TORIC RESIDUE CODES: I

ROY JOSHUA AND REZA AKHTAR

Abstract. In this paper, we begin exploring the construction of algebraic codes from toric varieties using toric residues. Though algebraic codes have been constructed from toric varieties, they have all been evaluation codes, where one evaluates the sections of a line bundle at a collection of rational points. In the present paper, instead of evaluating sections of a line bundle at rational points, we compute the residues of differential forms at these points. We show that this method produces codes that are close to the dual of those produced by the first technique. We conclude by studying several examples, and also discussing applications of this technique to the construction of quantum stabilizer codes and also to decryption of toric evaluation codes.

Table of Contents

1. Introduction
2. Review of basic techniques
3. Toric residue codes
4. Duality results and estimation of parameters
5. Examples
6. Application I: The construction of quantum stabilizer codes from toric varieties
7. Application II: Decryption of toric evaluation codes
8. Appendix
References

The first author was supported by the IHES, MPI (Bonn) and a grant from the NSA.
1. Introduction

This is the first in a series of papers exploring the construction of algebraic codes using toric residues. The technique of toric residues was introduced by David Cox in [3], and studied extensively by several authors: see [4], [6], [7], [8] and [9]. The present paper started with trying to apply the corresponding toric residue theorems to construct codes from toric varieties which could be candidates for duals of toric evaluation codes. For this, one needs to resolve problems on several fronts:

- The first is to establish certain basic results for toric residues over finite fields, extending those already studied and worked out in the above papers. (See Theorem 1.1 below, for example.)

- A technique that has proven convenient for constructing evaluation codes from higher dimensional varieties is to apply methods of intersection theory. (See [16] and [17].) One needs to extend such techniques to codes constructed using toric residues. (See section 3.2.)

- In the case of projective algebraic curves, the Riemann-Roch theorem enables one to compute the parameters of the dual code, and the residue theorem enables one to relate residue codes on curves to the dual of evaluation codes. One also needs to find suitable replacements for these techniques. (See Proposition 4.8 and Corollary 4.10.)

- In order to apply the above techniques to the construction of quantum stabilizer codes, one needs to be able to apply the above techniques to construct codes that contain their dual codes. (See Theorem 4.13.)

In the present paper we make a start in this direction, by carrying out this program for toric surfaces, and we hope to consider higher dimensional cases like toric three-folds elsewhere. A major motivation for us in studying toric residue codes is to construct quantum stabilizer codes from toric varieties.

We will presently try to condense the main ideas of the paper. As discussed in the next section, we begin with evaluation codes, i.e., codes obtained by evaluating sections of line bundles on toric varieties at a specified number of rational points on the toric variety. If $X$ is the toric variety, defined over the finite field $k$, $E$ is a divisor on $X$ and $P = \{P_1, \ldots, P_m\}$ denotes a set of $k$-rational points on $X$, $C(X, E, P)$ will denote this code. The parameters of such codes have been analyzed (mainly for toric surfaces) using intersection theory: see [16].

The new construction we introduce here is that of residue codes, where instead of the set of sections of a line bundle, $\Gamma(X, \mathcal{O}_X(E))$, one starts with $\Gamma(X, \omega_X(E))$, which is a set of differential forms, and takes the residues of these forms at a specified number of given $k$-rational points $P = \{P_1, \ldots, P_m\}$. Such residue codes have been so far considered only for curves, and their importance, at least for curves, stems from the fact that these residue codes on curves provide duals to the evaluation codes. (Here dual means the dual code in the sense of standard coding theory.) In fact, the classical residue theorem for curves plays a key role in proving the appropriate form of duality in this context which then makes it possible to construct quantum stabilizer codes from algebraic curves. Together with Riemann-Roch for curves, one can then estimate the parameters of evaluation codes and residue codes on complete smooth curves. In section 2, we review the basic techniques applying intersection theory to estimate parameters of evaluation codes as well as basic material on toric residues. Section 3 begins with introducing toric residue codes. We follow this by extending the Hansen technique of using intersection theory to estimate parameters of residue codes. This is followed by a detailed list of hypotheses that need to be satisfied by the toric variety and a line bundle on it, so that one may construct codes from it.

In section 4, we begin by proving the following theorem which will play a key role in the construction of toric residue codes. Throughout the paper $k$ will denote a fixed finite field of characteristic $p$.

**Theorem 1.1.** (See Theorem 4.3.) Assume that $X$ is a projective smooth toric variety of dimension $d$ defined over $k$ by a polytope $P$. Let $D_i$, $i = 1, \ldots, d$ denote $d$ effective ample divisors on $X$ and let $\cap_{i=1}^d D_i = \{R_i\}$ denote a set of $k$-rational points. Assume, in addition to the above situation, that for each point $R_i$ one is given $v_i(R) \in k^*$ so that the sum $\Sigma_i v_i(R_i) = 0$. Then there exists a differential form $\eta \in \Gamma(X, \omega_X(\Sigma_i D_i))$ so that $Res_{R_i}(\eta) = v_i(R_i)$.

This theorem follows along the same lines as the proof of the corresponding statement for non-singular projective complex algebraic varieties in the place of $X$: see [14, (3.8) Theorem]. The main difference is that, such a statement in not true in general in positive characteristic - see [?, LaRa] however the technique of Frobenius splitting for toric varieties enables one to prove such a result for projective smooth toric varieties. We provide a complete proof of this theorem in section 4.

For the remainder of the paper, we consider codes, $C(X, \omega_X, E, P)$ where $X$ is a smooth toric variety defined over a finite field $k$, $E$ is divisor on $X$, $\omega_X$ is the sheaf of top differential forms on $X$, and $P$ is a given set of
Theorem 1.2. Let $X$ denote a smooth projective toric variety defined over a finite field $k = \mathbb{F}_{2^n}$ with polytope $\Delta$, and $X$ satisfying the basic hypotheses in 3.3. Let $\mathcal{P} = \{P_1, \ldots, P_m\}$ be a set of $k$-rational points on $X$, and $D, E$ divisors on $X$ all chosen as in 3.4. Then the modified residue code $C(X, \omega_X, E, \mathcal{P})$ (defined as in 4.3) maps surjectively onto the dual code $C(X, E, \mathcal{P})^\perp$. Therefore, the dual code $C(X, E, \mathcal{P})^\perp$ has length $m$ and dimension at least $m - P$ (where $P$ is the number of lattice points in the polytope corresponding to the effective divisor $E$); moreover, the minimum distance of $C(X, E, \mathcal{P})^\perp$ is at least the minimum distance of the residue code $C(X, \omega_X, E, \mathcal{P})$.

The remainder of this section is devoted to applying this theorem to compute parameters of dual codes: here the various hypotheses we listed in section 3 on the choice of rational points and the line bundle play an important role. Theorem 4.13 then shows how to obtain codes containing their dual codes this way which would be useful in constructing quantum stabilizer codes on toric surfaces.

In section 5, we discuss several examples in detail: for example, construction of toric residue codes on the projective plane, the projective plane with a point blown-up, and on Hirzebruch surfaces $F_2$. One cannot construct quantum stabilizer codes for the usual $\mathbb{P}^2$, but nevertheless, we analyze this basic example in detail. We also explicitly compute the dimensions of the space of global sections for the residue code and the dual code in this case: this analysis seems valid only over the complex numbers, but nevertheless we hope it sheds some insight into the relationship between the dimensions of these two spaces of global sections as stated in the last theorem. This is followed by studying some applications of these techniques. This is explored in section 6 following upon the discussion in the last two examples discussed in section 5. One may summarize some of these results in the following examples. In both of these examples $c = |\mathbb{F}_q| = 2^{2t}$. In each case, a quantum stabilizer code with length $m$ (which is the number of $k$-rational points where the residues are taken), dimension $= k_Q$, and distance $= d_Q$ is constructed by starting with two (classical) residue codes with parameters $m, k, d$ and $m, k', d'$. (The reader may consult the beginning of section 6, where we recall some of the background material on the construction of quantum stabilizer codes. The values of $k, k', d$ and $d'$ are computed in the last two examples in section 5.)

Examples 1.3. The projective space $\mathbb{P}^2$ with a point blown-up. In this case we construct quantum stabilizer codes with parameters given by

$$
\begin{align*}
\text{(1.0.1)} & \quad k_Q = 2t(k + k' - n) \geq 2t((92/360)c^2 - 3c + 2) \\
& \quad d_Q = \min(d, 3/2d') \geq c^2/2 + (1/6)c + 2
\end{align*}
$$

The Hirzebruch surface $F_2$. In this case the parameters of the corresponding quantum stabilizer codes are given by

$$
\begin{align*}
\text{(1.0.2)} & \quad k_Q = 2t(k + k' - n) \geq 2t((598/1440)c^2 - 3c + 2) \\
& \quad d_Q = \min(d, 3/2d') \geq c^2/2 + (13/12)c + 4
\end{align*}
$$

We conclude the paper by discussing briefly applications of toric residue codes to the decryption of toric evaluation codes. The authors plan to extend these techniques to higher dimensional toric varieties in the future.

Throughout the paper $k$ will denote a finite field of characteristic $p$. We will restrict to the category of smooth projective toric varieties over $k$. We would like to point out that though we work over a fixed finite field, it may become necessary to consider a finite extension for all our results to hold fully.

2. Review of basic techniques

In this section, which should serve as a reference, we recall the definition of evaluation codes from algebraic varieties over finite fields and a technique, first introduced in [16] for estimating their parameters using methods of intersection theory. We also quickly review rational differential forms on toric varieties and their residues following [3].
2.1. Evaluation codes and their parameters via intersection theory.

