 \cdots d_n$. Furthermore, it meets this upper bound if and only if $\mathbb{K}$ has all the $d_i$-th roots of unity, for every $i \in [n]$, see Theorem 3.7.

Let $Y$ be a subgroup of $T_X(\mathbb{F}_q)$. Then, $I(Y) = I_L$ for a unique lattice $L$ with $(q - 1)L_\beta \subseteq L \subseteq L_\beta$, see Lemma 4.2. Moreover, the number of $\mathbb{F}_q$-rational points in $Y$ is given in Theorem 4.4 by

$$|Y| = |V_{X(\mathbb{F}_q)}(I_L)| = |L_\beta/L| = d_1 \cdots d_n.$$
Furthermore, we observe that the set $V_{X(\mathbb{F}_q)}(I_L)$ of $\mathbb{F}_q$-rational points coincide with the set of $\mathbb{F}_q$-rational points $V_X(I_L) := V_{X(\mathbb{F}_q)}(I_L)$ in Lemma 5.1 for lattices with $(q - 1)L_\beta \subseteq L \subseteq L_\beta$. As a consequence, we also prove a Nullstellensatz type result over the finite field $\mathbb{F}_q$ saying that $I(V_X(I_L)) = I_L$ establishing a 1-1 correspondence between the subgroups $V_X(I_L)$ and the lattice ideals $I_L$, where $(q - 1)L_\beta \subseteq L \subseteq L_\beta$, see Theorem 5.2. This result will eliminate the need for an algorithm to compute the vanishing ideal of the subgroup $V_X(I_L)$, which will save time in search of codes with good parameters. In literature, Nullstellensatz type results over finite fields have been obtained (see [10] for a nice survey) and used effectively for computing the basic parameters of evaluation codes on subvarieties of affine and projective spaces, see [15, Theorems 3.12, 3.13] and [25, Corollary 4.4].

If $I_L$ is a homogeneous ideal of dimension $d = r - n$, then its degree is just the constant Hilbert polynomial, which is computed to be $\deg(I_L) = |L_\beta/L| = d_1 \cdots d_n$, in Theorem 6.3, generalizing the nice result [19, Theorem 3.13]. This will be nothing but the mixed volume of the Newton polytopes of binomials generating $I_L$ by Corollary 6.5. It is worth to mention [24, Theorem 4.6] also generalizing [19, Theorem 3.13] and giving a nice formula for the degree of $I_L$, when $X$ is an affine space and $L$ is an arbitrary lattice, see also [30, Theorem 9.4.2].

Finally, we uncover the structure and give two descriptions for the points of the subgroup cut out by the lattice ideal $I_L$. More precisely, we have

$$V_{X(\mathbb{F}_q)}(I_L) = \langle \{P_i\} \rangle \times \cdots \times \langle \{P_n\} \rangle,$$

for the point $[P_i] = [\eta_t^{\alpha_{i1}} \cdots \eta_t^{\alpha_{ir}}]$, where $\eta_t$ is a primitive $d_i$-th root of unity in $\mathbb{K}$, for each $i \in [n]$. In addition,

$$V_{X(\mathbb{F}_q)}(I_L) = Y_Q = \{[t^{\eta_1^{q_1}} \cdots t^{\eta_r^{q_r}}] | t \in (\mathbb{F}_q^*)^n\}$$

is parameterized by the columns of the matrix $Q = [\mathbf{q}_1 \mathbf{q}_2 \cdots \mathbf{q}_r]$, whose $i$-th row is $(q - 1)/d_i$ times the $i$-th row of the matrix $A$, see Theorem 7.1.

As application, we compute the main parameters of generalized toric codes on subgroups of the torus of Hirzebruch surfaces, generalizing the existing literature, see Theorem 8.4. The parameterization above is especially useful in computing the minimum distance.

2. PRELIMINARIES

In this section we fix our notation and recall standard facts from toric geometry relying on the most recent wonderful book [7], although there are other well known excellent books.

Let $\Sigma$ be a complete simplicial fan with rays generated by the lattice vectors $\mathbf{v}_1, \ldots, \mathbf{v}_r \in \mathbb{R}^n$. The fan gives the following short exact sequence:

$$\mathbb{P} : 0 \longrightarrow \mathbb{Z}^n \overset{\phi}{\longrightarrow} \mathbb{Z}^r \overset{\beta}{\longrightarrow} \mathbb{Z}^d \longrightarrow 0,$$

where $\phi$ denotes the matrix $[\mathbf{v}_1 \cdots \mathbf{v}_r]^T$ and $d = r - n$ is the rank of the class group $\text{ClX}$ of $X := X_\Sigma$. Denote by $L_\beta$ the key sublattice of $\mathbb{Z}^r$ which is isomorphic to $\mathbb{Z}^n$ via $\phi$, whose basis is given by the columns $\mathbf{u}_1, \ldots, \mathbf{u}_n$ of $\phi$.

The homogeneous coordinate ring $\mathbb{K}[x_1, \ldots, x_r]$ of the toric variety $X$ over $\mathbb{K}$ is graded naturally by the columns of the matrix $\beta$ via $\deg(x_j) = \beta_j$, for each $j \in [r]$. A polynomial whose monomials $x_1^{{\alpha}_1} \cdots x_r^{{\alpha}_r}$ have the same degree $\alpha = a_1\beta_1 + \cdots + a_r\beta_r$ is called $\beta$-graded, $L_\beta$-homogeneous or just homogeneous when
there is no harm of confusion. We are interested in sublattices $L$ of $L_\beta$ and the $L_\beta$-homogeneous lattice ideals they define in the Cox ring $\mathbb{K}[x_1, \ldots, x_r]$ of $X(\mathbb{K})$:

$$I_L = \langle x^{m^+} - x^{m^-} | m = m^+ - m^- \in L \rangle.$$  

Applying Hom$(-, \mathbb{K}^r)$ functor to $\mathfrak{P}$ we get the following dual short exact sequence since $\mathbb{K}^r$ is divisible:

$$(2.2) \quad \mathfrak{P}^* : 1 \longrightarrow G \xrightarrow{i} (\mathbb{K}^r)_r \xrightarrow{\pi} (\mathbb{K}^r)^n \longrightarrow 1,$$

where $\pi : P \mapsto (x^{u_1}(P), \ldots, x^{u_n}(P))$ is expressed using the notation $x^n(P) = p_1^{e_1} \cdots p_n^{e_n}$ for $P = (p_1, \ldots, p_r) \in (\mathbb{K}^r)^r$ and for $a = (a_1, \ldots, a_r) \in \mathbb{Z}^r$.

Notice also that the algebraic group $G = \text{ker}(\pi)$ is the zero locus in $(\mathbb{K}^r)^r$ of the toric (prime lattice) ideal $I_{L_\beta}$:

$$V(I_{L_\beta}) \cap (\mathbb{K}^r)^r : = \{ P \in (\mathbb{K}^r)^r | (x^{m^+} - x^{m^-})(P) = 0 \text{ for all } m \in L_\beta \}$$

$$= \{ P \in (\mathbb{K}^r)^r | x^n(P) = 1 \text{ for all } m \in L_\beta \},$$

where $V(J)$ denotes the usual affine subvariety of $\mathbb{K}^r$ cut out by the ideal $J$.

As proved by Cox in [6], when $\mathbb{K}$ is an algebraic closure of $\mathbb{K}$, the toric variety $X$ over $\mathbb{K}$, is isomorphic to the geometric quotient $(\mathbb{K}^r \setminus V(B))/G$, where $B$ is the monomial ideal in $\mathbb{K}[x_1, \ldots, x_r]$ generated by the monomials $x^a = \prod_{\sigma \in \Sigma} x_{\sigma}$ corresponding to cones $\sigma \in \Sigma$.

Hence, $\mathbb{K}$-rational points $X(\mathbb{K})$ are orbits $[P] := G \cdot P$, for $P \in \mathbb{K}^r \setminus V(B)$. By (2.2), we have $T_X = (\mathbb{K}^r)^r/G$ and since the toric variety is split we have $T_X(\mathbb{K}) \cong (\mathbb{K}^r)^n$.

By resolving the singularity, if needed, we may assume without loss of generality that there is at least one smooth cone $\sigma \in \Sigma$. Hence, the first $n$ rows of the matrix $\phi$ in (2.1) are $v_1 = e_1, \ldots, v_n = e_n$. Thus, the map $\pi$ in (2.2) becomes

$$\pi(x_1, \ldots, x_r) = (x_1 x^{u_1-e_1}, \ldots, x_n x^{u_n-e_n}).$$

Hence, given $(t_1, \ldots, t_n) \in (\mathbb{K}^r)^n$, solving $x_i x^{u_n-e_n} = t_i$, we get

$$x_i = t_i x^{u_n-e_n} = t_i x_{n+1} x_{n+1} \cdots x_{n+i}, \text{ for all } i \in [n].$$

As a result, the set $\pi^{-1}(t_1, \ldots, t_n)$ consists of the points

$$(2.3) \quad \{(t_1 \lambda_1^{-u_{n+1}} \cdots \lambda_d^{-u_1}, \ldots, t_n \lambda_1^{-u_{n+1}} \cdots \lambda_d^{-u_1}, \lambda_1, \ldots, \lambda_d) : \lambda_1 \in \mathbb{K}^r \}.$$

for $(\lambda_1, \ldots, \lambda_d) = (x_{n+1}, \ldots, x_r) \in (\mathbb{K}^r)^d$, yielding the parameterization:

$$G = \{(\lambda_1^{-u_{n+1}} \cdots \lambda_d^{-u_1}, \ldots, \lambda_1^{-u_{n+1}} \cdots \lambda_d^{-u_1}, \lambda_1, \ldots, \lambda_d) : \lambda_1 \in \mathbb{K}^r \}.$$

When $(t_1, \ldots, t_n) \in (\mathbb{K}^r)^n$, there is a point $P = (t_1, \ldots, t_n, 1, \ldots, 1) \in (\mathbb{K}^r)^r$ with $\pi(P) = (t_1, \ldots, t_n)$. Therefore, points of $T_X(\mathbb{K}) = (\mathbb{K}^r)^r/G$ have representatives with components from $\mathbb{K}^r$. Furthermore, equivalence of two points $(x_1, \ldots, x_r, x_1', \ldots, x_r') \in (\mathbb{K}^r)^r$ with respect to the action of $G$ and that of $G(\mathbb{K})$ are the same. This is because, when $G \cdot (x_1, \ldots, x_r) = G \cdot (x_1', \ldots, x_r')$, there is a point $g_1, \ldots, g_r) \in G \subset (\mathbb{K}^r)^r$ with $x_i = g_i x'_i$ for all $i \in [r]$. In particular, we have $x_{n+i} = \lambda_i x_{n+i}$ forcing $\lambda_i = x_{n+i} x_{n+i}' \in \mathbb{K}$, for all $i \in [d]$.

For an $L_\beta$-graded ideal $J$, we introduce the subvariety of the toric variety $X$ defined by $J$ as follows

$$V_X(J) = \{ [P] \in X(\mathbb{K}) : F(P) = 0, \text{ for any homogeneous } F \in J \}.$$
Its $\mathbb{K}$-rational points form the subset
\[ V_X(\mathbb{K})(J) = \{ [P] \in X(\mathbb{K}) : F(P) = 0, \text{ for any homogeneous } F \in J \}. \]
Therefore, any point $[P] \in V_X(\mathbb{K})(J)$ is an equivalence class $G \cdot P$ of a point $P$ from $V(J) \setminus V(B) \subseteq \mathbb{K}^r \setminus V(B)$, for the subgroup $G \subset (\mathbb{K}^*)^r$.

As the elements of the algebraic torus $(\mathbb{K}^*)^r$ in $\mathbb{P}^*$ are already identified with the characters $\rho : \mathbb{Z}^r \to \mathbb{K}$ and $T_X(\mathbb{K}) = (\mathbb{K}^*)^r/G$, we take the approach to investigate characters $\rho : \mathbb{Z}^r \to \mathbb{K}^*$ in order to compute the number of $\mathbb{K}$-rational points of the lattice ideal $I_L$ on the toric variety $X$.

3. SUBGROUPS DEFINED BY LATTICE IDEALS OVER ANY FIELD

In this section, we study subgroups of the torus $T_X$ defined by lattice ideals $I_L$ inside $\mathbb{K}[x_1, \ldots, x_r]$, which is an $L_\beta$-graded ring via $\deg(x_i) = \beta_i$, where $\beta_i$ is the $i$-th column of the matrix $\beta$ in (2.1) and $L$ is a sublattice of $L_\beta$.

First of all, $\text{rank } L_\beta = n$ since $L_\beta$ is isomorphic to $\mathbb{Z}^n$ via the map $\phi$ in the sequence $\mathbb{P}$ in (2.1). On the other hand, it is well-known that $\dim J = r - \text{height}(J)$, where $\dim J$ is the Krull dimension of the quotient ring $\mathbb{K}[x_1, \ldots, x_r]/J$. So, we have
\[ \text{rank } L = n = \text{height}(I_L) \iff \dim I_L = d = r - n. \]

As the vanishing ideals of subgroups of the torus $T_X$ are $L_\beta$-homogeneous lattice ideals of Krull-dimension $d$ by [28, Proposition 2.6], and $I_L$ is $L_\beta$-homogeneous if and only if $L \subseteq L_\beta$ by [28, Proposition 2.3], we focus on lattices $L$ satisfying $L \subseteq L_\beta$ and $\text{rank } L = n$.

**Lemma 3.1.** Let $L \subseteq L_\beta$ and $\text{rank } L = n$. Then, $\ell L_\beta \subseteq L$ for the order $\ell = |L_\beta/L|$.

**Proof.** Since $L_\beta/L$ is a finite group of order $\ell$, we have $\ell (m + L) = L$, for every $m \in L_\beta$. This means that $\ell m \in L$ for all $m \in L_\beta$. \hfill \Box

**Lemma 3.2.** $L \subseteq L'$ if and only if $I_L \subseteq I_{L'}$.

**Proof.** $(\Rightarrow)$ If $L \subseteq L'$, then every $m \in L$ lies in $L'$. Therefore, every binomial generator $x^{m^+} - x^{m^-}$ of $I_L$ lies in $I_{L'}$. So, $I_L \subseteq I_{L'}$.

$(\Leftarrow)$ Assume that $I_L \subseteq I_{L'}$ and $m \in L$. Then, the binomial $x^{m^+} - x^{m^-}$ of $I_L$ lies in $I_{L'}$. It follows from [19, Lemma 3.2] that $m \in L'$. \hfill \Box

**Proposition 3.3.** Let $L \subseteq L_\beta$ and $\text{rank } L = n$. Then, $V_X(\mathbb{K})(I_L)$ is a subgroup of $T_X(\mathbb{K})$.

**Proof.** By Lemma 3.1, we have $\ell L_\beta \subseteq L \subseteq L_\beta$ for the order $\ell = |L_\beta/L|$. As smaller lattices correspond to smaller lattice ideals by Lemma 3.2, it follows that $I_{\ell L_\beta} \subseteq I_L \subseteq I_{L_\beta}$. Thus, we have the inclusions below:
\[ \{ [1] \} = V_X(\mathbb{K})(I_{L_\beta}) \subseteq V_X(\mathbb{K})(I_L) \subseteq V_X(\mathbb{K})(I_{\ell L_\beta}), \]
where $[1]$ denotes the orbit of the point $(1, \ldots, 1) \in \mathbb{K}^r \setminus V(B)$. So as to prove that $V_X(\mathbb{K})(I_L)$ is a subset of the torus $T_X(\mathbb{K})$, it suffices to reveal that $V_X(\mathbb{K})(I_{\ell L_\beta}) \subseteq T_X(\mathbb{K})$. Given any point $[P] \in V_X(\mathbb{K})(I_{\ell L_\beta})$, we have $P \in V(I_{\ell L_\beta}) \setminus V(B)$. By definition, $P \in V(I_{\ell L_\beta})$ exactly when $x^{m^+}(P) = x^{m^-}(P)$ for all $m = m^+ - m^- \in L_\beta$. Since $x^{m^+}(P) = x^{m^-}(P^\ell)$ is equivalent to $x^{m^+}(P^\ell) = x^{m^-}(P^\ell)$, it follows that $P \in V(I_{\ell L_\beta})$ if and only if $P^\ell \in V(I_{L_\beta})$. As $B$ is a monomial ideal, $P \notin V(B)$ if and only if $P^\ell \notin V(B)$. Thus, $P \in V(I_{\ell L_\beta}) \setminus V(B)$ implies that $P^\ell \in V(I_{L_\beta}) \setminus V(B) = G$. 


As $G$ lies in the torus $(\mathbb{K}^*)^r$, we have $P \in (\mathbb{K}^*)^r$ yielding $[P] \in T_X(\mathbb{K})$. Hence, $V_{X(\mathbb{K})}(I_L) \subseteq T_X(\mathbb{K})$.

If $[P], [Q] \in V_{X(\mathbb{K})}(I_L)$, then we have the following:

$$x^{m^+} (P \cdot Q^{-1}) = x^{m^+} (P)x^{m^+} (Q)^{-1} = x^{m^+} (P)x^{m^+} (Q)^{-1} = x^{m^+} (P \cdot Q^{-1}).$$

Thus, $[P] \cdot [Q]^{-1}$ lies in $V_{X(\mathbb{K})}(I_L)$ demonstrating that it is indeed a subgroup. □

**Remark 3.4.** It is easy to see that $V_X(I_L) \cap T_X$ is a subgroup of $T_X$, when we only have $L \subseteq L_{\beta}$, see also [28, Corollary 2.4]. But, if rank $L < n$, then $V_X(I_L)$ need not lie inside the torus $T_X$, see [28, Example 3.6].

For any $m = m^+ - m^- \in L$, the binomial $x^{m^+} - x^{m^-} \in I_L$, hence we have $x^{m^+} (P) = x^{m^+} (P)$ for a point $[P] \in V_{X(\mathbb{K})}(I_L)$. If we further assume that $L \subseteq L_{\beta}$ and rank $L = n$, then $x^{m}(P) = 1$ as $V_{X(\mathbb{K})}(I_L) \subseteq T_X(\mathbb{K})$. Therefore, a point $[P] \in V_{X(\mathbb{K})}(I_L)$, defines a character $\chi_P : L_{\beta}/L \rightarrow \mathbb{K}^*$ via

$$\chi_P(m + L) := x^m(P) = p_1^{m_1} \cdots p_r^{m_r},$$

for all $m = (m_1, \ldots, m_r) \in L$ under these circumstances.

**Lemma 3.5.** Let $L \subseteq L_{\beta}$ and rank $L = n$. Then the groups $V_{X(\mathbb{K})}(I_L)$ and $\text{Hom}(L_{\beta}/L, \mathbb{K}^*)$ are isomorphic.

**Proof.** Let $\psi : V_{X(\mathbb{K})}(I_L) \rightarrow \text{Hom}(L_{\beta}/L, \mathbb{K}^*)$ be defined by $[P] \rightarrow \chi_P$.

- The map $\psi$ is well-defined, for if $g \in G = V(I_{L_{\beta}}) \cap (\mathbb{K}^*)^r$, then $\chi_{gP} = \chi_P$, since for all $m \in L_{\beta}$, we have

$$x^m(gP) = g^mx^m(P) = x^m(P).$$

- $\psi$ is a homomorphism, since $\chi_{P \cdot P'} = \chi_P \cdot \chi_{P'}$.
- It is injective, as $\chi_P(m + L) = x^m(P) = 1$, for all $m \in L_{\beta}$, implies that $P \in G$ that is $[P] = [1]$.
- It is surjective, as we prove now. Let $\{u_1, \ldots, u_n\}$ be the $\mathbb{Z}$-basis for the lattice $L_{\beta}$. For a given $\chi : L_{\beta}/L \rightarrow \mathbb{K}^*$, let $t_i = \chi(u_i + L)$ for each $i \in [n]$.

Every element $m \in L_{\beta}$ is written as $m = c_1u_1 + \cdots + c_nu_n$ for some $(c_1, \ldots, c_n) \in \mathbb{Z}^n$. Thus, we have

$$\chi(m + L) = t_1^{c_1} \cdots t_n^{c_n} = (x^{u_1}(P))^{c_1} \cdots (x^{u_n}(P))^{c_n} = \chi_P(m + L).$$

If $m \in L$, then it follows that $x^m(P) = \chi(m + L) = 1$ for all $m \in L$ and so $[P] \in V_X(I_L)$. Hence, we have $\chi = \chi_P$.

These complete the proof. □

**Lemma 3.6.** Let $L \subseteq L_{\beta}$ and rank $L = n$. If $d_i$ is an invariant factor of the group $L_{\beta}/L$ and $C_i := \{c \in \mathbb{K}^* : c^{d_i} = 1\}$ is the group of $d_i$-th roots of unity lying inside $\mathbb{K}$, for each $i \in [n]$, then the groups $\text{Hom}(L_{\beta}/L, \mathbb{K}^*)$ and $C_1 \times \cdots \times C_n$ are isomorphic.

**Proof.** Let $\{m_1, \ldots, m_n\}$ be a $\mathbb{Z}$-basis for the lattice $L_{\beta}$ such that

$$\{d_1m_1, \ldots, d_nm_n\}$$

is a $\mathbb{Z}$-basis of $L$. 
We regard elements in Hom($L_\beta/L, K^*$) as (partial) characters $\rho : L_\beta \to K^*$ whose restriction to $L$ is the identity $1_L$. So, we have $\rho(m_i)^{d_i} = \rho(d_im_i) = 1$, for each $i \in [n]$. Since $\rho$ is determined by the values $\rho(m_1), \ldots, \rho(m_n)$, the map $\Theta : \text{Hom}(L_\beta/L, K^*) \to C_1 \times \cdots \times C_n$, defined by $\Theta(\rho) = (\rho(m_1), \ldots, \rho(m_n))$ is well-defined.

- $\Theta$ is a homomorphism as $\Theta(\rho \circ \rho') = \Theta(\rho) \cdot \Theta(\rho')$.
- $\Theta$ is injective, since $\Theta(\rho) = (\rho(m_1), \ldots, \rho(m_n)) = (1, \ldots, 1) \implies \rho = 1_{L_\beta}$.
- $\Theta$ is surjective as we demonstrate below.

Every choice of $(c_1, \ldots, c_n) \in C_1 \times \cdots \times C_n$ determines an element

$$\rho : L_\beta \to K^* \quad \text{via} \quad \rho(k_1m_1 + \cdots + k_nm_n) = c_1^{k_1} \cdots c_n^{k_n}.$$ 

Furthermore, if $m = k_1m_1 + \cdots + k_nm_n \in L$ then $d_i$ divides $k_i$ for all $i$ and thus $\rho(m) = 1$, as $c_1^{k_1} = \cdots = c_n^{k_n} = 1$. Hence, $\rho \in \text{Hom}(L_\beta/L, K^*)$.

Thus, $\Theta$ is the required isomorphism, completing the proof. \hfill $\square$

**Theorem 3.7.** Let $L \subseteq L_\beta$ and rank $L = n$. If $d_i$ is an invariant factor of the group $L_\beta/L$ and $C_i := \{ c \in K^* : c^{d_i} = 1 \}$ is the group of $d_i$-th roots of unity lying inside $K$, for each $i \in [n]$, then $V_{X(K)}(I_L) \cong C_1 \times \cdots \times C_n$, and thus the number of $K$-rational points $|V_{X(K)}(I_L)|$ is $|C_1| \cdots |C_n| = d_1 \cdots d_n$. Moreover, $|V_{X(K)}(I_L)| = d_1 \cdots d_n \iff K$ has all the $d_i$-th roots of unity, for every $i \in [n]$.

**Proof.** It follows from Lemma 3.5 that $V_{X(K)}(I_L) \cong \text{Hom}(L_\beta/L, K^*)$. We also have $\text{Hom}(L_\beta/L, K^*) \cong C_1 \times \cdots \times C_n$ by Lemma 3.6, whence $V_{X(K)}(I_L) \cong C_1 \times \cdots \times C_n$.

Since $|C_i| \leq d_i$ in general, we have $|V_{X(I_L)}| = |C_1| \cdots |C_n| \leq d_1 \cdots d_n$.

The second part follows, since $|C_i| = d_i \iff K$ has all the $d_i$-th roots of unity, for every $i \in [n]$. \hfill $\square$

### 4. Subgroups defined by lattice ideals over a finite field

In this section, we compute the number of $F_q$-rational points of a subgroup of the algebraic group $T_X$, where $X$ is a toric variety over the finite field $F_q$. By the virtue of Theorem 3.7, this amounts to computing the order of the cyclic subgroup $C_i$ of $d_i$-th roots of unity lying inside the cyclic group $F_q^*$ of order $q - 1$.

**Theorem 4.1.** If $L \subseteq L_\beta$ and rank $L = n$, then the number of $F_q$-rational points is given by $|V_{X(F_q)}(I_L)| = (d_1, q - 1) \cdots (d_n, q - 1)$, where $(d_i, q - 1)$ is the greatest common divisor of $q - 1$ with the invariant factor $d_i$.

**Proof.** Fix $i \in [n]$. Recall that $C_i = \{ c \in K^* : c^{d_i} = 1 \}$ is a cyclic subgroup of $F_q^*$ of order $|C_i|$, and so $|C_i|$ divides $q - 1$. The order $|C_i|$ of a generator of $C_i$ divides $d_i$, as well. Hence, $|C_i|$ divides $(d_i, q - 1)$. On the other hand, as $(d_i, q - 1)$ divides $q - 1$, there is a cyclic subgroup of $F_q^*$ of order $(d_i, q - 1)$, which is clearly contained in $C_i$, since $(d_i, q - 1)$ divides $d_i$. Therefore, $|C_i| = (d_i, q - 1)$.

The proof now follows directly from Theorem 3.7. \hfill $\square$

Before going further, let us single out lattices corresponding to subgroups of $T_X$.

**Lemma 4.2.** If $Y$ is a subgroup of $T_X(F_q)$ then $I(Y) = I_L$ for a unique lattice $L$ with $(q - 1)L_\beta \subseteq L \subseteq L_\beta$. Therefore, subgroups of $T_X(F_q)$ are of the form $V_{X(F_q)}(I_L)$ for lattices with $(q - 1)L_\beta \subseteq L \subseteq L_\beta$. 

Proof. By [28, Theorem 2.9] \( I(Y) = I_L \) for a unique lattice \( L \) with \( L \subseteq L_\beta \). Since \( Y \subseteq T_X(\mathbb{F}_q) \) implies \( I(T_X(\mathbb{F}_q)) \subseteq I(Y) \) and we have \( I(T_X(\mathbb{F}_q)) = I_{(q-1)L_\beta} \) by [28, Corollary 4.14 (ii)], the first claim follows from Lemma 3.2.

If \( Y \) is a subgroup of \( T_X(\mathbb{F}_q) \), then \( Y = V_X(\mathbb{F}_q)(I(Y)) \) by [28, Lemma 2.8] which is nothing but \( V_X(\mathbb{F}_q)(I_L) \) by above for a unique lattice \( L \) with \((q-1)L_\beta \subseteq L \subseteq L_\beta \). \( \square \)

Therefore, in order to compute the order of a subgroup of the torus \( T_X(\mathbb{F}_q) \) of \( X \), it is enough to focus on lattices with \((q-1)L_\beta \subseteq L \subseteq L_\beta \).