**Definition 2.1** (Code definition). Let $X$ be a smooth projective variety of dimension $d$ over a finite field $k$, and let $\mathcal{L}$ be a line bundle on $X$ also defined over $k$. Given $P_1, P_2, \ldots, P_M$ distinct $k$-rational points on $X$, fix isomorphisms $\mathcal{L}_{P_i} \otimes k(P_i) \cong k$ at each stalk (induced from the local triviality of the line bundle $\mathcal{L}$). Define the **code** $C(X, \mathcal{L})$ as the image of the germ map

$$\alpha : \Gamma(X, \mathcal{L}) \to \bigoplus_{i=1}^{M} L_{P_i} \cong k^M$$

In case $\mathcal{L} = \mathcal{O}_X(E)$ is the line bundle associated to the divisor $E$, and the given points $P_1, P_2, \ldots, P_M$ do not intersect with the polar part of $E$, this map is evaluation of a section of $\mathcal{L}$, viewed as a rational function, at each $P_i$. (i.e. We send a section of $\mathcal{L}$ viewed as a rational function $f$ to the image of $f \in \mathcal{O}_{X, P_i}/m_{P_i} \cong k$.)

**Remarks 2.2.** 1. Observe also that the definition of the code using the germ map depends on the choice of a local trivialization. However, different trivializations clearly lead to equivalent codes.

2. Observe that now $\Gamma(X, \mathcal{L}) = \{ f \in K(X) | (f) + E \geq 0, \text{ or } f = 0 \}$ where $K(X)$ denotes the function field of $X$.

3. Observe that the hypothesis that the poles of $E$ and $\{ P_i \}$ are disjoint will be satisfied by replacing the divisor $E$, if necessary, with a linearly equivalent divisor (possibly after a finite extension of the base field): see [24, p. 134, Theorem 1]. Therefore, we will henceforth assume always that this hypothesis is satisfied.

Next we will consider the following rather (by-now) well-known result in producing codes from higher dimensional algebraic varieties.

**Theorem 2.3.** [16, Theorem 5.9] Suppose $X$ is a smooth and projective variety over $k$, $d = \dim X \geq 2$, and $C_1, C_2, \ldots, C_n$ are irreducible curves on $X$ with $k$-rational points $P_1, P_2, \ldots, P_M$ lying on the union of the $C_i$’s. Assume there are $\leq b$ $k$-rational points on each $C_i$. Let $\mathcal{L} = \mathcal{O}_X(G)$ be a line bundle with associated divisor $G$ such that the intersection numbers $G \cdot C_i \geq 0$ for all $i$. Let

$$l = \sup_{s \in \Gamma(X, \mathcal{L})} \# \{ i : C_i \subseteq Z(s) \}$$

where $Z(s)$ is the divisor of zeros of $s$, $s$ being a section of $\mathcal{L}$. Then the code $C(X, \mathcal{L})$ has length $M$ and minimum distance

$$d \geq M - lb - \sum_{i=1}^{n} G \cdot C_i$$

If $G \cdot C_i = \delta \leq N$ for all $i$ then

$$d \geq M - lb - (n-1)\delta$$

In particular, if $X$ is a non-singular surface, $H$ is a nef divisor on $X$ with $H \cdot C_i > 0$, then

$$l \leq \frac{D \cdot H}{\min \{ C_i \cdot H \}}$$

Thus if $G \cdot H < C_i \cdot H$ for all $i$, then $l = 0$ and $d \geq M - \sum_{i=1}^{n} G \cdot C_i$

2.2. (Rational) Differential forms and Residues. To do this systematically we will begin with a discussion of differential forms on projective spaces followed by one on differential forms on smooth toric varieties. We will closely follow [3] in these.

Let $f_0, \ldots, f_d$ denote homogeneous polynomials of degree $n$ which do not vanish simultaneously on $k^{d+1}$ except at the origin, and let $g$ be homogeneous polynomial of degree $\rho = (d+1)(n-1)$. Then we consider the $d$-form

$$\Omega = \sum_{i=0}^{d} (-1)^i x_i \, dx_0 \wedge \cdots \wedge \widehat{dx_i} \wedge \cdots \wedge dx_d$$

As is well-known, our assumptions on $g$ and $f_0, \ldots, f_d$ imply that

$$\omega_g = \frac{g \, \Omega}{f_0 \cdots f_d}$$

descends to a global rational $d$-form on $\mathbb{P}^d$, also denoted $\omega_g$. The affine open sets

$$U_i = \{ x \in \mathbb{P}^d : f_i(x) \neq 0 \}$$
clearly form an open cover $\mathcal{U}$ of $\mathbb{P}^d$, and $\omega_\rho$ is regular on $U_0 \cap \cdots \cap U_d$, so it is a Čech co-chain in $C^d(\mathcal{U}, \Omega^0_{\mathcal{P}^d})$. Further, since $\mathcal{U}$ has $d+1$ elements, $\omega_\rho$ is a Čech co-cycle and thus defines a class $[\omega_\rho] \in H^d(\mathcal{U}, \Omega^0_{\mathcal{P}^d}) \cong H^d(\mathbb{P}^d, \Omega^0_{\mathcal{P}^d})$.

Observe that on the open affine sub-scheme where $x_0 \neq 0$, the form $\Omega$ reduces to $d\left(\frac{x_1}{x_0}\right) \wedge \cdots \wedge d\left(\frac{x_d}{x_0}\right)$ since $\frac{x_1}{x_0}, \ldots, \frac{x_d}{x_0}$ form a local system of parameters on this sub-scheme.

We will next consider a $d$-dimensional projective toric variety $X$ over the fixed field $k$. $X$ is now determined by a complete fan $\Sigma$ in $\mathbb{R}^d$. As usual, $\mathbb{M}$ will denote the dual lattice of $\mathbb{N}^d = \mathbb{Z}^d$ (= the lattice of characters of the dense torus $T$), and $\Sigma(1)$ will denote the set of 1-dimensional cones in $\Sigma$. Each $\rho \in \Sigma(1)$ determines a divisor $D_\rho$ on $X$ and a generator $n_\rho \in \mathbb{N} \cap \rho$. (Standard references for toric varieties are [15] and [23].) Alternatively, one may assume that the toric variety is defined by a convex polytope in $\mathbb{M} \mathbb{R}$ where the vertices are all assumed to have rational co-ordinates. One takes the polynomial ring $S$ over the base field $k$ in variables $x_\rho$ corresponding to each of the faces $\rho$ of the polytope. Two monomials $\Pi_\rho x_\rho^{m_\rho}$ and $\Pi_\mu x_\mu^{m_\mu}$ are identified if there exists a character $m \in \mathbb{M}$ so that $a_\rho = m_n, n_\rho = +b_\rho$ for all $\rho$ where $n_\rho$ is the primitive generator in $\mathbb{N}$ of the half-line $\mathbb{R}_+ \rho$. Therefore, the degree of the monomial $\Pi_\rho x_\rho^{m_\rho}$ is given by the class of the corresponding divisor $\sum_i a_\rho D_\rho \in CH_1(X)$ where $D_\rho$ is the divisor corresponding to the face $\rho$ and $CH_1(X)$ denotes the Chow-group of dimension 1-cycles modulo rational equivalence.

As explained in [4], $X$ has the homogeneous coordinate ring $S = k[\mathcal{X}]$, which is graded by the Chow group $A_{d-1}(X)$ so that a monomial $\Pi_\rho x_\rho^{m_\rho}$ has degree defined above. Given a class $\alpha \in A_{d-1}(X)$, we let $S_\alpha$ denote the graded piece of $S$ in degree $\alpha$; we write $\deg(f) = \alpha$ when $f \in S_\alpha$.

We next construct an analog of the form (2.2.1). Fix an integer basis $m_1, \ldots, m_d$ for the lattice $\mathbb{M}$. Then, given a subset $I = \{i_1, \ldots, i_d\} \subset \Sigma(1)$ consisting of $d$ elements, we let

$$\det(n_I) = \det((m_i, n_{i_\rho})_{1 \leq i, \rho \leq d}) .$$

$(n_{i_\rho})$ denote the primitive vectors in the lattice $\mathbb{M}$ along the rays $\rho_{i_\rho}$.) Also set $dx_I = dx_{i_1} \wedge \cdots \wedge dx_{i_d}$ and $\hat{x}_I = \Pi_\rho x_\rho^{m_\rho}$. Note that $\det(n_I)$ and $dx_I$ depend on how the $\rho \in I$ are ordered, while their product $\det(n_I)dx_I$ does not. Then we define the $d$-form $\Omega$ by the formula

$$\Omega = \sum_{|I| = d} \det(n_I) \hat{x}_I dx_I$$

where the sum is over all $d$-element subsets $I \subset \Sigma(1)$. This form is well-defined up to $\pm 1$, the sign depending on the ordering of the basis $m_1, \ldots, m_d$. We will call this an Euler form.

Now consider the graded $S$-module $\hat{\Omega}_d^S = S : \Omega$, where $\Omega$ is considered to have degree $\beta_0 = \sum_\rho \deg(x_\rho) = \sum_\rho D_\rho = A_{d-1}(X)$.

Thus $\hat{\Omega}_d^S \simeq S(-\beta_0)$ as graded $S$-modules. By [4, section 3], every graded $S$-module gives rise to a sheaf on $X$, and by [5, Section 9], the sheaf associated to $\hat{\Omega}_d^S$ is exactly $\omega_X = \omega X$ of the differential forms of degree $d$. Furthermore, we can describe sections of $\omega_X$ with prescribed poles as follows: see [3, Proposition 2.1].