**Lemma 4.3.** Let \( L \subseteq L_\beta \) and rank \( L = n \). Then, \((q-1)L_\beta \subseteq L \) if and only if \( \exp(L_\beta/L) = d_n \) divides \( q-1 \). Recall that the exponent \( \exp(H) \) of a finite group \( H \) is the least common multiple of the orders of all elements in \( H \).

**Proof.** Recall that \( L_\beta \) has a basis \( \{m_1, \ldots, m_n\} \) such that \( \{d_1m_1, \ldots, d_nm_n\} \) is a basis of \( L \), where \( d_i \)'s are the invariant factors of \( L_\beta/L \). By the structure theorem for finite abelian groups \( L_\beta/L \) and \( \mathbb{Z}d_1 \oplus \cdots \oplus \mathbb{Z}d_n \) are isomorphic. Since \( d_i \) divides \( d_{i+1} \) for each \( i \in [n-1] \), the exponent of \( L_\beta/L \) is \( d_n \).

Therefore, if \((q-1)L_\beta \subseteq L \), then \((q-1)m_i \in L \). Since \( \{d_1m_1, \ldots, d_nm_n\} \) is a basis of \( L \), it follows immediately that \( d_i \) divides \( q-1 \), for every \( i \in [n] \). Thus, \( \exp(L_\beta/L) \) divides \( q-1 \). Conversely, if the exponent divides \( q-1 \), then each \( d_i \) divides \( q-1 \), and hence \((q-1)m_i \in L \) yielding to the inclusion \((q-1)L_\beta \subseteq L \). \( \square \)

We are now ready to prove the main result of the section yielding to an efficient method to count the number of \( \mathbb{F}_q \)-rational points of the subgroup \( V_X(I_L) \) of \( T_X \) using a basis of \( L \).

**Theorem 4.4.** If \((q-1)L_\beta \subseteq L \subseteq L_\beta \), then the number of \( \mathbb{F}_q \)-rational points is given by 
\[
|V_X(\mathbb{F}_q)(I_L)| = \prod_{i=1}^n d_i.
\]

**Proof.** By Lemma 4.3, it follows that \( d_i \) divides \( q-1 \), and hence \((d_i, q-1) = d_i \), for every \( i \in [n] \). Therefore, \( |V_X(\mathbb{F}_q)(I_L)| = \prod_{i=1}^n d_i \), by Theorem 4.1. \( \square \)

**Remark 4.5.** Theorem 4.4 follows also from Lemma 3.5 together with a more general fact which is communicated in private to us by Laurence Barker: given a finite group \( A \) and a finite field \( \mathbb{F}_q \), \( \text{Hom}(A, \mathbb{F}_q^*) \) is isomorphic to \( A \) if and only if \( \exp(A) \) divides \( q-1 \). The proof provided by Barker is as follows.

The usual dual of \( A \), sometimes called the Pontryagin dual, is defined to be \( A^* = \text{Hom}(A, \mathbb{Q}/\mathbb{Z}) \). The group \( \mathbb{Q}/\mathbb{Z} \), is isomorphic to the torsion subgroup of \( \mathbb{C}^* \). So \( A^* \) can be identified with the group of irreducible complex characters of \( A \).

The standard result that \( A \) is non-canonically isomorphic to \( A^* \) is plain when \( A \) is cyclic. It is easy to see that \( (A_1 \times A_2)^* \cong A_1^* \times A_2^* \). So the general case follows by decomposing \( A \) as a direct product of cyclic groups.

Viewing finite cyclic groups as embedded in each other wherever possible, then \( \mathbb{Q}/\mathbb{Z} \) is the union of all those groups, in other words, the colimit of the diagram of embeddings. In particular, \( A^* \) can be identified with \( \text{Hom}(A, C) \) for any cyclic group \( C \) that is sufficiently large in the sense where \( C' \leq C \) provided \( |C'| \) divides \( |C| \). The exact criterion for \( C \) to be sufficiently large is that every homomorphism \( A \to \mathbb{Q}/\mathbb{Z} \) has image contained in the subgroup isomorphic to \( C \). That is equivalent to saying that the exponent of \( A \) divides \( |C| \). Taking \( C = \mathbb{F}_q^* \) completes the proof.

**Corollary 4.6.** If \((q-1)L_\beta \subseteq L \subseteq L_\beta \), then \( |V_X(\mathbb{F}_q)(I_L)| = |\det ML| \), where \( ML \) is the matrix with entries \( b_{ij} \in \mathbb{Z} \) such that the \( j \)-th basis element of \( L \) is written as \( b_1u_1 + \cdots + b_nu_n \) in terms of the basis \( \{u_1, \ldots, u_n\} \) of \( L_\beta \).
Thus, the class group is \( \mathbb{Z} \) be a subset of \( \mathbb{Z} \) and \( \mathbb{M} \) be a subset of \( \mathbb{Z} \) constituting a \( \mathbb{Z} \)-basis for the lattice \( \Lambda \). By abusing the notation, let us denote by \( \mathbb{M} \) the matrix whose columns are the elements of the set \( \mathbb{M} \).

It is known that the volume of the fundamental domain \( \Pi(\mathbb{M}) \) of \( \mathbb{M} \) is \( \det \mathbb{M} \), where

\[
\Pi(\mathbb{M}) := \left\{ \sum_{i=1}^{n} \lambda_i \mathbf{b}_i : 0 \leq \lambda_i < 1 \right\}.
\]

It is also known that \( \det \mathbb{M} \) is the number \( \#(\Pi(\mathbb{M}) \cap \mathbb{Z}^n) \) of lattice points inside \( \Pi(\mathbb{M}) \) as well as the index \( |\mathbb{Z}^n : \Lambda| = |\mathbb{Z}^n / \Lambda| \).

Altogether, we have \( |V_{X(\mathbb{F}_q)}(I_L)| = |L_\beta / L| = |\mathbb{Z}^n / \Lambda| = |\det \mathbb{M}|. \)

**Corollary 4.7.** If \( \{c_1 \mathbf{u}_1, \ldots, c_n \mathbf{u}_n\} \) constitute a basis for \( L \), for positive integers \( c_i \) dividing \( q - 1 \), then \( |V_{X(\mathbb{F}_q)}(I_L)| = c_1 \cdots c_n \).

**Proof.** Since \( \{\mathbf{u}_1, \ldots, \mathbf{u}_n\} \subseteq \mathbb{Z}^n \) form a basis of \( L_\beta \) and \( \phi(\mathbf{e}_i) = \mathbf{u}_i \), we observe that \( \phi(c_i \mathbf{e}_i) = c_i \mathbf{u}_i \) for all \( i \in [n] \). So, \( \mathbb{M} = \{c_1 \mathbf{e}_1, \ldots, c_n \mathbf{e}_n\} \) is a basis for the lattice \( \Lambda \) that appeared in the proof of Corollary 4.6 and \( |\det \mathbb{M}| = c_1 \cdots c_n \). Therefore, it follows that \( \ell = |L_\beta / L| = c_1 \cdots c_n \) and that \( V_{X(\mathbb{F}_q)}(I_L) \) has \( c_1 \cdots c_n \) elements by Corollary 4.6.

If \( (q - 1)L_\beta \subseteq L \subseteq L_\beta \), then obviously \( \ell = |L_\beta / L| \) is coprime to \( p = \text{char} \mathbb{F}_q \). On the other hand, whenever \( \ell = |L_\beta / L| \) is not divisible by a prime \( p \), there are finite fields of characteristic \( p \) verifying this condition as we demonstrate next.

**Proposition 4.8.** Let \( L \subseteq L_\beta \) and rank \( L = n \). If \( \ell = |L_\beta / L| \) is not divisible by a prime \( p \), then there is a finite field \( \mathbb{F}_q \) of characteristic \( p \) such that \( \exp(L_\beta / L) \) divides \( q - 1 \). Thus, we have \( (q - 1)L_\beta \subseteq L \subseteq L_\beta \) in this case.

**Proof.** Let \( \mathbb{F}_q \) be the splitting field of \( x^\ell - 1 \) over \( \mathbb{F}_p \). As \( p \) does not divide \( \ell \), \( x^\ell - 1 \) and its derivative \( \ell x^{\ell - 1} \) have no roots in common. So, roots of \( x^\ell - 1 \) are all distinct. It is easy to see that they form a cyclic subgroup of \( \mathbb{F}_q^\ell \) of order \( \ell \). Thus, \( \ell \) divides \( q - 1 \) whence so does \( \exp(L_\beta / L) \).

The second part follows from Lemma 4.3.

We close the section with an interesting example illustrating the results.

**Example 4.9.** Consider the Hirzebruch surface \( X = \mathcal{H}_2 \) whose fan in \( \mathbb{R}^2 \) have rays generated by

\[
\mathbf{v}_1 = (1, 0), \mathbf{v}_2 = (0, 1), \mathbf{v}_3 = (-1, 2), \text{ and } \mathbf{v}_4 = (0, -1).
\]

The exact sequence in (2.1) becomes:

\[
\mathcal{P} : 0 \rightarrow \mathbb{Z}^2 \xrightarrow{\phi} \mathbb{Z}^4 \xrightarrow{\beta} \mathbb{Z}^2 \rightarrow 0,
\]

where

\[
\phi = \begin{bmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 2 & -1 \end{bmatrix}^T \text{ and } \beta = \begin{bmatrix} 1 & -2 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}.
\]

Thus, the class group is \( \mathcal{A} = \mathbb{Z}^2 \) grading the Cox ring \( S = \mathbb{F}_q[x_1, x_2, x_3, x_4] \) of \( X \) via

\[
\deg_{\mathcal{A}}(x_1) = \deg_{\mathcal{A}}(x_3) = (1, 0), \deg_{\mathcal{A}}(x_2) = (-2, 1), \deg_{\mathcal{A}}(x_4) = (0, 1).
\]
Clearly, a $\mathbb{Z}$-basis of $L_\beta$ is given by $u_1 = (1, 0, -1, 0)$ and $u_2 = (0, 1, 2, -1)$.

Consider the lattice $L$ spanned over $\mathbb{Z}$ by $3u_1$ and $5u_2$. Since $B = \{3e_1, 5e_2\}$ is a basis for the lattice $\Lambda$ that appeared in the proof of Corollary 4.6 we have $\ell = |L_\beta/L| = \det B = 15$ and so $15L_\beta \subseteq L \subseteq L_\beta$ by Lemma 3.1. Hence, if $15$ divides $q - 1$, which is the case for instance when $q = 16$ or $q = 31$, then the subgroup $V_{X(\mathbb{F}_q)}(I_L)$ has $15$ members of $T_X$ over the finite field $\mathbb{F}_q$.

5. Finite Nullstellensatz for lattice ideals

In this section, we prove a Nullstellensatz type result over $\mathbb{F}_q$ establishing a one-to-one correspondence between the subgroups $V_{X(\mathbb{F}_q)}(I_L)$ and lattice ideals $I_L$, such that $(q - 1)L_\beta \subseteq L \subseteq L_\beta$.

**Lemma 5.1.** If $(q - 1)L_\beta \subseteq L \subseteq L_\beta$, then the subgroups $V_{X(\mathbb{K})}(I_L)$ and $V_{X(\mathbb{F}_q)}(I_L)$ are the same, for any field $\mathbb{K}$ which is an extension of $\mathbb{F}_q$.

**Proof.** Since $\mathbb{F}_q^* \subseteq \mathbb{K}^*$, we have the inclusion $V_{X(\mathbb{F}_q)}(I_L) \subseteq V_{X(\mathbb{K})}(I_L)$. By Theorem 4.4, $|V_{X(\mathbb{F}_q)}(I_L)| = d_1 \cdots d_n$, and so $\mathbb{F}_q^*$ has all the $d_i$-th roots of unity. Thus, $\mathbb{K}^*$ has all the $d_i$-th roots of unity and hence $|V_{X(\mathbb{K})}(I_L)| = d_1 \cdots d_n$ as well, by Theorem 3.7. Having the same orders, $V_{X(\mathbb{K})}(I_L) = V_{X(\mathbb{F}_q)}(I_L)$ for any field $\mathbb{K}$ which is an extension of $\mathbb{F}_q$. 

It is now time to demonstrate that the necessary condition suggested by the Lemma 4.2 for a lattice to correspond to a vanishing ideal of a subgroup is indeed sufficient.

**Theorem 5.2.** If $(q - 1)L_\beta \subseteq L \subseteq L_\beta$, then $I(V_{X(\mathbb{K})}(I_L)) = I_L$, for any field $\mathbb{K}$ which is an extension of $\mathbb{F}_q$.

**Proof.** By the same reason in the proof of [28, Theorem 5.1(iii)], we have the following minimal primary decomposition for the vanishing ideal of $V_{X(\mathbb{K})}(I_L)$ in $S = \mathbb{F}_q[x_1, \ldots, x_r]$:

$$I(V_{X(\mathbb{K})}(I_L)) = \bigcap_{[P] \in V_{X(\mathbb{K})}(I_L)} I([P]).$$

Suppose now that $p \in S$ is a minimal prime of the radical ideal $I_L \subseteq I(V_{X(\mathbb{K})}(I_L))$. Then, as $p \supseteq I_L$, we have $V_{X(\mathbb{F}_q)}(p) \subseteq V_{X(\mathbb{F}_q)}(I_L)$. As $V_{X(\mathbb{F}_q)}(p)$ cannot be empty over the algebraically closed field $\overline{\mathbb{F}}_q$, it has a point $[P] \in V_{X(\mathbb{F}_q)}(I_L)$.
Since $V_{X}(I_{L}) = V_{X}(I_{L}) = V_{X}(I_{L})$, by Lemma 5.1, $[P] \in V_{X}(I_{L})$ as well. Therefore, $[P] \in V_{X}(I_{L})$ so that $p \subseteq I(V_{X}(I_{L})) \subseteq I([P]) \subseteq S$. So, height$(p) \leq$ height$(I([P])) = n$. Since we also have $p \supseteq I_{L}$, it follows that height$(p) \geq$ height$(I_{L}) = n$. Thus, height$(p) = \text{height}(I([P])) = n$ and these primes must coincide: $p = I([P])$. Therefore, the two ideals $I_{L} \subseteq I(V_{X}(I_{L}))$ having the same minimal primary decomposition must coincide: $I_{L} = I(V_{X}(I_{L}))$.