Let $\alpha \in A_{d-1}(X)$ be the class of a Cartier divisor, and let $Y \subset X$ be defined by the vanishing of $f \in S_\alpha$. Then

$$H^0(X, \omega_X(Y)) = \left\{ g \frac{\Omega}{f} : g \in S_{\alpha-\beta_0} \right\} \simeq S_{\alpha-\beta_0}$$

If we choose $f_0, \cdots, f_\beta \in S_{\beta}$, then $f = f_0 \cdots f_\beta \in S_{(d+1)\beta}$. For each $g \in S_{(d+1)\beta-\beta_0}$, we obtain a $d$-form

$$\omega_g = g \frac{\Omega}{f_0 \cdots f_\beta} \in \omega_X(U_0 \cap \cdots \cap U_d)$$

(Here $U_i$ is the complement in $X$ of the zero locus of $f_i$.) Hence $[\omega_\rho]$ defines a class in the Čech cohomology $H^d(X, \omega_X) \cong H^d(X, \omega_X)$ for all $g$. Moreover, if $D_i = Z(f_i)$, then $Z(f_0 \cdots f_\beta) = \sum_i D_i = D$. Therefore, the same $\omega_g$ defines an element of $\Gamma(X, \omega_X(D))$: see Definition 3.1 below. The toric residue of such an $\omega_g$ is defined in [3] to be the image of this element under the trace map $Tr : H^d(X, \omega_X) \rightarrow k$.

2.3. Cartier divisors associated to rational differential forms. Recall a rational differential form is a global section of the sheaf $K(X) \otimes \omega_X$. Choosing a local trivialization of $\omega_X$ by the open cover $\{U_i|i\}$ of $X$ with transition functions given by $\omega_{i,j} \in \Gamma(U_i \cap U_j, \Omega_X)$, this means a rational differential form on $X$ is given by a collection $\{(V_i, f_i)\}_{i \in (V_i)|i|}$, where $\{V_i|i\}$ is an open cover of $X$ possibly refining $\{U_i|i\}$ so that on $U_i \cap U_j$,
\[ f_i = g_{i,j} f_j. \] Clearly the same data \( \{(V_i, f_i) \mid f_i \in K(V_i), i \} \) defines a Cartier divisor on \( X \) which we call the Cartier divisor associated to the given rational differential form. If \( \omega \) is a rational differential form, \( (\omega) \) will denote the associated Cartier divisor.

By taking the covering \( \{V_i|i\} \) to be also a refinement of the affine open cover defined by the fan, one may see that \( \omega_\Delta \) above is a rational differential form, and that conversely any rational differential form may be expressed as \( \omega_\Delta \) for a suitable choice of \( g \) and \( f_0, \ldots, f_d \). (This observation follows readily from the construction of the homogeneous coordinate ring of a toric variety as in [4]: see especially [4, Lemma 2.2].)

**Definition 2.4.** In particular we let \( \omega_{can} = \Omega_{\sum E \Delta(1)} \). The associated Cartier divisor is clearly the canonical divisor \( K = -\Sigma \rho \in \Sigma(1) D_\rho \).

3. Toric residue codes

3.1. Definition of Toric residue codes.

**Definition 3.1.** Let \( X \) be a smooth projective toric variety as before of pure dimension \( d \) defined over a finite field \( k \), with \( c = \mid k^* \mid \). Assume that \( \{D_i|i = 1, \ldots, d\} \) are \( d \) effective divisors whose union of supports contains the discrete set of \( k \)-rational points \( \mathcal{P} = \{P_i|i = 1, \ldots, m\} \). If \( E \) is a divisor and \( \mathcal{L} \cong \mathcal{O}(E) \) is the associated line bundle, \( \omega_X(E) \) will denote \( \omega_X \otimes \mathcal{L} \). Now

\[
\Gamma(X, \omega_X(E)) = \{ \omega \in \Gamma(X, K(X) \otimes_{\mathcal{O}_X} \omega_X) \mid (\omega) + E \geq 0, \omega = 0 \}
\]

Instead of using the map in 2.1 to map this code to \( k^m \), we will make use of the following **Residue** map by sending the form \( \omega \) to \( (Res_{\mathcal{P}}(\omega), \ldots, Res_{\mathcal{P}}(\omega)) \). Here \( Res_{\mathcal{P}}(\omega) \) denotes the local Grothendieck residue of \( \omega \) at \( P_i \). This code will be denoted \( C(X, \omega_X(E), \mathcal{P}) \). This will be called the **residue code** associated to the line bundle \( \mathcal{O}(E) \) and the set of rational points \( \mathcal{P} \).

3.2. Extension of the Hansen technique to toric residue codes. Henceforth we will make the following assumptions: the set \( \{P_i|i = 1, \ldots, m\} \) of rational points are all in the dense orbit and all their co-ordinates are non-zero. We begin with the following observation (see [8, (0.4)]) on residues of rational functions on an \( n \)-dimensional split torus:

**Proposition 3.2.** Let \( g_1, \ldots, g_d, h \in k[t_1, \ldots, t_d] \) so that the following holds. Let \( u < \mid k^* \mid \). For each \( i = 1, \ldots, d \), \( j = 1, \ldots, u \), let \( a_i(j) \in k^* \), so that for each \( i \), \( a_i(1), \ldots, a_i(u) \) are all distinct. Let \( f = (f_1, \ldots, f_d) \in (k^*)^d \) be a chosen point so that each \( f_i \) is distinct from the \( a_i(j), j = 1, \ldots, u \). Let \( g_i(t_1, \ldots, t_d) \) be a polynomial chosen in one of the following two ways:

- either \( g_i(t_1, \ldots, t_d) = \prod_{j=1}^u (t_i - a_i(j)) \) or
- and \( g_i(t_1, \ldots, t_d) = \prod_{j=1}^u (t_i - a_i(j)) \prod_{j \neq i} (t_j - f_j) \)

Let \( P \) denote any one of the \( u^d \) points in \( (k^*)^d \) formed by taking as the \( i \)-th entry any of the \( u \)-points, \( a_i(1), \ldots, a_i(u) \). Then the Jacobian \( J(g_1, \ldots, g_d, h) \) \( P \neq 0 \), where \( P \) denotes any of the above points. Therefore, the local residue of the form \( \omega_0 = hdt_{1} \wedge \cdots \wedge dt_{d} \) at each of the above points \( P \) is given by \( \frac{h(P)}{J(g_1, \ldots, g_d)(P)} \). In particular this is non-zero if \( h(P) \neq 0 \) as well.

3.2.1. We may in fact choose \( h = J(g_1, \ldots, g_d) \) so that the local residue at each of the points \( P_i \) of the form \( \omega_0 \) is 1. One may homogenize the differential form \( \omega_0 = \frac{J(g_1, \ldots, g_d) t_1 \wedge \cdots \wedge t_d}{g_1 \cdot \cdots \cdot g_d} \) by substituting everywhere for the variables \( t_j \) in terms of the homogeneous co-ordinates \( x_1, \ldots, x_N \) (where \( N = \mid \Delta(1) \mid \) is the number of 1-dimensional rays in the fan \( \Delta \)) and by observing that the form \( \frac{dt_{1} \wedge \cdots \wedge dt_{d}}{g_1 \cdot \cdots \cdot g_d} \) homogenizes to \( \Omega_{\frac{\Delta \cdot \cdots \cdot \Delta}{\Sigma(1)}} \). (See [7, Theorem 4].) (Observe that the multi-degree in \( (t_1, \ldots, t_d) \) of \( J(g_1, \ldots, g_d) t_1 \cdot \cdots \cdot t_d = deg(g_1, \ldots, g_d) \) is zero.) Thus the above form \( \omega_0 \) defines a global rational differential form, which we denote by \( \omega_0 \). Clearly \( \omega_{can} \) is also a global rational differential form and \( \omega_{can} = g \omega_{can} \) where \( g \) is the rational function obtained by homogenizing \( \frac{J(g_1, \ldots, g_d) t_1 \wedge \cdots \wedge t_d}{g_1 \cdot \cdots \cdot g_d} \). It follows that the divisors associated to the form \( \omega_{can} \) and \( \omega_0 \) are linearly equivalent. The latter restricts to \( \omega_0 \) on the dense torus, and therefore, has local residue 1 at all the \( u^d \) rational points \( P \) considered above. Therefore, for computations that involve divisors up to linear equivalence, we may assume that \( Res_{\mathcal{P}}(\omega_{can}) = 1 \) for any of the \( u^d \) rational points \( P \) chosen above. However, the two forms \( \omega_0 \) and \( \omega_{can} \) are distinct and we will, in general, distinguish between the two.

**Remark 3.3.** Since \( \overline{\omega_0} = g \omega_{can} \), the polytope associated to the line bundle \( \omega_X(D) \cong \mathcal{O}_X(D + K) \) is a translate of the polytope associated to the line bundle \( \omega_X(D + div(g)) \cong \mathcal{O}_X(D + K + div(g)) \). This observation will be used
in working with the polytopes for the examples considered in section 5. The divisor $K + \text{div}(g)$ will be denoted $K'$ henceforth.

For any divisor $F$ on $X$, recall $\Gamma(X, \mathcal{O}_X(F)) = \{f \in K(X) | \text{div}(f) + F \geq 0, \text{ or } f = 0\}$ and that $\Gamma(X, \omega_X(F)) = \{\omega \in \Gamma(X, K(X) \otimes \omega_X) | (\omega + F) \geq 0, \text{ or } \omega = 0\}$.

**Proposition 3.4.** Multiplication by the differential form $\omega_0$ induces an isomorphism $\Gamma(X, \mathcal{O}_X(F + K')) \to \Gamma(X, \omega_X(F))$. Moreover, if $F = D - E$, (where $D = \text{div}(g)_\infty$) for some effective divisor $E$ and $f \in \Gamma(X, \mathcal{O}_X(F + K'))$, $\text{Res}_{P_i}(f, \omega_0) = f(P_i)$, $i = 1, \cdots, m$.