Recall that subgroups of $T_{X}(F_{q})$ are of the form $Y_{Q} = \{t^{q_{1}} \cdot \cdots \cdot t^{q_{r}} | t \in (F_{q})^{*}\}$ for a matrix $Q = [q_{1} q_{2} \cdots q_{r}] \in M_{r \times r}(Z)$ by [28, Theorem 3.2 and Corollary 3.7]. In [2], a handier description of the lattice of the ideal $I(Y_{Q})$ is given, in terms of $Q$ and $\beta$, under a condition on the lattice $L = QL_{\beta} = \{Qm|m \in L_{\beta}\}$. Before stating this result, let us remind that $L : (q - 1) = \{m \in Z^{n} | (q - 1)m \in L\}$ and that the lattice $L_{Q} \subseteq Z^{r}$ is the kernel of the multiplication map defined by $Q$, i.e. $L_{Q} = \{z \in Z^{r} : Qz = 0\}$.

**Theorem 5.3 ([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 $L = (q - 1)$.

If $L_{Q} \subseteq L_{\beta}$, then $I_{L_{Q}}$ is an $L_{\beta}$-homogeneous toric ideal whose zero locus inside the torus is denoted $V_{Q} := V_{X}(I_{L_{Q}}) \cap T_{X}$. The following consequence of Theorem 5.3 ensures that $V_{Q}$ coincides with the subgroup $V_{Y}$ if the condition $L = L : (q - 1)$ holds, following [25, Proposition 4.3] and [25, Corollary 4.4].

**Theorem 5.4 ([2]).** If $L_{Q} \subseteq L_{\beta}$ and $L = L_{Q} + (q - 1)L_{\beta}$, then we have the following

1. $V_{Q} = V_{X}(I_{L})$.
2. $V_{Q} = V_{Y}$, if the condition $L = L : (q - 1)$ holds.
3. $I(V_{X}(I_{L})) = I_{L}$, if the condition $L = L : (q - 1)$ holds.

Using Theorem 5.2, we are now able to prove that $V_{Q}$ coincides with the subgroup $Y_{Q}$ if and only if the condition $L = L : (q - 1)$ holds.

**Corollary 5.5.** If $L = (L_{Q} \cap L_{\beta}) + (q - 1)L_{\beta}$, then $Y_{Q} = V_{X}(I_{L})$ if and only if $L = L : (q - 1) = L$.

**Proof.** It $L = L : (q - 1) = L$ then by Theorem 5.3 we have $I(Y_{Q}) = I_{L}$ implying that $Y_{Q} = V_{X}(I_{L})$. For the converse it suffices to note that the lattice $L = (L_{Q} \cap L_{\beta}) + (q - 1)L_{\beta}$ satisfies the condition $(q - 1)L_{\beta} \subseteq L \subseteq L_{\beta}$ of Theorem 5.2, and hence $I(Y_{Q}) = I(V_{X}(I_{L})) = I_{L}$. Applying Theorem 5.3 again, we get $L = L : (q - 1) = L$.

We close this section by sharing a procedure for computing the vanishing ideal of $V_{X}(I_{L}) \cap T_{X}$ for lattices $L \subseteq L_{\beta}$ not satisfying the condition $(q - 1)L_{\beta} \subseteq L$.

**Corollary 5.6.** If $L \subseteq L_{\beta}$, then the vanishing ideal of $V_{X}(I_{L}) \cap T_{X} = I_{L'}$, for the lattice $L' = L + (q - 1)L_{\beta}$. Moreover, the order of $V_{X}(I_{L}) \cap T_{X} = |L_{\beta}/L'|$.

**Proof.** If $L' = L + (q - 1)L_{\beta}$, then $I_{L'} = I_{L} + I(1 - q)L_{\beta}$. Since $I(T_{X}(F_{q})) = I(1 - q)L_{\beta}$ it follows that we have

$V_{X}(I_{L'}) = V_{X}(I_{L}) \cap V_{X}(I_{(q - 1)L_{\beta}}) = V_{X}(I_{L}) \cap T_{X}$.

As $(q - 1)L_{\beta} \subseteq L'$, Theorem 5.2 implies that $I_{L'} = I(V_{X}(I_{L}) \cap T_{X})$. Hence, the $B$-saturated ideal corresponding to $Y = V_{X}(I_{L}) \cap T_{X}$ is $I(Y) = I_{L'}$. The second claim follows directly from Theorem 4.4. □
6. Degree of a lattice ideal

In this section, we assume that the \( n \)-dimensional toric variety \( X \) is smooth and projective. Let \( S \) be the Cox ring of \( X \) and \( M \) an \( S \)-graded module. Denote by \( H_M(\alpha) \) the multigraded Hilbert function of \( M \), that is, \( H_M(\alpha) = \dim_K(M_\alpha) \). Maclagan and Smith proved in [20, Proposition 2.10] that there is a polynomial \( P_M(t_1, \ldots, t_d) \in \mathbb{Q}[t_1, \ldots, t_d] \) called the multigraded Hilbert polynomial of \( M \) such that \( P_M(\alpha) = H_M(\alpha) \) for a non-empty subset of \( \mathbb{N}^\beta \). They also showed that for a multigraded ideal \( I \), the Hilbert polynomials of \( S/I \) and that of \( S/(I \colon B^\infty) \) are the same, where \( (I : B^\infty) \) is the \( B \)-saturation of \( I \), see [20, Lemma 2.13]. Therefore, if \( I \) is the \( B \)-saturated ideal corresponding to a finite set of points then its Hilbert polynomial is constant and equal to the cardinality of \( V_X(I) \), see [20, Example 4.12]. Inspired from these, we make the following

**Definition 6.1.** Let \( I \) be the \( B \)-saturated homogeneous ideal corresponding to a finite set of points. The degree of \( I \) is the constant Hilbert polynomial \( P_{S/I} \).

**Lemma 6.2.** If \( I_L \) is an \( L_\beta \)-homogeneous ideal, then its (multigraded) Hilbert function defined by \( H_{I_L}(\alpha) := \dim_K(S_\alpha/I_L) \) is independent of the field \( K \).

**Proof.** Recall that the vector space \( S_\alpha \) is spanned by the monomials

\[
x^\alpha = x_1^{a_1} \cdots x_r^{a_r} \quad \text{with} \quad \deg(x^\alpha) = \sum_{j=1}^r a_j \beta_j = \alpha.
\]

By [22, Theorem 7.3], the quotient ring \( S/I_L \) is isomorphic to the semigroup ring of the semigroup \( \mathbb{N}^r / \sim_L \), where \( a_1 \sim_L a_2 \iff a_1 - a_2 \in L \). Since \( I_L \) is \( L_\beta \)-homogeneous, we have \( L \subseteq L_\beta \). Therefore, \( a_1 - a_2 \in L \) implies \( a_1 - a_2 \in L_\beta \), i.e. if \( x^{a_1} + I_L = x^{a_2} + I_L \) in \( S/I_L \), then \( \deg(x^{a_1}) = \deg(x^{a_2}) \) meaning that \( \sum_{j=1}^r a_j \beta_j = \alpha \). This number is independent of the field, completing the proof.

**Theorem 6.3.** If \( I_L \) is an \( L_\beta \)-homogeneous ideal of dimension \( d = r - n \), then its degree is \( \deg(I_L) = |L_\beta/L| = d_1 \cdots d_n \), where \( d_i \)'s are the invariant factors of \( L_\beta/L \).

**Proof.** By Lemma 6.2, the multigraded Hilbert polynomial of \( I_L \) is independent of the field. Under the hypothesis \( \text{rank } L = n \) and \( L \subseteq L_\beta \), so by Proposition 4.8 there is a finite field \( \mathbb{F}_q \) such that \( (q - 1)L_\beta \subseteq L \subseteq L_\beta \). Thus, the number of \( \mathbb{F}_q \)-rational points is \( |V_X(I_L)(\mathbb{F}_q)| = d_1 \cdots d_n \) by Theorem 4.4. On the other hand, the \( B \)-saturated ideal corresponding to \( V_X(I_L) \) is \( I(V_X(I_L)) = I_L \) by Theorem 5.2. Thus, the Hilbert polynomial of \( I_L \) will be \( d_1 \cdots d_n \), which is the degree of \( I_L \).

The following reveals that Theorem 6.3 generalizes the main result of the nice paper [19] by Lopez and Villarreal. \( X \) is the projective space \( \mathbb{P}^n \) in this case. The matrix \( \beta = [1 \cdots 1] \), \( L_\beta = \mathbb{Z}\{e_1 - e_r, \ldots, e_{r-1} - e_r\} \) and hence an ideal is \( L_\beta \)-homogeneous with respect to the standard grading: \( \deg(x_i) = 1 \), for each \( i \in [r] \), where \( r = n + 1 \).
Corollary 6.4. [19, Theorem 3.13] If $I_L$ is an $L_\beta$-homogeneous ideal of dimension 1, then its degree is $\deg(I_L) = |T(Z'/L)|$, where $T(Z'/L)$ is the torsion part of the group $Z'/L$.

Proof. It is well known from the fundamental structure theorem for finitely generated abelian groups that the order of the torsion part $T(Z'/L)$ of the group $Z'/L$ is $d_1 \cdots d_n$, where $d_i$'s are the invariant factors of the matrix whose columns span the lattice $L$, see [14, pp. 187—188]. So, Theorem 6.3 completes the proof. □

If an ideal $I = \langle F_1, \ldots, F_n \rangle$ is a complete intersection generated in semi-ample degrees $\alpha_1, \ldots, \alpha_n$, then its Hilbert Polynomial is the Bernstein–Kushnirenko bound, which is the mixed volume $nV(P_{\alpha_1}, \ldots, P_{\alpha_n})$ of the Newton polytopes $P_{\alpha_1}, \ldots, P_{\alpha_n}$ by the proof of [29, Theorem 3.16]. The following reveals the same is true in the special case that $I = I_L$ is a lattice ideal, without the assumption that the degrees $\alpha_1, \ldots, \alpha_n$ are semi-ample.

Corollary 6.5. Assume that $\{d_1m_1, \ldots, d_nm_n\}$ is a basis of the lattice $L$ such that $\{m_1, \ldots, m_n\}$ is a basis of $L_\beta$. If $P_i$ is the Newton polytope of the binomial $F_i = x^{d_im_i} - x^{d_im_i}$, for $i \in [n]$, then the degree of $I_L$ is the mixed volume $nV(P_1, \ldots, P_n)$.

Proof. By Proposition 4.8, there is a finite field $K = \mathbb{F}_q$ containing all the $d_i$-th roots of unity, for each $i \in [n]$. We know that $V_X(I_L)(K)$ lies inside the torus $T_X(K)$ by Proposition 3.3. So, localizing to the torus does not change the order of $V_X(I_L)(K)$. This amounts to passing to the Laurent polynomial ring

$$K[x^\pm] = K[x_1, \ldots, x_r|x_1 \cdots x_r = \mathbb{F}[x_1, \ldots, x_r, x_1^{-1}, \ldots, x_r^{-1}].$$

By [9, Theorem 2.1], the ideal $K[x^\pm]I_L$ is a local complete intersection generated by the Laurent polynomials $x^{d_1m_1} - 1, \ldots, x^{d_nm_n} - 1$ forming a regular sequence, even if $I_L$ is not the (global) complete intersection ideal

$$(x^{d_1m_1} - x^{d_1m_1}, \ldots, x^{d_nm_n} - x^{d_nm_n}).$$

Letting $t_i := x^{m_i}$ be the local variables for the torus $T_X(K) \cong (K^*)^n$, we get the system $t_1 = \cdots = t_n = 1$ having $d_1 \cdots d_n$ solutions as $K$ has all the $d_i$-th roots of unity, for each $i \in [n]$. Thus, $|V_X(I_L)(K)|$ meets the Bernstein–Kushnirenko bound $nV(P_1, \ldots, P_n) = d_1 \cdots d_n$ by [13] as $P_i$ are just line segments, see also [4, 17]. Hence, Theorem 6.3 completes the proof. □

Example 6.6. We revisit Example 4.9. Consider the fan in $\mathbb{R}^2$ with rays generated by $v_1 = (1,0)$, $v_2 = (0,1)$, $v_3 = (1,2)$, and $v_4 = (0,-1)$. Then the corresponding toric variety is the Hirzebruch surface $X = H_2$. Recall that a $\mathbb{Z}$-basis of $L_\beta$ is given by $u_1 = (1,0,-1,0)$ and $u_2 = (0,1,2,-1)$. Consider the lattice $L$ spanned over $\mathbb{Z}$ by $3u_1$ and $5u_2$. Then, clearly $15L_\beta \subset L \subset L_\beta$. So, the degree of $I_L$ is just the order $|L_\beta/L| = 15$.