Proof. Let $f \in \Gamma(X, \mathcal{O}_X(F + K'))$. Then $\text{div}(f) + K' + F \geq 0$. But $K'$ is the Cartier divisor associated to $\omega_0$, so that $(\text{div}(\omega_0) + F = \text{div}(f) + (\omega_0) + F \geq 0$. It follows that multiplication by $\omega_0$ sends $f \in \Gamma(X, \mathcal{O}_X(F + K'))$ to $f \omega_0 \in \Gamma(X, \omega_X(F))$. Since one may multiply by $1/f$, the bijectivity of the above map is clear. This proves the first assertion. Let $f \in \Gamma(X, \mathcal{O}_X(F + K'))$ with $E$ as above. Then $\text{div}(f)_0 - \text{div}(f)_\infty + D - E + K + \text{div}(g)_0 - \text{div}(g)_\infty = \text{div}(f)_0 - E + K + \text{div}(g)_0 - \text{div}(f)_\infty$ since $D = \text{div}(g)_\infty$. Therefore, the hypothesis that $\text{div}(f) + D - E + K' \geq 0$ implies that $\text{div}(f)_\infty$ is contained in $\text{div}(g)_0$ which is disjoint with the points $\{P_i | i = 1, \cdots, m\}$. Therefore, $\text{Res}_{P_i}(\omega_0) = f(P_i). \text{Res}_{P_i}(\omega_0) = f(P)$ since $\text{Res}_{P_i}(\omega_0) = 1$ for all the chosen points $P_i$. This proves the second assertion. 

It follows from the proposition above that the residue $\text{Res}_{P_i}(f, \omega_0) = 0$ if and only if $f(P) = 0$ where $P$ is one of the chosen rational points. Therefore, we obtain the following variant of Hansen’s theorem discussed above.

**Theorem 3.5.** Suppose $X$ is a projective smooth toric variety over the finite field $k$ and $d = \dim X \geq 2$, $C_1, C_2, \cdots, C_n$ are irreducible curves on $X$ with k-rational points $P_1, P_2, \cdots, P_n$ distributed over the curves $C_i$, and which are assumed to be among the $u^d$ $k$-rational points considered above in Proposition 3.2. Assume there are $\leq b$ points on each $C_i$, these points are all contained in the dense orbit, and have all co-coordinates different from zero. For each $i = 1, \cdots, d$, let $D_i$ denote the divisor chosen as the closure of $Z(g_i(x_1, \cdots, x_d)) = \{(x_1, \cdots, x_d) \in G_m^d \mid g_i(x_1, \cdots, x_d) = 0\}$. Then $\Gamma^0_{\mathcal{O}}[D_i]$ clearly contains the rational points $\mathcal{P} = \{P_1, \cdots, P_n\}$.

Assume the following hypotheses as well: (i) Let $F$ be a divisor on $X$ and let $F' = F + K'$, where $K' = K + \text{div}(g)$ is the divisor considered above in the last Proposition. (ii) Let $Z(s) = \{P \in X | \text{Res}_{P}(s) = 0\}$ where $s \in \Gamma(X, \omega_X(F))$, and let

$$l = \sup_{s \in \Gamma(X, \omega_X(F))} \# \{i : C_i \subseteq Z(s)\}$$

(iii) Assume $F' \cdot C_i \geq 0$ for all $i = 1, \cdots, m$.

Then the code $C(X, \omega_X, F, \mathcal{P})$ has length $m$ and minimum distance

$$d \geq m - lb - \sum_{i=1}^{m} F' \cdot C_i$$

If $F' \cdot C_i = \delta \leq N$ for all $i$, then

$$d \geq m - lb - (n - l)\delta$$

In particular, if $X$ is a non-singular surface, $H$ is a nef divisor on $X$ with $H \cdot C_i > 0$, then

$$l \leq \frac{F' \cdot H}{\min \{C_i \cdot H\}}$$

Thus if $F' \cdot H < C_i \cdot H$ for all $i$, then $l = 0$ and $d \geq m - \sum_{i=1}^{m} F' \cdot C_i$.

Proof. The proof of this is very similar to the proof of Hansen’s Theorem 2.3. We will briefly provide some details mainly for the sake of completeness. Let $s \in \Gamma(X, \omega_X(F))$ and let $Z(s) = \{P \in X | \text{Res}_{P}(s) = 0\}$. Let $s = f\omega_0$, with $s \in \Gamma(X, \omega_X)$ and $f \in \Gamma(X, \mathcal{O}_X(F + K'))$. Then a chosen rational point $P$ either is contained in one of the curves $C_i \subseteq Z(s)$ or by the above Proposition $\text{Res}_{P}(s) = 0$ if and only if $f(P) = 0$. Therefore, the number of points among the chosen points $\{P_i | i\}$ where $\text{Res}(s)$ is zero is at most $lb + \sum_{i=1}^{m} F' \cdot C_i$. Since $F' \cdot C_i \geq 0$ (by assumption), it follows that $d \geq m - lb - \sum_{i=1}^{m} F' \cdot C_i$. These prove all but the last statement, which follows as in the proof of Hansen’s Theorem (see [16]). Alternatively, one may make use of the last Proposition to reduce this theorem to Hansen’s theorem quoted above. 

\[\square\]
3.3. Basic Hypotheses on the choice of rational points. One obvious choice of the set of \( k \)-rational points are all the \( k \)-rational points belonging to the open dense orbit: assuming the tori are all split, this corresponds to picking these points to be all the \( k \)-rational points in \( \mathbb{G}_m^d \) if \( dim_k(X) = d \). This is the common choice made in the construction of classical codes from toric varieties - see [17]. For the purposes of our constructions below, and especially for the applications to residue codes, it seems nevertheless preferable to consider a slightly smaller subset of \( k \)-rational points chosen as follows. Let \( k[\mathbb{G}_m^d] = k[t_1, t_1^{-1}, t_2, t_2^{-1}, \ldots, t_d, t_d^{-1}] \). The variable \( t_i \) will also denote the \( i \)-th co-ordinate of a point in \( \mathbb{G}_m^d \). For each rational point \( a \in k^* \) and \( i = 1, \ldots, d \), we let \( D_{i,a} \) denote the divisor which is the closure of \( div(t_i - a) \) in the given toric variety \( X \). We will often denote this by \( Z(t_i - a) \) as well. For a subset \( J_i \) of the \( k \)-rational points forming the \( i \)-th factor of \( \mathbb{G}_m^d \), we let \( D_{J_i} = \sum_{a \in J_i} D_{i,a} \). For each divisor \( F \), we let \( |F| \) denote its support.

We choose the divisors as follows. We let \( J_i = k^* \), for \( i = 1, \ldots, d \). For each \( i = 1, \ldots, d \), we let \( f_i \in k^* \) denote a single chosen rational point. Then we let \( J'_i \subseteq J_i - \{ f_i \} \) be such that \( |J'_i| \geq |k^*|/2 \). In the case \( D_{i,a} \) is ample for each \( i \) and any \( a \in k^* \), we let

\[
D_i = \sum_{a \in k^* \mid a \neq f_i} D_{i,a} + \sum_{j=2}^d D_{j,f_j}, \quad D = \sum_{a \in k^* \mid a \neq f_i} D_{i,a}, \quad i = 2, \ldots, d. \tag{3.3.1}
\]

(See the first example in section 5 where this situation occurs.) Otherwise we let

\[
D_i = D_{J'_i} + \sum_{j \neq i} D_{j,f_j}, \quad i = 1, \ldots, d. \tag{3.3.2}
\]

We let \( |J'_i| = n_i \) and also let \( D'_i = D_{J'_i} \). In this case, observe that the intersection \( \bigcap_{i=1}^d |D'_i| \) has at least \( (c/2)^d \) \( k \)-rational points in the dense orbit \((c = |k^*|) \) whereas the intersection \( \bigcap_{i=1}^d |D_i| \) has more points. This intersection always contains the point \( f = (f_1, \ldots, f_d) \) when \( D_i \) is defined by (3.3.2).

The basic hypotheses we put in both the above cases are the following:

\[
D_{i,a} \cdot V(\rho) \geq 0, \quad i = 1, \ldots, d,
\]

\[
(\sum_{i=1}^d D_{i,a}) \cdot V(\rho) > 0 \quad \text{and}
\]

\[
\bigcap_{i=1}^d |D_i| \text{ is finite}
\]

where \( V(\rho) \) denotes any of the \( d - 1 \)-dimensional cones in the given fan and \( a \in k^* \) is any rational point.

Remark 3.6. These hypotheses need to be verified on a case by case basis: we show these are satisfied in all the two dimensional examples we consider in section 5. The importance of the first two conditions is so that the next Proposition is true, which together with the last condition enables one to apply Theorem 4.3 as well as Theorem 4.1. The last hypothesis is automatically satisfied by toric surfaces: now the prime divisors appearing in each \( D_i \) are lines and they intersect with the dense orbit in an open non-empty sub-variety. (Therefore, the points on each of these divisors lying outside the dense orbit is a finite collection of points.)

Proposition 3.7. Under the hypothesis (3.3.3), each of the divisors \( D_i \) defined above is ample.

Proof. In case each \( D_{i,a} \) is ample, it is clear that so is \( D_i = \sum_{a \in k^* \mid a \neq f_i} D_{i,a} \). Next we consider the second case where \( D_i = D_{J'_i} + \sum_{j \neq i} D_{j,f_j} \). Here we make use of the observation that the divisors \( D_{i,a} \) and \( D_{i,b} \) are linearly equivalent for any two \( k \)-rational points \( a, b \in k^* \). This assertion follows from the next Lemma. Therefore, \( D_i \cdot V(\rho) = D_{J'_i} \cdot V(\rho) + \sum_{j \neq i} D_{j,f_j} \cdot V(\rho) = |J'_i| D_{i,a} \cdot V(\rho) + \sum_{j \neq i} D_{j,f_j} \cdot V(\rho) = (\sum D_{i,a})V(\rho) + |J'_i| - 1)D_{i,a} \cdot V(\rho) \) where \( a \in k^* \) is any point. Since \( (\sum D_{i,a}) \cdot V(\rho) > 0 \) by our hypothesis (3.3.3), it follows that \( D_i \cdot V(\rho) > 0 \) as well. Therefore, the conclusion follows readily from the toric Nakai criterion: see Theorem 5.1.

Lemma 3.8. The divisor \( D_{i,a_i} \) is linearly equivalent to \( Z(x_i) \), for any \( k \)-rational point \( a_i \).

Proof. First observe that the divisor \( D_{i,a_i} \) is the closure of \( Z(t_i - a_i) \) in \( X \), where \( t_i \) denotes the \( i \)-th co-ordinate on the torus \( T = \mathbb{G}_m^d \). On homogenizing, this divisor becomes \( Z(x_i - a_i \phi_i) \) where \( \phi_i \) are chosen as in 3.4(4) below. Multiplying by the rational function \( \frac{1}{(x_i - a_i \phi_i)} \), we see that this divisor is linearly equivalent to the divisor \( Z(x_i) \).

Remark 3.9. The divisors \( D'_i \) need not be ample in general. This is the main reason for introducing the divisors \( D_i \): see the second and third examples considered in section 5 where this occurs.

8 ROY JOSHUA AND REZA AKHTAR
We let $D'$ denote the divisor $\Sigma_{i=1}^n D'_i$ and $D$ denote the divisor $\Sigma_{i=1}^n D_i$. We let
\[(3.3.4)\quad \mathcal{P} = \{P_i | i = 1, \ldots, m\}\]
denote the set of points in the intersection of $\bigcap_{i=1}^d |D_i|$ and the dense orbit.

We will denote the remaining points in $\bigcap_{i=1}^d |D_i|$ by $\{P_{m+1}, \ldots, P_M\}$.

### 3.4. Basic Hypotheses on the toric variety and the line bundle
We will make the following hypotheses throughout the remainder of the paper. The first two are merely observations or notational conventions, the conditions (2), (3) and (7) are basic hypotheses on the toric variety and the shape of the corresponding polytope, while (4) is a condition on the Euler form and (5), (6) are conditions on the line bundle.

1. The cardinality of $k^*$ is denoted $c$. (Observe that, if $k = F_p$ for some prime $p$ and $s \geq 1$, then $c = p^s - 1$.)
2. $X$ is a smooth projective toric variety defined over $k$ by the complete fan $\Sigma \subseteq \mathbb{N}$ or equivalently by the (rational) polytope $P \subseteq \mathbb{M}_\mathbb{Q}$. Let $\Sigma(1) = \{\rho_i | i = 1, \ldots, N\}$ denote the 1-dimensional cones in the fan, and let $\{x_i | i = 1, \ldots, N\}$ denote the corresponding variables in the associated homogeneous co-ordinate ring of $X$. We will often denote the divisor $Z(x_1^i)$ by $B_i$.
3. We will assume that $d = \dim_k X = \dim_k (\mathbb{M}/\mathbb{Z}_\mathbb{M})$. We will also assume that $d$ faces of the polytope $P$ lie on the co-ordinate planes in $\mathbb{R}^d \cong \mathbb{M}_\mathbb{R}$: we may assume without loss of generality these faces correspond to the variables $x_i, i = 1, \ldots, d$.
4. Let $(t_1, \ldots, t_d)$ denote co-ordinates on the dense torus $T = \mathbb{G}_m^d$. On homogenizing the differential form \[\frac{dt_1 \cdots dt_d}{p_{1,1}^{(t_1-\alpha_1)(\psi_1)} \cdots p_{d,1}^{(t_d-\alpha_d)(\psi_d)}}\]
we obtain a differential form of the form \[\frac{\Omega}{(x_{d+1}+1)(t_1-\alpha_1)(\psi_1) \cdots (x_d-\alpha_d)(\psi_d)}\]
where each $\phi_i$ is a product of non-negative powers of the variables $x_{d+1}, \ldots, x_N$ and each $t_i \in \mathbb{Z}$. We also require that the weight of $x_i$ is the weight of $\phi_i$. (In particular, this means, on the dense orbit, the co-ordinates $(t_1, \ldots, t_d)$ are given by $t_i = x_i/\phi_i, i = 1, \ldots, d$).
5. We will also assume that the given line bundle $\mathcal{L} = \mathcal{O}_X(E)$, where $E$ is the divisor $x_{d+1}(Z(x_{d+1} - h_{d+1}\psi_{d+1}) + \cdots + E_N(Z(x_N - h_N\psi_N))$ with the variables (i.e faces) $x_{d+1}, \ldots, x_N$ distinct from the variables $x_i, i = 1, \ldots, d$, and where $\psi_j$ is a polynomial in the variables different from $x_j$ with weight of $\psi_j$ the weight of $x_j$. Moreover, $h_i, h_j$ are chosen so that the intersection $|E| \cap (\cap_{i=1}^d |D_i|)$ is empty. We also require $e_i > 0$ for all $i$ and that $\Sigma_{i=d+1}^N e_i \geq d$.
6. In addition, we require that there exist a section $s_0 \in \Gamma(X, \mathcal{L})$ of the following form:
   - in the case where the divisors $D_i$ are chosen as in (3.3.1), we require this to be given by
     \[\frac{(x_{d+1} - \alpha_1)(\psi_1)}{(x_{d+1} - f_1 + \alpha_1)(\psi_1)} \cdots (x_d - \alpha_d)(\psi_d)}\]
   - in the case where the divisors $D_i$ are chosen as in (3.3.2), we require this to be given by
     \[\frac{(x_1 - \alpha_1)(\psi_1) \cdots (x_d - \alpha_d)(\psi_d)}{(x_{d+1} - h_{d+1}\psi_{d+1}) \cdots (x_N - h_N\psi_N)}\]
   where the $f_i$ are chosen as in 3.3 and the $\{g_i | i\}$ are non-negative integers. (Observe that $s_0(P_i) \neq 0$ for any of the chosen points above. This follows from the observation that the points $P_i$ have all co-ordinates different from $f_i, i = 1, \ldots, d$).
7. A generic point on the 1-dimensional rays $\rho_i$, for $i = d+1, \ldots, N$ belongs to the region of $\mathbb{N}_\mathbb{R} \cong \mathbb{R}^d$ with all the co-ordinates $x_1, \ldots, x_d$, non-positive.

One may see from the examples worked out in section 5 that these hypotheses are in fact satisfied in many cases. Observe also that since $\{P_i | i = 1, \ldots, M\} \subseteq (\cap_{i=1}^d |D_i|)$, $|E| \cap \{P_i | i = 1, \ldots, M\}$ is empty, i.e. the global sections of the line bundle $\mathcal{L} = \mathcal{O}_X(E)$, viewed as rational functions on $X$, do not have poles at any $P_i, i = 1, \ldots, M$.

### 3.5. Generic examples of toric varieties satisfying some of the above hypotheses
We discuss a class of examples of toric varieties for which some of the above hypotheses are easy to verify. We discuss a few of these at length in the last section, where we verify all of these hypotheses.

**Proposition 3.10.** Given $d$ functions $g_1, \ldots, g_d$ as in Proposition 3.2 so that their common zeroes is a finite set of points in $\mathbb{G}_m^d$, there exists a projective toric variety $X$ such that the divisor $D_i = \text{the closure of } Z(g_i)$ in $X$, ...
i = 1, · · · , d, and the divisors $D_i$, $i = 1, · · · , d$, have as intersection the same finite set of points $\{P\} = \cap_{i=1}^d Z(g_i)$. In particular, one may choose $X$ to be one of the following:(i) $(\mathbb{P}^1)^d$, (ii) $\mathbb{P}^d$ or (iii) $\mathbb{P}^d(w)$ which is a weighted projective space with suitable choice of weights.

Proof. There are two obvious possible constructions of a toric compactification. The first is $(\mathbb{P}^1)^d$. The second is $\mathbb{P}^d$. Moreover, if the variables $x_i$ are weighted by weights $w_i$ (not necessarily 1), then the corresponding toric compactification would be the corresponding weighted projective space. The statement that the intersection of the divisors $D_i$ coincides with the same set of points $\{P\}$ follows readily from the arguments in [8, (1.3) - (1.3')] it suffices to observe that the leading terms of the polynomials $g_i$ satisfy the hypothesis in [8, (1.3)].

The following proposition shows that starting with projective smooth toric varieties satisfying the above basic hypotheses, one may produce more examples of such varieties by blowing up along smooth toric sub-varieties contained in the complement of the dense open orbit.

Proposition 3.11. Let $\pi : \tilde{X} \rightarrow X$ denote a blow-up of a projective smooth $d$-dimensional toric variety over $k$ along some closed $T$-stable sub-variety. Let $D_i (\tilde{D}_i), i = 1, · · · , d$, denote the divisor defined as the closure of the divisor $Z(g_i)$ in the dense torus $T$ in $X \backslash \{\pi: \}$. If the intersection $\cap_{i=1}^d |D_i|$ is contained in the dense torus $T$, so is the intersection $\cap_{i=1}^d |\tilde{D}_i|$.

Proof. This is clear in view of the observation that since the center of the blow-up is outside the dense orbit, the inverse image of the dense torus in $X$ by $\pi$ is the dense torus in $\tilde{X}$.