If $p$ is a prime number other than 3 or 5, then by Proposition 4.8 there is a finite field $\mathbb{F}_{q'}$ whose characteristic is $p$ for which $(q - 1)L_\beta \subset L \subset L_\beta$ is satisfied and thus $I_L = I(V_X(\mathbb{F}_{q'})(I_L))$ is the $B$-saturated ideal of $V_X(\mathbb{F}_{q'})(I_L)$ by Theorem 5.2 over the field $\mathbb{F}_{q'}$, where $B = (x_1x_2, x_2x_3, x_3x_4, x_4x_1)$. This is the case for instance with $p = 2$, and thus, $V_X(\mathbb{F}_q)(I_L)$ has 15 = $\deg(I_L)$ members of $T_X$ over $\mathbb{F}_{16}$. Similarly, $I_L$ is the $B$-saturated ideal of $V_X(\mathbb{F}_q)(I_L)$ over the finite field $\mathbb{F}_q$ of
characteristic \( p = 11 \), with \( q = 11^2 = 121 \) elements, as 15 divides 120. \( V_{X(\mathbb{F}_q)}(I_L) \) has 15 = \( \deg(I_L) \) members of \( T_X \) over \( \mathbb{F}_{121} \).

However, if \( q = p = 11 \) then \( I_L \) is not the B-saturated ideal of \( V_{X(\mathbb{F}_q)}(I_L) \) as 15 does not divide 10. Over the field \( \mathbb{F}_{11} \), we have to replace \( L \) by \( L' = L + (q-1)L \), so as to obtain the correct lattice whose ideal \( I_{L'} \) is the B-saturated vanishing ideal of \( V_{X(\mathbb{F}_q)}(I_L) \), by Corollary 5.6. A basis for the lattice \( L' \) is given by \( u_1 \) and \( 5u_2 \), since \( u_1 = -3(3u_1) + 10u_1 \in L' \). The Smith-normal form of the matrix with columns \( u_1 \) and \( 5u_2 \) is \([e_1|5e_2]\), where \( e_i \) is a standard basis vector of \( \mathbb{Z}^1 \). Thus, \( V_{X(\mathbb{F}_q)}(I_L) \) has 5 = \( \deg(I_L') \) members of \( T_X \) over the finite field \( \mathbb{F}_{11} \).

7. Parameterization of the subgroup cut out by a lattice ideal

In this section, we describe the points of the subgroup \( V_{X(K)}(I_L) \) of the torus \( T_X \) defined by the lattice ideal \( I_L \).

Let \( B \) be an \( r \times n \) matrix whose columns constitute a basis for \( L \subseteq L \); let \( A \) and \( C \) be unimodular matrices of sizes \( r \times r \) and \( n \times n \), respectively, so that

\[
D = ABC = [d_1e_1|\ldots|d_ne_n]
\]

is the Smith-Normal form of \( B \), where \( e_1, \ldots, e_n \in \mathbb{Z}^r \). Recall that \( d_i \) divides \( d_{i+1} \), for all \( i \in [n-1] \). If \( A^{-1} = [m_1|\ldots|m_n] \) is the inverse of \( A \), then its columns span \( \mathbb{Z}^r \). Thus, the columns \( \{d_im_1, \ldots, d_nm_n\} \) of \( A^{-1}D = BC \) provide us with another basis of the lattice \( L \) such that \( \{m_1, \ldots, m_n\} \) is a basis of \( L \). Since \( \operatorname{rank} L = n \), we have \( V_{X(K)}(I_L) \subseteq T_X \) by Proposition 3.3.

**Theorem 7.1.** Let \( L \subseteq L \) be a lattice of rank \( n \). Then, the following hold:

(i) If \( [P_i] = [\eta_i^{a_1}:\ldots:\eta_i^{a_r}] \), where \( \eta_i \) is a generator for the cyclic subgroup of \( d_i \)-th roots of unity in \( K \), for all \( i \in [n] \), and \( a_i \)'s are the entries of \( A \), then

\[
V_X(I_L)(K) \subseteq \langle [P_1] \rangle \times \ldots \times \langle [P_n] \rangle.
\]

(ii) If \( d_i \) divides \( q-1 \), for all \( i \in [n] \), and \( Q \) is the matrix whose \( i \)-th row is \([a_1(q-1)/d_i|\ldots|a_r(q-1)/d_i]\), which is \( (q-1)/d_i \) times the \( i \)-th row of the matrix \( A \), then \( V_X(I_L)(\mathbb{F}_q) = Y_Q \).

**Proof.** The algebraic isomorphism induced by the change of basis map \( \mathbb{Z}^r \to \mathbb{Z}^r \) defined via multiplication by the matrix \( A = [a_1|\ldots|a_n] \) is as follows:

\[
\Phi_A : (\mathbb{K}^*)^r \to (\mathbb{K}^*)^r, \quad \Phi_A(y_1, \ldots, y_r) = (y^{a_1}, \ldots, y^{a_n}).
\]

with the following inverse isomorphism:

\[
\Phi_A^{-1} : (\mathbb{K}^*)^r \to (\mathbb{K}^*)^r, \quad \Phi_A^{-1}(x_1, \ldots, x_r) = (x^{a_1}, \ldots, x^{a_n}).
\]

Recall that \( G \) is the subgroup \( V(I_{L_{\beta}}) \cap (\mathbb{K}^*)^r \) and thus \( (x_1, \ldots, x_r) \in G \) if and only if \( x^{a_1} = \cdots = x^{a_n} = 1 \). Therefore, if \( (y_1, \ldots, y_r) = \Phi_A^{-1}(x_1, \ldots, x_r) \), then it follows that \( (x_1, \ldots, x_r) \in G \) if and only if \( y_1 = \cdots = y_n = 1 \). Thus, the group \( G' := \Phi_A^{-1}(G) \) is described by

\[
G' = \{1,\ldots,1, y_{n+1}, \ldots, y_r) : y_i \in (\mathbb{K}^*)^r \}.
\]

On the other hand, since a basis for \( L \) is given by the set \( \{d_1m_1, \ldots, d_nm_n\} \), we similarly have the following:

\[
(x_1, \ldots, x_r) \in V(I_L) \cap (\mathbb{K}^*)^r \iff x^{d_1m_1} = \cdots = x^{d_nm_n} = 1.
\]
Finally, as the elements $[x_1 : \cdots : x_r] \in T_X(\mathbb{K})$ are orbits $G \cdot (x_1, \ldots, x_r)$, it follows that

$$[x_1 : \cdots : x_r] \in T_X(\mathbb{K}) \iff [y_1 : \cdots : y_n : 1 : \cdots : 1] \in (\mathbb{K}^*)^r/G'.$$

Thus, $\Phi_A^{-1}$ induces an isomorphism between $T_X(\mathbb{K})$ and the torus $(\mathbb{K}^*)^r/G'$ identifying the subgroup $V_X(I_L)(\mathbb{K})$ of $T_X(\mathbb{K})$ with the following subgroup:

$$G_L := \{[y_1 : \cdots : y_n : 1 : \cdots : 1] \in (\mathbb{K}^*)^r/G' : y_1^{d_1} = \cdots = y_n^{d_n} = 1\}.$$

If $C_i = \{y_i \in \mathbb{K}^* : y_i^{d_i} = 1\}$, for all $i \in [n]$, then, $G_L$ is isomorphic to $C_1 \times \cdots \times C_n$, via

$$[y_1 : \cdots : y_n : 1 : \cdots : 1] \mapsto (y_1, \ldots, y_n).$$

If $C_i$ is the cyclic subgroup of $\mathbb{K}^*$ generated by $\eta_i$, then the elements of $G_L$ are of the form

$$[y_1 : \cdots : y_n : 1 : \cdots : 1] = [\eta_1^{i_1} : \cdots : \eta_n^{i_n} : 1 : \cdots : 1],$$

which bijectively correspond to the n-tuples $(k_1, \ldots, k_n)$ with $0 \leq k_i \leq |C_i| - 1$. Let $[P] = [x_1 : \cdots : x_r]$ be a point with $x_i = y_a^{i_1} \cdots y_n^{i_n}$. Then, we have

$$[P] \in V_X(I_L)(\mathbb{K}) \iff \Phi_A^{-1}(P) \in G_L.$$

Therefore, $[P] \in V_X(I_L)(\mathbb{K}) \iff$ there is an n-tuple $(k_1, \ldots, k_n)$ with $0 \leq k_i \leq |C_i| - 1$ such that

$$(7.3) \quad [P] = [\eta_1^{a_1 k_1} \cdots \eta_n^{a_n k_n} : \cdots : \eta_1^{a_1 k_1} \cdots \eta_n^{a_n k_n}].$$

This proves the first part (i):

$$V_X(I_L)(\mathbb{K}) = \langle [P_1] \rangle \times \cdots \times \langle [P_n] \rangle.$$

When $\mathbb{K} = \mathbb{F}_q$ and $d_i$ divides $q - 1$, $C_i$ becomes the cyclic subgroup of $\mathbb{F}_q^*$ of order $d_i$, generated by $\eta_i = \eta^{q^{-1}/d_i}$, for all $i \in [n]$. Letting $t_i = \eta^{k_i}$ for all $i \in [n]$, we observe that the point in (7.3) becomes

$$[P] = [\eta_1^{t_1 (q-1)/d_1} \cdots \eta_n^{t_n (q-1)/d_n} : \cdots : \eta_1^{t_1 (q-1)/d_1} \cdots \eta_n^{t_n (q-1)/d_n}].$$

If $Q$ is the matrix whose $i$-th row is $[a_{i1}(q-1)/d_1] \ldots [a_{ir}(q-1)/d_i]$, then it follows that $[P] \in V_X(I_L)(\mathbb{F}_q)$ implies $[P] \in Y_Q$.

In order to prove the converse inclusion, take $[P] \in Y_Q$. Then, there are $t_i \in \mathbb{F}_q^*$ such that

$$[P] = [t_1^{a_2(q-1)/d_1} \cdots t_n^{a_n(q-1)/d_n} : \cdots : t_1^{a_2(q-1)/d_1} \cdots t_n^{a_n(q-1)/d_n}].$$

Since $\mathbb{F}_q^* = \langle \eta \rangle$, we have $t_i$ between 0 and $q - 2$ for which $t_i = \eta^{k_i}$, for all $i \in [n]$. Then, there is a unique $k_i$ between 0 and $d_i - 1$ such that $t_i \equiv k_i$ modulo $d_i$. Thus, $t_1^{(q-1)/d_1} = \eta^{k_1(q-1)/d_1} = \eta^{k_1(q-1)/d_1}$, yielding $[P] \in V_X(I_L)(\mathbb{F}_q)$. 

\textbf{Corollary 7.2.} If $V_X(I_L)(\mathbb{F}_q)$ is a cyclic subgroup, then $V_X(I_L)(\mathbb{F}_q) = Y_Q$ for a row matrix $Q = [a_{n1}(q-1)/d_n] \ldots [a_{nr}(q-1)/d_n]$ which is $(q - 1)/d_n$ times the n-th row of the matrix A.
Example 7.4. We revisit the Example 4.9 by considering the Hirzebruch surface $X$ matrices provided in Theorem 7.1 and Corollary 7.2 that are more natural and given in Remark 7.3.

By Theorem 4.4, $\text{det} P = 1$ and $\text{det} Q = 1$ due to the fact that $Y$ is the matrix whose $i$-th row is $(q-1)/d_i$ times the $i$-th row of the matrix $A$. When $d_i = 1$, the following point

$$[P] = [t_1^{a_{11}(q-1)/d_1} \cdots t_n^{a_{nn}(q-1)/d_n} : \cdots : t_1^{a_{1n}(q-1)/d_1} \cdots t_n^{a_{nn}(q-1)/d_n}]$$

due to the fact that $t_i^{a_{ij}(q-1)/d_i} = 1$, for all $i \in [n-1]$ and $j \in [r]$. Thus, $[P]$ is a point of $Y_Q$. As the converse is also true, the claim follows.

**Remark 7.3.** Although a parameterization $Y_Q$ of the subgroup $V_X(\mathbb{F}_q)(I_L) \cap T_X$ is given in [28, Proposition 3.4], the size of the matrix $Q$ for which $V_X(\mathbb{F}_q)(I_L) \cap T_X = Y_Q$ was always $r \times r$, even if the subgroup is cyclic. This is in contrast with the matrices provided in Theorem 7.1 and Corollary 7.2 that are more natural and succinct.

We illustrate the main result of this section working with $k = \mathbb{R}$ and $\mathbb{K} = \mathbb{C}$.