4. Duality results and estimation of parameters

4.1. Duality results. The following theorem is well-known (see [14], [6]) over the complex numbers even when the divisors are not ample. For the purposes of this paper, it suffices to prove this theorem only when the divisors $D_i$ are ample. We will provide of this theorem that is valid over any field in this case and making use of the ideas in the proof of Theorem 4.3. Therefore, we sketch a proof only after the proof of 4.3.

Theorem 4.1. Let $X$ denote a smooth projective toric variety defined over a field $k$. Let $d = \dim_k X$. Let $D_1, · · · , D_d$ denote an effective ample Cartier divisors defined by homogeneous polynomials in the homogeneous coordinate ring of the toric variety, and whose intersection is a finite set of points. Let $\omega$ denote a differential form in $\Gamma(X, \omega X (D_1 + ... + D_n))$, i.e. $\omega$ has poles contained in $\Sigma_{i=1}^d D_i$. Then

$$\sum_{\pi \in D_1 \cap ... D_n} Res_{\omega}(\omega) = 0$$

where $Res_{\omega}(\omega)$ denotes the local residue of the differential form $\omega$ at $x$.

Next we consider some key results on residues which form a converse to the above theorem. Since the case when $X = \mathbb{P}^d$ is rather simple and straightforward, we will consider this next. We will assume that $x_1, · · · , x_d, x_{d+1}$ are the homogeneous co-ordinates on $\mathbb{P}^d$.

For each $i = 1, · · · , d$ let $d_i$ denote a positive integer $\leq c$ and let $B_i = \sum_{j=1}^{d_i} Z(x_i - a_i(j)x_{d+1})$. Let $R_i[\pi]$ denote all the $k$-rational points that lie in intersection of the supports of all $B_i$, $i = 1, · · · , d$.

Lemma 4.2. (See [28, pp. 36-37].) Let $R_1 = (R_1, · · · , R_1, d), R_2 = (R_2, · · · , R_2, d)$ denote two arbitrarily chosen distinct points from the set $\{R_i[\pi]\}$ above. Then there exists a differential form $\eta_{i, 2} \in \Gamma(X, \omega (\Sigma_i B_i))$ so that $Res_{R_1}(\eta_{i, 2}) = 1$ and $Res_{R_2}(\eta_{i, 2}) = 0$ for all $R_i$ different from $R_1$ and $R_2$.

Proof. We let $\eta_{i, 2} = \frac{1}{(x_1/x_{d+1} - R_{1, 1})^{d_1}(x_2/x_{d+1} - R_{1, 2})^{d_2}... (x_{d}/x_{d+1} - R_{1, d})^{d_d}} - \frac{1}{(x_1/x_{d+1} - R_{2, 1})^{d_1}(x_2/x_{d+1} - R_{2, 2})^{d_2}... (x_{d}/x_{d+1} - R_{2, d})^{d_d}}$. First the term $d(x_1/x_{d+1}) \wedge \cdots \wedge d(x_d/x_{d+1})$ is simplified using the quotient rule to $\frac{\partial}{\partial x_{d+1}}$. Next the term

$$\frac{1}{(x_1/x_{d+1} - R_{1, 1})^{d_1}(x_2/x_{d+1} - R_{1, 2})^{d_2}... (x_{d}/x_{d+1} - R_{1, d})^{d_d}}$$

simplifies to

$$\frac{1}{(x_1/x_{d+1} - R_{1, 1})^{d_1}(x_2/x_{d+1} - R_{1, 2})^{d_2}... (x_{d}/x_{d+1} - R_{1, d})^{d_d}}$$

and similarly for the other terms. Hence $\eta_{i, 2}$ is a key point here is the following: the terms in the numerator that do not contain $x_{d+1}$ as a factor will cancel out when the difference

$$\frac{1}{(x_1/x_{d+1} - R_{1, 1})^{d_1}(x_2/x_{d+1} - R_{1, 2})^{d_2}... (x_{d}/x_{d+1} - R_{1, d})^{d_d}} - \frac{1}{(x_1/x_{d+1} - R_{2, 1})^{d_1}(x_2/x_{d+1} - R_{2, 2})^{d_2}... (x_{d}/x_{d+1} - R_{2, d})^{d_d}}$$

is simplified and written with the common denominator which is the product of the two denominators. Therefore, all the remaining terms in the numerator will have $x_{d+1}$ as a factor, and this will cancel with the $x_{d+1}$ in the
denominator of $\frac{\Omega}{x_{i1}^{d+1}}$. Therefore, $\eta_{1,2}$ identifies with the form:

$$
\Omega_g = \frac{(x_1 - R_{1,1}x_{d+1})(x_1 - R_{2,1}x_{d+1}) \cdots (x_d - R_{1,d}x_{d+1})(x_d - R_{2,d}x_{d+1})}{(x_1 - R_{1,1}x_{d+1})(x_1 - R_{2,1}x_{d+1}) \cdots (x_d - R_{1,d}x_{d+1})(x_d - R_{2,d}x_{d+1})}
$$

where $g$ is some homogeneous polynomial in the variables $x_1, \cdots, x_d, x_{d+1}$. In particular, the poles of this differential form are contained in the union of the supports of the divisors $B_i$. One may compute the residues at the points $R_i$, $i = 1, 2$ and observe these are 1 and $-1$, respectively. The residues at the other points $R_i$, $i \neq 1, 2$ are clearly zero since the above differential form has no poles at these points. 

**Theorem 4.3.** Assume that $X$ is a projective smooth toric variety of dimension $d$ defined over $k$ by a polytope $P$ satisfying the basic hypotheses as in 3.4. $D_i$, $i = 1, \cdots, d$ is a set of effective ample divisors on $X$ and $\cap_{i=1}^{d} |D_i| = \{ R_i | i = 1, \cdots, M \}$ where each $R_i$ is a $k$-rational point of $X$. Assume that each divisor $D_i$ is defined by a homogeneous polynomial in the homogeneous co-ordinate ring of the toric variety, and that for each point $R_i$, one is given $v_i(R_i) \in k^+$ so that the sum $\sum_i v_i(R_i) = 0$. Then there exists a differential form $\eta \in \Gamma(X, \omega_X(\Sigma D_i))$ so that $\text{Res}_{R_i}(\eta) = v_i(R_i)$.

**Proof.** A corresponding result is proven for the special case when $X = \mathbb{P}^d$ in [28, pp. 36-37], where the divisor $D_i = B_i$ as in the last lemma. Since this proof is straightforward we will discuss this next, the key starting point being the above lemma. Let the total number of the given rational points $\{ R_i | i \}$ be $M$. For each pair of points $R_1, R_2$ among the given rational points, let $\eta_{1,2}$ denote the differential form constructed in the last lemma. We show there exists a rational linear combination of these differential forms, $\eta = \sum_{i,j} \eta_{i,j}$ identifying with the required properties. Here the $x_{i1}, x_{i2}$ are the variables and there are altogether $N = M - 1$ such variables. Taking the residues of the form $\eta$ at the given points $R_i$, one provides us with the following system of $M$-linear equations in the above variables:

$$
\Sigma_{i,j} \text{Res}_{R_i}(\eta_{i,j}) x_{i1} x_{i2} = v_i(R_i)
$$

$$
\cdots
$$

$$
\Sigma_{i,j} \text{Res}_{R_m}(\eta_{i,j}) x_{i1} x_{i2} = v_M(R_M)
$$

Since each fixed point $R_i$ appears along with every other point $R_j$ as a pair $(R_i, R_j)$, and $\text{Res}_{R_i}(\eta_{i,j}) = 1$, $\text{Res}_{R_j}(\eta_{i,j}) = -1$, one may readily observe the following: (i) the rank of the corresponding coefficient matrix is $M - 1$, and (ii) the sum of the rows of the augmented matrix (i.e. the matrix whose first columns are the coefficients of the variables and whose last column is the right-hand-sides of the equation) is 0. It follows that the ranks of the augmented and coefficient matrices are both $M - 1$ so that (4.1.2) has a solution in $k^N$. This concludes the proof for the case $X = \mathbb{P}^d$ where the divisor $D_i = B_i$.

Next we consider the general case. The proof we give now largely follows the proof of the corresponding assertion in characteristic 0 for general projective smooth varieties worked out in [14, (3.8) Theorem]. We will show that the same proof carries over to projective toric varieties. A key observation here is that Kodaira vanishing holds for these varieties in view of the observation that they are Frobenius split: see [2, Chapter 1]. (Though they state their results over algebraically closed fields, one may see that the same arguments as in the proof of [2, 1.2.9 Theorem] carry over readily to smooth toric varieties over finite fields. We have outlined some of the key results on Frobenius splitting over finite fields, in the appendix.)