**Example 7.4.** We revisit the example 4.9 by considering the Hirzebruch surface $X = \mathcal{H}_2$ over $\mathbb{K} = \mathbb{R}$ or $\mathbb{K} = \mathbb{C}$ this time. Consider the lattice $L$ spanned by the columns of the matrix $B = [2u_1 \quad 3u_2]$. Then the Smith-Normal form $D$ of $B$ is given by

$$D = ABC = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 3 & 4 \\ 1 & 0 & 1 & 2 \end{bmatrix} \begin{bmatrix} 2 & 0 \\ 0 & 3 \\ -2 & 6 \\ 0 & -3 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 6 \\ 0 & 0 \end{bmatrix}.$$  

The cyclic subgroup $C_1$ of the 1-st roots of unity is trivial over $\mathbb{R}$ or $\mathbb{C}$. But, the cyclic subgroup $C_2$ of the 6-th roots of unity are as follows respectively over $\mathbb{R}$ or $\mathbb{C}$.

$$C_2 = \{c \in \mathbb{R}^* : c^6 = 1\} = \{-1, 1\},$$

$$C_2 = \{c \in \mathbb{C}^* : c^6 = 1\} = \langle \eta_2 \rangle = \langle (1 + i\sqrt{3})/2 \rangle = \{1, (1 + i\sqrt{3})/2, (-1 + i\sqrt{3})/2, -1, (-1 - i\sqrt{3})/2, (1 - i\sqrt{3})/2\}.$$

It follows from Theorem 3.7 that $|V_X(\mathbb{K})(I_L)| = |C_1| \cdot |C_2|$ which is 2 and 6 over $\mathbb{R}$ and $\mathbb{C}$ respectively. Indeed,

$$V_X(\mathbb{K})(I_L) = \{[x_1 : x_2 : x_3 : x_4] \in X(\mathbb{K}) : x_1^2 = x_2^3 = x_3^2 = (x_2 x_3)^3\}.$$

Since $G = \{[\lambda_1 : \lambda_2 : \lambda_3 : \lambda_4] : \lambda_1, \lambda_2, \lambda_3, \lambda_4 \in \mathbb{C}^*\}$, we have

$$V_X(\mathbb{R})(I_L) = \{[x_1 : x_2 : x_3 : x_4] : [x_1 : x_2 : -x_1 : x_2^2] : [x_3, x_4] \in \mathbb{R}^*\},$$

$$V_X(\mathbb{C})(I_L) = \{[1 : 1 : 1 : 1] \cap [1 : 1 : -1 : 1], [1 : 1 : 1 : \eta_2], [1 : 1 : \pm 1 : \eta_2]\}.$$

Notice that $V_X(\mathbb{C})(I_L) = \langle [P_1] \times [P_2] \rangle$, where $[P_1] = [\eta_2^0 : \eta_2^0 : \eta_2^0 : \eta_2^0]$ and $[P_2] = [\eta_2^0 : \eta_2^0 : \eta_2^0 : \eta_2^0]$ as stated in Theorem 7.1. The isomorphism between the groups $V_X(\mathbb{K})(I_L)$ and $C_1 \times C_2$ is not clear at this stage.
Therefore, the map $\Phi^{-1}: (\mathbb{K}^*)^4 \to (\mathbb{K}^*)^4$ is given by

$$\Phi^{-1}(x_1, x_2, x_3, x_4) = (x_1^2 x_2^3 x_3^4 x_4^{-3}, x_1^{-1} x_2 x_3 x_4^3, x_2, x_1) = (y_1, y_2, y_3, y_4).$$

Hence, we have

$$\Phi_{A^{-1}}^{-1}(V_{X(\mathbb{K})}(I_L)) = G_L(\mathbb{K}) = \{[y_1 : y_2 : 1 : 1] \in X(\mathbb{K}) : y_1 = 1 \text{ and } y_2^6 = 1\},$$

which is canonically isomorphic to $C_1 \times C_2$. Clearly,

$$\Phi_{A^{-1}}^{-1}(1, 1, \pm 1, \eta_2^j) = (1, \pm \eta_2^j, 1, 1), \text{ for all } j = 0, 2, 4.$$

Thus, we have

$$\Phi_{A^{-1}}^{-1}(V_{X(\mathbb{C})}(I_L)) = G_L(\mathbb{C}) = \{[1 : \pm 1 : 1 : 1], [1 : \pm \eta_2^2 : 1 : 1], [1 : \pm \eta_4^2 : 1 : 1]\}.$$

Similarly, we have $\Phi_{A^{-1}}^{-1}(V_{X(\mathbb{R})}(I_L)) = G_L(\mathbb{R}) = \{[1 : 1 : 1 : 1], [1 : -1 : 1 : 1]\}$.

8. Evaluation codes on subgroups of the torus $T_X(\mathbb{F}_q)$

In this section, we apply the main results of the paper to compute basic parameters of toric codes on subgroups $Y = V_{X(\mathbb{F}_q)}(I_L)$ of the torus $T_X(\mathbb{F}_q)$, where a basis for $L$ is given by $\{c_1 u_1, \ldots, c_n u_n\}$ for positive integers $c_i$ dividing $q - 1$.

We first recall the evaluation code defined on a subset $Y = \{[P_1], \ldots, [P_N]\}$ of $T_X(\mathbb{F}_q)$. Let $\mathbb{N}^\beta$ be the subsemigroup of $\mathbb{N}^n$ generated (not necessarily minimally) by $\beta_1, \ldots, \beta_r$. Recall that the Cox ring $S = \bigoplus_{\alpha \in \mathbb{N}^\beta} S_\alpha$ of $X$ is multigraded by $\mathbb{N}^\beta$ via \[ \deg(x_i) = \beta_i \text{ for } i = 1, \ldots, r. \]

For any multidegree $\alpha \in \mathbb{N}^\beta$, we have the following evaluation map

$$\text{ev}_Y : S_\alpha \to \mathbb{F}_q^N, \quad F \mapsto (F(P_1), \ldots, F(P_N)).$$

The image $C_{\alpha, Y} = \text{ev}_Y(S_\alpha)$ is a linear code, called the generalized toric code. The three basic parameters of $C_{\alpha, Y}$ are block-length which is $N$, the dimension which is $K = \text{dim}_\mathbb{K}(C_{\alpha, Y})$, and the minimum distance $\delta = \delta(C_{\alpha, Y})$ which is the minimum of the numbers of nonzero components of nonzero vectors in $C_{\alpha, Y}$.

It is clear that the kernel of the linear map $\text{ev}_Y$ equals the homogeneous piece $I(Y)_\alpha$ of the vanishing ideal $I(Y)$ in degree $\alpha$. Therefore, the code $C_{\alpha, Y}$ is isomorphic to the $\mathbb{K}$-vector space $S_\alpha/I(Y)_\alpha$. Thus, the dimension of $C_{\alpha, Y}$ is the multigraded Hilbert function $H_Y(\alpha) := \text{dim}_\mathbb{K} S_\alpha - \text{dim}_\mathbb{K} I(Y)_\alpha$ of $I(Y)$. As $C_{\alpha, Y}$ is a subspace of $\mathbb{F}_q^N$, we have $H_Y(\alpha) \leq N$. When we have the equality $K = H_Y(\alpha) = N$, the code becomes trivial, i.e. $\delta = \delta(C_{\alpha, Y}) = 1$, by the Singleton bound $\delta \leq N + 1 - K$. A related algebraic notion useful to eliminate these trivial codes is the so-called multigraded regularity defined by

$$\text{reg}(Y) := \{ \alpha \in \mathbb{N}^\beta : H_Y(\alpha) = |Y| \} \subseteq \mathbb{N}^d.$$
The values of the Hilbert function $H_Y(\alpha)$ can also be used to detect (monomially) equivalent codes. Indeed, by [29, Proposition 4.3], the codes $C_{\alpha,Y}$ and $C_{\alpha',Y}$ are equivalent if $H_Y(\alpha) = H_Y(\alpha')$ and $\alpha - \alpha' \in \mathbb{N}I_n$.

The first application of our results is that the length of the code $C_{\alpha,Y}$ is given by $N = |Y| = c_1 \cdots c_n$, due to Corollary 4.7, where $Y = V_X(\mathcal{I}_L)$ for the lattice $L$ with a basis given by $\{c_1u_1, \ldots, c_nu_n\}$ for positive integers $c_i$ dividing $q - 1$.

In order to compute the dimension and minimum distance of the code $C_{\alpha,Y}$, we need to determine a minimal generating set for the vanishing ideal $I(Y)$. We apply our Theorem 5.2 together with a characterization of complete intersection lattice ideals given by Morales and Thoma [23] using the following concept.

**Definition 8.1.** Let $A$ be a matrix whose entries are all integers. $A$ is called mixed if there is a positive and a negative entry in every column. If no square submatrix of $A$ is mixed, it is called dominating.

**Theorem 8.2.** [23, Theorem 3.9] Let $L \subseteq \mathbb{Z}^{r}$ be a lattice with the property that $L \cap \mathbb{Z}^{r} = 0$. Then, $I_L$ is complete intersection if and only if $L$ has a basis $m_1, \ldots, m_k$ such that the matrix $[m_1 \cdots m_k]$ is mixed, dominating. In the affirmative case, we have $I_L = \langle x^{m_1} - x^{m_2}, \ldots, x^{m_k} - x^{m_k} \rangle$. □

Applying our Theorem 5.2 to $Y = V_X(\mathcal{I}_L)$ we immediately obtain the equality of the ideals $I(Y) = I_L$. Using then Theorem 8.2, one can confirm when $I(Y) = I_L$ is a complete intersection by looking at a basis of the lattice $L$. The rest of the section discusses an instance where everything works very well.

Let $X = \mathcal{H}_\ell$ be the Hirzebruch surface whose fan have primitive ray generators given by $v_1 = (1,0)$, $v_2 = (0,1)$, $v_3 = (-1,\ell)$, and $v_4 = (0,-1)$, for any positive integer $\ell$. The exact sequence in (2.1) becomes

$$
\begin{CD}
\mathcal{P} : 0 @>>> \mathbb{Z}^2 @>\phi>> \mathbb{Z}^4 @>\beta>> \text{Cl}(\mathcal{H}_\ell) @>>> 0
\end{CD}
$$

for $\phi = [u_1 \ u_2]$ with $u_1 = (1,0,-1,0)$, $u_2 = (0,1,\ell,-1)$ and $\beta = \begin{bmatrix}
1 & 0 & 1 & \ell \\
0 & 1 & 0 & 1
\end{bmatrix}$ with $L_\beta = \langle u_1, u_2 \rangle$. The dual sequence in (2.2) over $\mathbb{K} = \mathbb{F}_q$ becomes

$$
\begin{CD}
\mathcal{P}^* : 1 @>>> G @>\beta^*>> (\mathbb{K}^*)^4 @>\pi>> (\mathbb{K}^*)^2 @>>> 1
\end{CD}
$$

where $\pi : t \mapsto (t_1t_3^{-1}, t_2t_4^{-1})$ and $G = \text{Ker}(\pi) = \{(t_1, t_2, t_1t_2) \mid t_1, t_2 \in \mathbb{K}^*\} \cong (\mathbb{K}^*)^2$. Hence, $\mathbb{K}$-rational points of the torus is $T_X(\mathbb{K}) \cong (\mathbb{K}^*)^2 \cong (\mathbb{K}^*)^4/G$ whereas $\mathbb{F}_q$-rational points is $T_X(\mathbb{F}_q) \cong (\mathbb{F}_q^*)^2 \cong (\mathbb{F}_q^*)^4/G$.

The Cox ring $S = \mathbb{F}_q[x_1, x_2, x_3, x_4]$ is $\mathbb{Z}^2$-graded via

$$
\deg(x_1) = \deg(x_3) = (1,0), \quad \deg(x_2) = (0,1), \quad \deg(x_4) = (\ell,1).
$$

**Proposition 8.3.** Let $X$ be the Hirzebruch surface $\mathcal{H}_\ell$. If $\{c_1u_1, c_2u_2\}$ constitute a basis for $L$, and $Y = V_X(\mathcal{I}_L)$ then $I(Y)$ is a complete intersection generated minimally by $x_3^{c_1} - x_1^{c_1}$ and $x_4^{c_2} - x_2^{c_2}$. Furthermore, $(c_1 + c_2, c_1 + c_2) + \mathbb{N}^2 \subseteq \text{reg}(Y)$.

**Proof.** By Theorem 5.2, we get $I(Y) = I_L$. Since the columns of $ML$ constitute a basis of $L$, where

$$
ML = [c_1 u_1 \ c_2 u_2] = \begin{bmatrix}
c_1 & 0 & -c_1 & 0 \\
c_2 & \ell c_2 & -c_2
\end{bmatrix}^T
$$
and ML is mixed dominating, it follows from Theorem 8.2 that
\[ I(Y) = \langle x_3^{c_1} - x_1^{c_1}, x_4^{c_2} - x_2^{c_2} x_3^{c_2} \rangle. \]

There is a geometrically significant subsemigroup \( K \) contained in the semigroup \( \mathbb{N}\beta = \mathbb{N}^2 \) whose elements are semiample degrees corresponding to the classes of numerically effective line bundles on \( X \), which is given by
\[ K = \bigcap_{\sigma \in \Sigma} \mathbb{N} \delta = \mathbb{N}(1,0) + \mathbb{N}(\ell,1), \]
where \( \mathbb{N} \delta \) is the semigroup generated by \( \beta_i \) corresponding to rays \( \rho_i \notin \sigma \), for details see [7, Theorem 6.3.12]. Thus, the degrees \( c_1(1,0) \) and \( c_2(\ell,1) \) of the generators are semiample. Therefore, \( (c_1 + c_2\ell, c_2) + \mathbb{N}^2 \subseteq \text{reg}(Y) \) by [29, Theorem 3.16].

It is now time to compute the other main parameters of the toric code \( C_{\alpha,Y} \), where \( \alpha = (c,d) \in \mathbb{N}\beta \). Hansen computed these parameters for the case \( Y = T_X(\mathbb{F}_q) \), \( c < q - 1 \) and \( d = b \), where \( b \) is to be defined below, see [12]. More recently, the conditions \( c < q - 1 \) and \( d = b \) is relaxed in [1] again for the torus \( Y = T_X(\mathbb{F}_q) \).

**Theorem 8.4.** Let \( \{c_1u_1, c_2u_2\} \) be a basis for \( L \) with \( c_1 \) and \( c_2 \) dividing \( q - 1 \), and \( Y = V_X(\mathbb{F}_q)(I_L) \) be the subgroup of the torus \( T_X \) of the Hirzebruch surface \( X = \mathcal{H}_t \) over \( \mathbb{K} = \mathbb{F}_q \) satisfying \( c_1 \leq tc_2 \). If \( \alpha = (c,d) \in \mathbb{N}\beta = \mathbb{N}^2 \), then the dimension \( K \) of the toric code \( C_{\alpha,Y} \) is given by
\[
\begin{cases}
(b + 1)[c + 1 - b\ell/2], & \text{if } c < c_1 \text{ and } b \leq c_2 - 1 \\
c_2[c + 1 - (c_2 - 1)\ell/2], & \text{if } c < c_1 \text{ and } c_2 - 1 < b \\
c_1(b' + 1) + (b - b')[c + 1 - \ell(b + b' + 1)/2], & \text{if } c \geq c_1 \text{ and } b' \leq b < c_2 - 1 \\
c_1(b' + 1) + (c_2 - 1 - b')[c + 1 - \ell(c_2 + b')/2], & \text{if } c \geq c_1 \text{ and } b < c_2 - 1 \leq b \\
c_1c_2, & \text{if } c \geq c_1 \text{ and } b' \geq c_2 - 1,
\end{cases}
\]
and the minimum distance equals
\[
\delta(C_{\alpha,Y}) = \begin{cases}
c_2[c_1 - c], & \text{if } c < c_1 \text{ and } b \leq c_2 - 1 \\
c_2[c_1 - c], & \text{if } c < c_1 \text{ and } c_2 - 1 < b \\
c_2 - b', & \text{if } c \geq c_1 \text{ and } b' \leq b < c_2 - 1 \\
c_2 - b', & \text{if } c \geq c_1 \text{ and } b < c_2 - 1 \leq b \\
1, & \text{if } c \geq c_1 \text{ and } b' \geq c_2 - 1.
\end{cases}
\]
where \( b \) is the greatest non-negative integer with \( c - b\ell \geq 0 \) and \( d - b \geq 0 \), and when \( c \geq c_1, b' \) is the greatest non-negative integer with \( c - b'\ell \geq c_1 - 1 \) and \( d - b' \geq 0 \).

**Proof.** We start by giving a parameterization which will be crucial especially in computing the minimum distance below. So, we first see that
\[
Q = \begin{bmatrix}
(q - 1)/c_1 & 0 & 0 & 0 \\
0 & 0 & 0 & (q - 1)/c_2
\end{bmatrix}
\]
parameterizes the subgroup \( Y = V_X(\mathbb{F}_q)(I_L) \). Let \( \eta_1 = \eta^{(q - 1)/c_1} \) and \( \eta_2 = \eta^{(q - 1)/c_2} \) where \( \eta \) is a generator for the cyclic group \( \mathbb{K}^* \). Then, \( Y_Q \) consists of the following...
It is clear that we assume from now on that it is worth to notice that this dimension is the number of monomials in \( \leq 2 \) which is defined by the inequalities \( 0 \leq a_4 \leq b \), and fixed \( 0 \leq a_4 \leq c - \ell a_4 \) the powers \( a_2 = d - a_4 \) and \( a_3 = c - \ell a_4 - a_1 \) in \( x^a = x_1^{a_1}x_2^{a_2}x_3^{a_3}x_4^{a_4} \) are fixed too. So,

\[
\tilde{B}_\alpha = \{ x_1^{a_1}x_2^{d-a_4}x_3^{c-\ell a_4-a_1}x_4^{a_4} | 0 \leq a_4 \leq b \text{ and } 0 \leq a_1 \leq c - \ell a_4 \}.
\]

Let us define the following two key numbers:

\[
\mu_1 := \min\{c, c_1 - 1\} \text{ and } \mu_2 := \min\{b, c_2 - 1\}.
\]

Since \( x_1^{c_1} = x_3^{c_1} \) and \( x_4^{c_2} = x_3^{c_2}x_3^{\ell c_2} \) in the ring \( S/I(Y) \), a basis for \( S_\alpha/I_\alpha(Y) \) is

\[
\tilde{B}_\alpha = \{ x_1^{a_1}x_2^{d-a_4}x_3^{c-\ell a_4-a_1}x_4^{a_4} | 0 \leq a_4 \leq \mu_2 \text{ and } 0 \leq a_1 \leq \mu_1 \}.
\]

It is clear that \( S_{(c,d)} = x_2^{d-b}S_{(c,b)} \). Since \( x_2 = 1 \) on \( Y \), the images \( ev_Y(S_{(c,d)}) \) and \( ev_Y(S_{(c,b)}) \) of the evaluation maps defined on \( S_{(c,d)} \) and \( S_{(c,b)} \) are the same code \( C_{(c,b),Y} \) when \( d > b \). Hence, if \( |c/\ell| < d \), we have \( b = \min\{|c/\ell|, d\} = |c/\ell| \), and thus the codes \( C_{(c,d),Y} \) and \( C_{(c,b),Y} \) are the same whose dimensions are

\[
\dim_{\mathbb{Q}} C_{\alpha,Y} = H_{\mathbb{Q}}(\alpha) = |\tilde{B}_{(c,b)}|, \text{ for } \alpha = (c,d) \text{ with } b = \min\{|c/\ell|, d\} = |c/\ell|.
\]

Therefore, it suffices to study codes \( C_{\alpha,Y} \), where \( \alpha = (c,d) \) with \( d \leq |c/\ell| \). Thus, we assume from now on that

\[
d \leq |c/\ell| \text{ so that } b = \min\{|c/\ell|, d\} = d.
\]

**The dimension.**

**Case I:** Let \( c = a + b \ell < c_1 \). Then, \( \mu_1 = c \) and thus we have

\[
(8.3) \dim_{\mathbb{Q}} C_{\alpha,Y} = |\tilde{B}_\alpha| = \sum_{a_4=0}^{\mu_2} (c - \ell a_4 + 1) = (\mu_2 + 1)(c + 1) - \mu_2(\mu_2 + 1)\ell/2 = (\mu_2 + 1)[c + 1 - \mu_2 \ell/2].
\]

If \( b \leq c_2 - 1 \), then \( \mu_2 = b \) and thus, we have

\[
\dim_{\mathbb{Q}} C_{\alpha,Y} = (b + 1)[c + 1 - b \ell/2].
\]

It is worth to notice that this dimension is the number of monomials in

\[
\tilde{B}_\alpha = \{ x_1^{a_1}x_2^{d-a_4}x_3^{c-\ell a_4-a_1}x_4^{a_4} | 0 \leq a_4 \leq b \text{ and } 0 \leq a_1 \leq c - \ell a_4 \}
\]

or equivalently the number of lattice points inside the polygon depicted in Figure 2 which is defined by the inequalities \( 0 \leq a_4 \leq b \) and \( 0 \leq a_1 \leq c - \ell a_4 \).

If \( c_2 - 1 < b \), then \( \mu_2 = c_2 - 1 \) and hence, we have

\[
\dim_{\mathbb{Q}} C_{\alpha,Y} = c_2[c + 1 - (c_2 - 1)\ell/2].
\]

As before, this dimension is the number of monomials in

\[
\tilde{B}_\alpha = \{ x_1^{a_1}x_2^{d-a_4}x_3^{c-\ell a_4-a_1}x_4^{a_4} | 0 \leq a_4 \leq c_2 - 1 \text{ and } 0 \leq a_1 \leq c - \ell a_4 \}
\]
or equivalently the number of lattice points inside the polygon depicted in Figure 3 which is defined by the inequalities $0 \leq a_4 \leq c_2 - 1$ and $0 \leq a_1 \leq c - \ell a_4$.

**Case II:** Let $c \geq c_1$. Then $\mu_1 = c_1 - 1$. Recall that $b'$ is the greatest non-negative integer with the property $c - b'\ell \geq c_1 - 1$ and $d - b' \geq 0$. In fact, if $a \geq c_1 - 1$, then $c - b' = a \geq c_1 - 1$, and thus $b' = b$. Otherwise,

$$b' = \lfloor (c - c_1 + 1)/\ell \rfloor = b - \lceil (c_1 - 1 - a)/\ell \rceil.$$  

**Case II(i):** $b' \geq c_2 - 1$.

If $b' \geq c_2 - 1$, then $\mu_2 = c_2 - 1$ as $b \geq b'$. So, for every choice of $a_4$ satisfying $0 \leq a_4 \leq c_2 - 1 \leq b'$ we have $c - \ell a_4 \geq c_1 - 1$, and hence $0 \leq a_1 \leq c_1 - 1$. Thus, we have

$$(8.4) \quad \dim_{\mathbb{F}_q} C_{\alpha,Y} = |\bar{B}_\alpha| = c_1 c_2 = N,$$
which is also the number of lattice points in the rectangle depicted in Figure 4 and described by the inequalities 0 ≤ a₁ ≤ c₁ − 1 and 0 ≤ a₄ ≤ c₂ − 1. Since the dimension reaches its maximum value, the code \( C_{\alpha,Y} \) is trivial, that is, \( \delta(C_{\alpha,Y}) = 1 \).

**Case II(ii):** \( b' < c₂ - 1 \).

By the definition of \( b' \), we have the following two cases:

\[
\min\{c - \ell a₄, c₁ - 1\} = \begin{cases} 
  c₁ - 1 & \text{if } 0 \leq a₄ \leq b' \\
  c - \ell a₄ & \text{if } b' < a₄ \leq \mu₂.
\end{cases}
\]

So, if 0 ≤ a₄ ≤ b’ then 0 ≤ a₁ ≤ c₁ − 1 but if a₄ > b’ then 0 ≤ a₁ ≤ c − \( \ell a₄ \), yielding the description of \( \bar{B}_{\alpha} \) to be the disjoint union of the following two sets:

\[
\begin{align*}
(8.5) \bar{B}_{\alpha}(1) &= \{a₁x₂^{a₄}x₃^{a₄ - a₄}x₄^{c₁ - a₄} | 0 \leq a₄ \leq b' \text{ and } 0 \leq a₁ \leq c₁ - 1\} \\
(8.6) \bar{B}_{\alpha}(2) &= \{a₁x₂^{a₄}x₃^{a₄ - a₄}x₄^{c₁ - a₄} | b' + 1 \leq a₄ \leq \mu₂ \text{ and } 0 \leq a₁ \leq c - \ell a₄\}.
\end{align*}
\]

Notice that \( |\bar{B}_{\alpha}(1)| \) is the number of lattice points in the rectangle in Figure 5 and \( |\bar{B}_{\alpha}(2)| \) is the number of lattice points in the trapezoid in Figure 5. Therefore, we have

\[
\dim_{F_q} C_{\alpha,Y} = \begin{cases} 
  c₁(b' + 1) + \sum_{a₄ = b' + 1}^{\mu₂} (c - \ell a₄ + 1) & \text{if } b' < c₂ - 1 \leq b, \\
  c₁(b' + 1) + (\mu₂ - b')(c + 1 - (\mu₂ + b' + 1)\ell/2) & \text{if } b < c₂ - 1.
\end{cases}
\]

If \( b < c₂ - 1 \), then \( \mu₁ = c₁ - 1 \) and \( \mu₂ = b \) in (8.7), yielding the formula

\[
\dim_{F_q} C_{\alpha,Y} = c₁(b' + 1) + (b - b')(c + 1 - (b + b' + 1)\ell/2).
\]

If \( b' < c₂ - 1 \leq b \), then \( \mu₁ = c₁ - 1 \) and \( \mu₂ = c₂ - 1 \) in (8.7), yielding the formula

\[
\dim_{F_q} C_{\alpha,Y} = c₁(b' + 1) + (c₂ - 1 - b')(c + 1 - (c₂ + b')\ell/2).
\]

**The minimum distance.**

Let us compute the minimum distance now. Recall that \( Y = V_{X(F_q)}(I_L) \) consists of the following points \( P_{i,j} = [\eta₁^i : 1 : 1 : \eta₂^j] \in T_X \), for \( i \in [c₁] \) and \( j \in [c₂] \).
For a given \( F \in S_\alpha \) we set \( J = \{ j \in [c_2] : x_4 - \eta_j^1 x_2 x_3^2 \text{ divides } F \} \). Then, we first prove that the number of zeroes of \( F \) in \( Y \) satisfies
\[
|V_X(F) \cap Y| \leq c_1|J| + (c_2 - |J|) \deg_{x_1} F.
\]

It is clear that \( F(P_{i,j}) = 0 \) whenever \( j \in J \) and there are \( c_1|J| \) many such points in \( Y \). Moreover, the polynomial \( f(x) := F(x_1, 1, 1, \eta_j^2) \in \mathbb{K}[x_1] \setminus \{0\} \) if \( j \notin J \). Thus, it can have at most \( \deg_{x_1} F := \deg(f) \) many zeroes for each \( j \notin J \). So, we can have at most \( (c_2 - |J|) \deg_{x_1} F \) many such roots. Therefore, altogether \( F \) can have at most \( c_1|J| + (c_2 - |J|) \deg_{x_1} F \) zeroes in \( Y \).

**Case I:** Let \( c < c_1 \).

Since \( \deg_{x_1} F \leq c - \ell|J| \) in this case, it follows from (8.8) that
\[
|V_X(F) \cap Y| \leq c_1|J| + (c_2 - |J|)(c - \ell|J|) \leq c_2c + |J|(c_1 - \ell c_2 - c + \ell|J|).
\]

Since \( 0 \leq |J| \leq |c/\ell| \) and \( c_1 \leq \ell c_2 \), we have
\[
|V_X(F) \cap Y| \leq c_2c + |J|(c_1 - \ell c_2 - c + \ell|J|) \leq c_2c.
\]

Therefore, \( F \) can have at most \( c_2c \) many zeroes in \( Y \). On the other hand, the following polynomial
\[
F = x_2^\ell \prod_{i=1}^c (x_1 - \eta_i^1 x_3) \in S_\alpha
\]
vanishes exactly at the \( c_2c \) points \( P_{i,j} = [\eta_i^1 : 1 : 1 : \eta_j^2] \in Y \), where \( 1 \leq i \leq c \) and \( 1 \leq j \leq c_2 \). Thus, there is a codeword \( ev_{\alpha,Y}(F) \) with weight \( c_1c_2 - c_2c \). Hence,
\[
\delta(C_{\alpha,Y}) = c_1c_2 - c_2c = c_2(c_1 - c).
\]

**Case II:** Let \( c \geq c_1 \). Then, we elaborate more on the upper bound given in (8.8) depending on whether \( |J| \leq b' \) or \( |J| > b' \).