One begins with the observation that, by Serre duality, one obtains the isomorphism:

$$
H^d(X, \omega_X) \cong k, \quad H^i(X^*, \omega_X) = 0, i \geq d
$$

where $X^* = X - (\cap_{i} |D_i|) = \cup_i (X - |D_i|)$. Therefore, one obtains the exact sequence:

$$
H^{d-1}(X^*, \omega_X) \to H^d(\cap_{i} |D_i|, \omega_X) \to H^d(X, \omega_X) \cong k \to 0
$$

The term $H^d_{\cap_{i} |D_i|}(X, \omega_X)$ identifies by excision with $\oplus_R H^d_R(X, \omega_X)$. Moreover, the map $H^d_R(X, \omega_X) \to k$ identifies with taking the residue at the point $R_i$. The exactness of the sequence in (4.1.4) now shows that if $v_i \in k$, $i = 1, \cdots, M$ are such that $\Sigma_i v_i = 0$, then there exists a class $\phi \in H^{d-1}(X^*, \omega_X)$ so that if $\phi_i$ denotes the image of $\phi$ in $H^d_R(X, \omega_X)$, then the local residue of $\phi_i$ at $R_i$ equals $v_i$, $i = 1, \cdots, m$. Therefore, in order to complete the proof of the theorem it suffices to show that there exists a global differential $d$-form $\Omega \in H^0(X, \omega_X(\Sigma_{i=1}^M D_i))$ that maps to the class $\phi$ by the map in (4.1.7).
Next we make use of the hypothesis that each of the divisors $D_i$ is ample. Making use of the observation that projective smooth toric varieties are Frobenius split (see [2, Chapter 6]), this implies that
\begin{equation}
H^i(X, \omega_X(D_1 + \cdots + D_d)) = 0, \quad i > 0
\end{equation}
for any subset $\{i_1, \ldots, i_p\}$ of $p$-elements in $1 \cdots d$. Next we make a complex out of $\{\omega_X(D_1 + \cdots + D_d)\}_{1 \leq i_1, \ldots, i_p \leq d}$ as follows. The term in degree $q$, for $1 \leq q \leq d$, is given by $\oplus_{i_1, \ldots, i_p, \epsilon(S) = q} \omega_X(D_1 + \cdots + D_d)$ where the sum varies over subsets $S$ of $\{1, \ldots, i_q \leq d\}$ with cardinality $q$. The differential $\delta : \oplus_{i_1, \ldots, i_p, \epsilon(S) = q} \Gamma(U, \omega_X(D_1 + \cdots + D_d)) \to \oplus_{i_1, \ldots, i_p, \epsilon(S) = q - 1} \Gamma(U, \omega_X(D_1 + \cdots + D_d))$ is given by $\delta(\alpha_{i_1, \ldots, i_p}) = \sum_{k=1}^{q+1} (-1)^k \alpha_{i_1, \ldots, \hat{i}_{q+1}}$ with the form $\alpha_{i_1, \ldots, \hat{i}_{q+1}}$ viewed as a form with poles contained in $D_1 + \cdots + D_{i_q+1} + D_{i_{q+1}}$. Since the above argument already appears in [14, (3.8) Theorem], at least in the case of complex varieties, we skip the proof that this defines a complex. This complex will be denoted $\omega_X(D_*)$.

We proceed to show that the above complex is acyclic on $X^*$ by constructing a chain null-homotopy of the above complex. It will follow that the complex $\omega_X(D_*)$ provides a resolution of the sheaf $\omega_{X^*}$, where $j : X^* \to X$ denotes the obvious open immersion. Let $x$ denote a fixed point of $X^*$, and let $t$ denote an index $1 \leq t \leq d$ so that $x \in X - \{D_t\}$. Let $\alpha \in \oplus_{i_1, \ldots, i_p, \epsilon(S) = q} \Gamma(U, \omega_X(D_1 + \cdots + D_t))$, where $U \subset X - \{D_t\}$ is an open neighborhood of $x$. Let $\theta(\alpha) \in \oplus_{i_1, \ldots, i_p, \epsilon(S) = q-1} \Gamma(U, \omega_X(D_1 + \cdots + D_{i_q}))$ be defined by
\begin{equation}
\theta(\alpha)_{i_1, \ldots, i_q} = \alpha_{i_1, \ldots, i_q - 1}
\end{equation}
Observe that the form $\alpha_{i_1, \ldots, i_q - 1} \in \Gamma(U, \omega_X(D_1 + D_{i_1} + \cdots + D_{i_q-1})) \cong \Gamma(U, \omega_X(D_1 + \cdots + D_{i_q}))$ since $U \subset X - \{D_t\}$. Therefore, $\theta : \oplus_{i_1, \ldots, i_p, \epsilon(S) = q} \Gamma(U, \omega_X(D_1 + \cdots + D_t)) \to \oplus_{i_1, \ldots, i_p, \epsilon(S) = q-1} \Gamma(U, \omega_X(D_1 + \cdots + D_{i_q}))$. Now it suffices to show that $d \circ \theta + \theta \circ d = id$: this is readily checked using the definition of $\theta$. (Observe that this argument is very similar to the argument for the exactness of the Čech resolution of a sheaf constructed using an open cover.)

It follows from the above arguments that the $i$-th cohomology of the complex $\Gamma(X, \omega_X(D_*))$ computes the cohomology $H^i(X^*, \omega_X)$. Since the complex $\omega_X(D_*)$ terminates with $\omega(\Sigma_{t=1}^d D_t)$, it follows that one has a surjection
\begin{equation}
H^0(X, \omega_X(\Sigma_{i=1}^d D_i)) \to H^{d-1}(X^*, \omega_X) \to 0
\end{equation}
This completes the proof of the theorem.

**Proof of Theorem 4.1.** Let $\omega$ denote a differential form in $\Gamma(X, \omega_X(D_1 + \cdots + D_d))$, i.e. $\omega$ has poles contained in $\Sigma_{t=1}^d D_t$. As above $\omega$ defines a class in $H^{d-1}(X^*, \omega_X)$ which maps to $\oplus_P H^0_P(X, \omega_X)$. The latter map is sending $\omega$ to $(\text{Res}_{P}(\omega)[i])$. The proof of the last theorem (see the exact sequence in (4.1.4)), now also shows that the sum $\Sigma \text{Res}_{P}(\omega)$ is zero. This completes the proof of Theorem 4.1. \qed

Throughout the remainder of this section, we will assume that the basic hypotheses 3.3 and 3.4 hold.

4.2. The example of projective spaces.

**Proposition 4.4.** Assume in addition to the above hypotheses that $N = d + 1$ (where $N$ is the number of variables in the homogeneous co-ordinate ring of $X$: see 3.4(2)), the divisor $E = c_{d+1} \text{div}(x_{d+1})$, and that the weight of each $x_i$, $i = 1, \ldots, d$ is 1. Assume further that the divisors $D_{i,a}$ are all ample and that $D_{1,a} = \Sigma_{a \in k^+ \setminus a \neq f_1 D_{1,a} + \Sigma_{j=2} D_{j,f_j}, D_{1} = \Sigma_{a \in k^+ \setminus a \neq f_1 D_{1,a}, i = 2, \ldots, d}$. (This situation occurs in the first example considered in section 5.)

Then there exists a section $\sigma \in \Gamma(X, \mathcal{L})$ so that the following conditions are satisfied:
\begin{enumerate}
    \item $\text{div}(\sigma) \subseteq [D_{d,f_d}]$
    \item $\sigma$ is regular at all the points $\{P_i | i = 1, \ldots, m\}$
    \item $\text{div}(\sigma) \cong E$
\end{enumerate}

If $c_{d+1} \geq d$, there exists a section $\sigma \in \Gamma(X, \mathcal{L})$ so that instead of (1) above, $\text{div}(\sigma) \subseteq [D_{d,f_d} + \cdots + D_{d,f_d}]$.

**Proof.** It follows readily that each $\phi_i = x_{d+1}$, where $\phi_i$ is as in 3.4(4). We let $s = \frac{(x - f_{d+1})^{e_{d+1}}}{x_{d+1}}$. In this case it is clear that $s(P_i) \neq 0$ at all the chosen points $P_i$, $i = 1, \ldots, m$, $\text{div}(s) \subseteq [D_{d,f_d}]$ and that $\text{div}(s) \cong E$. Alternatively one may choose $s = (x - f_{d+1})^{e_{d+1}} (x - f_{d+1})^{e_{d+1}}$ with $g_i \geq 1$ chosen in such a way that $g_{d+1} = c_{d+1}$.

**Corollary 4.5.** Under the same hypotheses as in the last Proposition the following hold:

(i) There exists a section $t \in \Gamma(X, \mathcal{L})$ so that the conditions (1) and (2) in the last proposition are satisfied and $\text{div}(t) \cong 2E$. 

(ii) There exists a section $u \in \Gamma(X, \mathcal{L})$ so that the conditions (1) and (2) in the last proposition are satisfied and $\text{div}(u) \cong 2E$.
(ii) There exists an \( \omega \in \Gamma(X, \omega(\Sigma D_i + 2D_d, f_d - 2E)) \) so that \( \text{Res}_{P_i}(\omega) \neq 0 \) for all the chosen (rational) points \( P_i \).

**Proof.** In order to prove (i), we may choose \( t = s^2 \) where \( s \) is the first section chosen in the last proposition. Then the required hypotheses on \( t \) are easy to verify.

Next we consider (ii). One starts with a differential form \( \omega' \in \Gamma(X, \omega(\Sigma D_i)) \) chosen as in the proof of Theorem 4.3 so that \( \text{Res}_{P_i}(\omega') \neq 0 \) for all the points \( P_i, i = 1, \cdots, m \) chosen as in the discussion preceding (3.3.2). Let \( t \) denote a section of \( L \) chosen as in (i). Now we let

\[
\frac{\omega'}{t} = \frac{\omega'}{s^2}
\]

Clearly \( \omega \) belongs to \( \Gamma(X, \omega X(D_1 + \cdots + D_d - 2E)) \) (more precisely to \( \Gamma(X, \omega X(D_1 + \cdots + D_d + 2D_d, f_d - 2E)) \). Since the support of \( E \) is disjoint from the support of \( \{ P_i[i] \} \), \( t \) is regular at all points of \( \{ P_i[i] \} \). \( \text{Res}_{P_i}(\omega') \neq 0 \) at each \( P_i \), i.e. \( \text{Res}_{P_i}(\omega) \neq 0 \) for each point \( P_i \).

\[
4.3. \text{ The modified evaluation and residue codes associated to an effective divisor} E \.
\]

Let \( C \) denote an ample line bundle on \( X \), associated to an effective divisor \( E \). Now \( L = \mathcal{O}(E) \). Let \( s \) denote a section of \( L \). We send any such section \( s \) to \( (s(P_1), s(P_2), \cdots, s(P_m), s(P_{m+1}), \cdots, s(P_M)) \in k^M \). Letting \( \mathcal{P} = \{ P_1, \cdots, P_m \} \), we define the code \( C(X, E, \mathcal{P}) \) to be the image in \( k^M \) by the evaluation map \( s \mapsto (s(P_1), s(P_2), \cdots, s(P_M)) \), of the \( k \)-subspace \( \{ s \in \Gamma(X, \mathcal{L}) | s(P_i) = 0, i = m + 1, \cdots, M \} \) in view of the fact that the last \( M - m \) co-ordinates are zero, one may view the code \( C(X, E, \mathcal{P}) \) as a sub-space of \( k^m \).