Suppose that \( 0 \leq |J| \leq b' \). Since \( \deg_{x_1} F \leq c_1 - 1 \), it follows from (8.8) that
\[
|V_X(F) \cap Y| \leq c_1|J| + (c_2 - |J|)(c_1 - 1) = c_2(c_1 - 1) + |J|.
\]

Since \( 0 \leq |J| \leq b' \), we have
\[
|V_X(F) \cap Y| \leq c_2(c_1 - 1) + b'.
\]

Suppose now that \( |J| > b' \). In this case, we write \( |J| = b' + k \) for some positive integer \( k \). Then, \( c - \ell(b' + 1) < c_1 - 1 \) or equivalently \( c - \ell(b' + 1) \leq c_1 - 2 \), by definition of \( b' \), which will be crucial below. Hence,
\[
c - \ell|J| = c - \ell(b' + 1) - \ell(|J| - b' - 1) \leq c_1 - 2 - \ell(k - 1).
\]

Since \( \deg_{x_1} F \leq c - \ell|J| \leq c_1 - 2 - \ell(k - 1) \), it follows from (8.8) that
\[
|V_X(F) \cap Y| \leq c_1|J| + (c_2 - |J|)(c - \ell|J| - c_1 + 1 + c_1 - 1) \leq c_1c_2 - c_2 + (c_2 - |J|)(c - \ell|J| - c_1 + 1 + |J|) \leq c_2(c_1 - 1) + (c_2 - |J|)(-1 - \ell(k - 1)) + |J|.
\]

Since \( b' - |J| = -k \), \( c_2 - |J| \geq 1 \) and \( \ell \geq 1 \) the difference
\[
b' - |J| + (c_2 - |J|)(-1 - \ell(k - 1)) = (b' - |J|) + (c_2 - |J|)(1 + \ell(k - 1)) \geq 0
\]
and thus we have that
\[
|V_X(F) \cap Y| \leq (c_1 - 1)c_2 + b'.
\]
Then, by (8.10) and (8.11), $F$ can have at most $(c_1 - 1)c_2 + b'$ many zeros in $Y$. On the other hand, the following polynomial

$$F = x_3^{c - b'} - (c_1 - 1)x_2^{d - b'} \prod_{i=1}^{c_1 - 1} (x_1 - \eta_i^2x_3) \prod_{j=1}^{b'} (x_4 - \eta_j^2x_2x_3^j)$$

vanishes exactly at $c_1 b' + (c_2 - b')(c_1 - 1) = c_2(c_1 - 1) + b'$, and thus there is a codeword with weight $c_2 - b'$. This shows that $\delta(C_{\alpha,Y}) = c_2 - b'$.

**Remark 8.5.** Let $(c,d) = (a + \ell b, a' + b)$. If $a \geq c_1 - 1$, then $c - \ell b = a \geq c_1 - 1$. So, $b' = b$. Since $b' = b < c_2 - 1$, then by (8.7) above $H_Y(\alpha) = |B_\alpha| = c_1(b+1)$. It follows that the codes $C_{\alpha,Y}$ with $a > c_1 - 1$ are equivalent to those with $a' = 0$ by the explanations above (8.2), and the codes with $b' \geq c_2 - 1$ are trivial, it suffices to consider codes corresponding to $(c,d) = (a + \ell b, b)$ where $a \leq c_1 - 1$ and $b' < c_2 - 1$.

The following makes the points of Remark 8.5 more precise as the extra condition $\ell \geq c_1$ bounds $b$ by $c_2 - 1$ and reduces the number of non-equivalent codes to $c_1 c_2$.

**Corollary 8.6.** Let $\{c_1u_1, c_2u_2\}$ be a basis for $L$, and $Y = V_X(I_L)(\mathbb{F}_q)$ be the subgroup of the torus $T_X$ of the Hirzebruch surface $\mathcal{H}_\ell$ over $K = \mathbb{F}_q$ for which $c_1$ and $c_2$ divides $q - 1$. If $\alpha = (c,d) = (a + \ell b, d)$ and $\ell \geq c_1$, then the parameters of the toric code $C_{\alpha,Y}$ are $\alpha = c_1 c_2$.

$$K = a + 1 \quad \text{and} \quad \delta' = c_2(c_1 - a), \quad \text{if} \quad c < c_1$$

$$K = c_1 b + 1 + a \quad \text{and} \quad \delta' = c_2 - b' + 1, \quad \text{if} \quad a < c_1 - 1 < c$$

$$K = c_1(b + 1) \quad \text{and} \quad \delta' = c_2 - b, \quad \text{if} \quad a = c_1 - 1 < c.$$  

Furthermore, $(c_1 - 1 + \ell(c_2 - 1), c_2 - 1) + \mathbb{N}^2 = \text{reg}(Y)$.

**Proof.** Let $\ell \geq c_1$. We may suppose that $a \leq c_1 - 1$ by the virtue of Remark 8.5. Since $a \leq c_1 - 1$, it follows that $b' = b$ if $a = c_1 - 1$ and $b' = b - 1$ if $a = c - \ell b < c_1 - 1$ as $c - \ell(b - 1) = c - \ell b + \ell \geq c_1 - 1$. So, if $b \geq c_2$, then $b' < c_2 - 1$ and thus the code is trivial by (8.4). Thus, non-equivalent codes occur only for $a = a(1,0) + b(\ell,1)$ where $0 \leq a \leq c_1 - 1$ and $0 \leq b \leq c_2 - 1$.

**Case I:** If $c = a + \ell b < c_1 \leq \ell$, then $0 \leq a < \ell(1 - b)$ implying that $b = 0$. Hence, $\text{dim}_{\alpha,Y} = H_Y(\alpha,0) = a + 1$ and $\delta(C_{\alpha,Y}) = c_2(c_1 - a)$ by Theorem 8.4, since $c = a$.

**Case II:** Let $c \geq c_1$. We appeal to Theorem 8.4 again.

If $a = c_1 - 1$, then $b' = b$ and $\text{dim}_{\alpha,Y} = H_Y(\alpha) = c_1(b+1)$. Furthermore, we have $\delta(C_{\alpha,Y}) = c_2 - b' = c_2 - b$.

If $a < c_1 - 1$, then $b' = b - 1$ and $\text{dim}_{\alpha,Y} = H_Y(\alpha) = c_1 b + c + 1 - \ell b = c_1 b + a$. Moreover, we have $\delta(C_{\alpha,Y}) = c_2 - b' = c_2 - b + 1$.

The final claim follows easily, since the the values $a + 1, c_1 b + a$ and $c_1(b+1)$ of $K$ above are strictly smaller than $c_1 c_2$ whenever $0 \leq a < c_1 - 1$ and $0 \leq b < c_2 - 1$, and $K = H_Y((c_1 - 1 + \ell(c_2 - 1), c_2 - 1)) = c_1 c_2$ as $a = c_1 - 1$ and $b = c_2 - 1$.

We finish the paper with a toy example illustrating the theory we developed.

**Example 8.7.** Let $X = \mathcal{H}_3$ over $\mathbb{F}_7$. Let $c_1 = 3, c_2 = 3$. Then the parameters of the code are given in Table 1. According to Markus Grassl’s Code Tables [11] a best-possible code with $N = 9$ has $K + \delta = 9$ or $K + \delta = 10$ (MDS codes). This
example provides us with a best possible code whose parameters are $[9, 7, 2]$ together with an MDS code $[9, 8, 2]$.

Table 1: Parameters of Toric Codes on $X = \mathcal{H}_3$.

| $(a, b)$ | $\alpha$ | $[N, K, \delta]$ |
|----------|-----------|--------------------|
| $(0, 0)$ | $(0, 0)$  | $[9, 1, 9]$        |
| $(1, 0)$ | $(1, 0)$  | $[9, 2, 6]$        |
| $(2, 0)$ | $(2, 0)$  | $[9, 3, 3]$        |
| $(0, 1)$ | $(3, 1)$  | $[9, 4, 3]$        |
| $(1, 1)$ | $(4, 1)$  | $[9, 5, 3]$        |
| $(2, 1)$ | $(5, 1)$  | $[9, 6, 2]$        |
| $(0, 2)$ | $(6, 2)$  | $[9, 7, 2]$        |
| $(1, 2)$ | $(7, 2)$  | $[9, 8, 2]$        |
| $(2, 2)$ | $(8, 2)$  | $[9, 9, 1]$        |

Acknowledgement

The author thanks Laurence Barker for his contribution explained in Remark 4.5 and Ivan Soprunov for his useful comments on the manuscript. He also expresses his gratitude to an anonymous referee who reads the paper carefully and helped improve the presentation considerably.

References

[1] Esma Baran and Mesut S¸ahin. On parameterised toric codes. Appl. Algebra Engrg. Comm. Comput., 2021.
[2] Esma Baran Özkan. Vanishing ideals of parameterized subgroups in a toric variety. Turkish J. Math., 46(6):2141–2150, 2022.
[3] Peter Beelen and Diego Ruano. The order bound for toric codes. In Applied algebra, algebraic algorithms, and error-correcting codes, volume 5527 of Lecture Notes in Comput. Sci., pages 1–10. Springer, Berlin, 2009.
[4] D. N. Bernstein. The number of roots of a system of equations. Funkcional. Anal. i Priloˇzen., 9(3):1–4, 1975.
[5] Gavin Brown and Alexander M. Kasprzyk. Seven new champion linear codes. LMS J. Comput. Math., 16:109–117, 2013.
[6] David A. Cox. The homogeneous coordinate ring of a toric variety. J. Algebraic Geom., 4(1):17–50, 1995.
[7] David A. Cox, John B. Little, and Henry K. Schenck. Toric varieties, volume 124 of Graduate Studies in Mathematics. American Mathematical Society, Providence, RI, 2011.
[8] Eduardo Dias and Jorge Neves. Codes over a weighted torus. Finite Fields Appl., 33:66–79, 2015.
[9] David Eisenbud and Bernd Sturmfels. Binomial ideals. Duke Math. J., 84(1):1–45, 1996.
[10] Sudhir R. Ghorpade. A note on Nullstellensatz over finite fields. In Contributions in algebra and algebraic geometry, volume 738 of Contemp. Math., pages 23–32. Amer. Math. Soc., [Providence], RI, [2019] ©2019.
[11] Markus Grassl. Bounds on the minimum distance of linear codes and quantum codes. Online available at http://www.codetables.de, 2007. Accessed on 2023-01-17.
[12] Johan P. Hansen. Toric varieties Hirzebruch surfaces and error-correcting codes. Appl. Algebra Engrg. Comm. Comput., 13(4):289–300, 2002.
[13] Birkett Huber and Bernd Sturmfels. A polyhedral method for solving sparse polynomial systems. Mathematics of Computation, 64(212):1541–1555, 1995.
[14] Nathan Jacobson. Basic algebra. I. W. H. Freeman and Company, New York, second edition, 1986.
Delio Jaramillo, Maria Vaz Pinto, and Rafael H. Villarreal. Evaluation codes and their basic parameters. *Des. Codes Cryptogr.*, 89(2):269–300, 2021.

David Joyner. Toric codes over finite fields. *Appl. Algebra Engng. Comm. Comput.*, 15(1):63–79, 2004.

A. G. Kušnirenko. Newton polyhedra and Bezout’s theorem. *Funkcional. Anal. i Priložen.*, 10(3):82–83, 1976.

John B. Little. Remarks on generalized toric codes. *Finite Fields Appl.*, 24:1–14, 2013.

Hiram H. López and Rafael H. Villarreal. Computing the degree of a lattice ideal of dimension one. *J. Symbolic Comput.*, 65:15–28, 2014.

Diane Maclagan and Gregory G. Smith. Uniform bounds on multigraded regularity. *J. Algebraic Geom.*, 14(1):137–164, 2005.

José Martínez-Bernal, Yuriko Pitones, and Rafael H. Villarreal. Minimum distance functions of graded ideals and Reed-Muller-type codes. *J. Pure Appl. Algebra*, 221(2):251–275, 2017.

Ezra Miller and Bernd Sturmfels. *Combinatorial Commutative Algebra*. Cambridge Studies in Advanced Mathematics. Springer-Verlag New York, 2005.

Marcel Morales and Apostolos Thoma. Complete intersection lattice ideals. *J. Algebra*, 284(2):755–770, 2005.

Liam O’Carroll, Francesc Planas-Vilanova, and Rafael H. Villarreal. Degree and algebraic properties of lattice and matrix ideals. *SIAM J. Discrete Math.*, 28(1):394–427, 2014.

Carlos Rentería-Márquez, Aron Simis, and Rafael H. Villarreal. Algebraic methods for parameterized codes and invariants of vanishing ideals over finite fields. *Finite Fields Appl.*, 17(1):81–104, 2011.

Diego Ruano. On the structure of generalized toric codes. *J. Symbolic Comput.*, 44(5):499–506, 2009.

Ivan Soprunov. Toric complete intersection codes. *J. Symbolic Comput.*, 50:374–385, 2013.

Mesut Şahin. Toric codes and lattice ideals. *Finite Fields Appl.*, 52:243–260, 2018.

Mesut Şahin and Ivan Soprunov. Multigraded Hilbert functions and toric complete intersection codes. *J. Algebra*, 459:446–467, 2016.

Rafael H. Villarreal. *Monomial algebras*. Monographs and Research Notes in Mathematics. CRC Press, Boca Raton, FL, second edition, 2015.

Department of Mathematics, Hacettepe University, Ankara, TURKEY

Email address: mesut.sahin@hacettepe.edu.tr