Assume that the divisors \( D_i, i = 1, \cdots, d \) are chosen as in (3.3.1). In this case we let \( \bar{D}_i = D_1 + D_2, f_d + \cdots + D_d, f_d \), and \( D_i = D_i, i = 2, \cdots, d \). Therefore, the sum \( \Sigma D_i + \Sigma_i D_i, f_i = \Sigma D_i \) and \( |D_i| = |D_i| \), for each \( i \) so that \( \bigcap_i |D_i| = \bigcap_i |D_i| \). Consider \( C(X, \omega X, E, \mathcal{P}) = \{ \alpha \in \Gamma(X, K(X) \otimes \omega X)(\alpha) + D + \Sigma_i D_i, f_i - E \geq 0 \} \), where \( \omega X \) denotes, as before, the sheaf of top-degree differential forms on \( X \). We call this the the **modified residue code** in this case.

Assume next that the divisors \( D_i, i = 1, \cdots, d \), are chosen as in (3.3.2). Let \( \sigma \) denote a permutation of \( 1, \cdots, n \) so that \( \sigma(i) \neq i \) for all \( i \). Now let \( \bar{D}_i = D_i + D_\sigma(i), f_\sigma(i) \), \( i = 1, \cdots, d \). Therefore, the sum \( \Sigma_i D_i + \Sigma_i D_i, f_i = \Sigma_i D_i \) and \( |D_i| = |D_i| \), for each \( i \) so that \( \bigcap_i |D_i| = \bigcap_i |D_i| \). In this case we let \( C(X, \omega X, E, \mathcal{P}) = \{ \alpha \in \Gamma(X, K(X) \otimes \omega X)(\alpha) + D + \Sigma_i D_i, f_i - E \geq 0 \} \), where \( \omega X \) denotes, as before, the sheaf of top-degree differential forms on \( X \). We call this the the **modified residue code** in this case.

**Definition 4.6.** We define \( \text{Res} : C(X, \omega X, E, \mathcal{P}) \rightarrow k^m \subset k^M \) by sending

\[
\alpha \in \Gamma(X, K(X) \otimes \omega X)(\alpha) \rightarrow (\text{Res}_{P_1}(\alpha), \cdots, \text{Res}_{P_m}(\alpha), 0, \cdots, 0).
\]

**Definition 4.7.** Let \( w \in (k^*)^m \). For a code \( C \subset k^m \), we define

\[
C_w^\perp = \{ x \in k^m | \Sigma_i w_i x_i y_i = 0 \text{ for any } y \in C \}
\]

In case \( w_i = 1 \), for all \( i \), we will denote \( C_w^\perp \) by \( C^\perp \).

**Proposition 4.8.** Assume the above situation. Then Theorem 4.1 above implies that the image of the code \( C(X, \omega X, E, \mathcal{P}) = \{ \alpha \in \Gamma(X, K(X) \otimes \omega X)(\alpha) + D + \Sigma_i D_i, f_i - E \geq 0 \} \) under the residue map Res above is contained in \( C(X, E, \mathcal{P})^\perp \).

**Proof.** We will explicitly consider only the proof in the second case where the divisors are defined as in (3.3.2), and the other case is similar. The key observation is that in both case \( |D_i| = |D_i| \) for all \( i = 1, \cdots, d \). Let \( f \in C(X, E, \mathcal{P}) \). Recall from above that \( f(P_i) = 0 \), for all \( i = m + 1, \cdots, M \). If \( \alpha \in \Gamma(X, \omega X, E, \mathcal{P}) \), then the product \( f \alpha \) has poles contained in \( \bigcup_i |D_i| = \bigcup_i |D_i| \), so that Theorem 4.1 and the observation above show the sum

\[
\Sigma_p \in \bigcap_i |D_i| \text{Res}_{P_i}(f \alpha) = \Sigma_{p \in \bigcap_i |D_i|} |D_i| \text{Res}_{P_i}(f \alpha) = \Sigma_p \in \bigcap_i |D_i| f(p) \text{Res}_{P_i}(\alpha) = 0.
\]

In particular, we may replace \( \text{Res}_{P_i}(\alpha) \) by \( 0 \) for all \( i = m + 1, \cdots, M \). The required conclusion follows.
Remark 4.9. One may now use this result to provide a lower bound estimate for the dimension of $C(X, E, \mathcal{P})^\perp$.

Under the above hypotheses we obtain the following corollary to the last Proposition.

**Corollary 4.10.** (i) Assume the above situation. Given any sequence $\{r_j \in k | j = 1, \ldots, m\}$ with the property that

\[ \Sigma_j f_p(r_j) = 0 \quad \text{for any global section } f \in C(X, E, \mathcal{P}), \]

there exists a differential form $\omega' \in \Gamma(X, \omega_X(D_1 + \cdots + D_d + \Sigma_{i=1}^d D_{i,f_i} - E))$ so that $\text{Res}_P(\omega') = r_i, i = 1, \ldots, m.$

(The divisor $D_{i,f_i}$ is defined in 3.3.) (ii) Therefore, the residue map defined in Definition 4.6 sends $C(X, \omega_X, E, \mathcal{P})$ onto $C(X, E, \mathcal{P})^\perp$.

**Proof.** Consider the sequence $\{r_is_0(P)|i = 1, \ldots, m\}$, where $s_0$ is the chosen section in $\Gamma(X, L)$, chosen as in 3.4(6), i.e. $s_0(P) \neq 0$ for all $i = 1, \ldots, m$. Define $r_j = 0$ for all $j = m+1, \ldots, M$. Next recall $s_0 \in K(X)$ so that $\text{div}(s_0) + E \geq 0$, where $L = O_X(E)$. Since $r_j = 0$ for all $j = m+1, \ldots, M$, clearly the sum $\Sigma_j r_is_0(P) = 0$ (where the sum is taken over all the $k$-rational points in the intersection $\cap_{i=1}^d |D_i|$) so that by Theorem 4.3, there exists a differential form $\omega \in \Gamma(X, \omega_X(\Sigma_{i=1}^d D_i))$, with $\text{Res}_P(\omega) = r_is_0(P), i = 1, \ldots, M$. Now consider the differential form $\omega' = \frac{\omega}{s_0}$; since $s_0$ is regular and does not vanish at each point $P_i, i = 1, \ldots, m$, it follows that $\text{Res}_P(\omega') = \text{Res}_P(\frac{\omega}{s_0}) = r_i, i = 1, \ldots, m.$ The hypotheses on $\omega$ and $s_0$ show that $\omega' \in \Gamma(X, \omega_X(\Sigma_{i=1}^d D_i) + \Sigma_{i=1}^d D_{i,f_i} - E)) = C(X, \omega_X, E, \mathcal{P})$ in case the divisors $D_i$ are defined as in (3.3.1), and that $\omega' \in \Gamma(X, \omega_X(\Sigma_{i=1}^d D_i + \Sigma_{i=1}^d D_{i,f_i} - E)) = C(X, \omega_X, E, \mathcal{P})$ in case the divisors $D_i$ are defined as in (3.3.2). This proves the first statement, and the second is clear.

**Remarks 4.11.** 1. Even if the residue map in Definition 4.6 is not necessarily injective, this is enough to provide an estimate for the width of the code $C = C(X, E, \mathcal{P})^\perp$.

2. Observe that for the evaluation code above, we only consider sections $f \in \Gamma(X, L)$ so that $f(P) = 0$, for all $i = m+1, \ldots, M$. For the residue codes we also send $P_i$ to $0 \in k, i = m+1, \ldots, M$. Therefore, we may restrict just to the first $m$ co ordinates, and assume both the evaluation and residue maps into $k^m$.

**Corollary 4.12.** Under the basic hypotheses as in 3.4 and 3.3 there exists a differential form

\[ \omega_1 \in C(X, \omega_X, 2E, \mathcal{P}) \]

so that $\text{Res}_P(\omega_1) \neq 0$ at all the chosen rational points $\{P_i | i = 1, \ldots, m\}$.

**Proof.** Observe that $C(X, \omega_X, 2E, \mathcal{P}) = \Gamma(X, \omega_X(\Sigma_{i=1}^d D_i + \Sigma_{i=1}^d D_{i,f_i} - 2E))$ in case the divisors are defined as in (3.3.1), and $\Gamma(X, \omega_X(\Sigma_{i=1}^d D_i + \Sigma_{i=1}^d D_{i,f_i} - 2E))$ in case the divisors $D_i$ are defined as in (3.3.2). We will consider explicitly only the second case. Choose a sequence $r_i \in k^*, i = 1, \ldots, m$ so that $\Sigma_{i=1}^m r_is_0(P) = 0$. Then there exists a differential form $\omega'_i \in \Gamma(X, \omega_X(\Sigma_{i=1}^d D_i))$ so that $\text{Res}_P(\omega'_i) = r_is_0(P), i = 1, \ldots, m$. Next let $\omega_1 = \frac{\omega}{s_0}$. Now $\text{Res}_P(\omega_1) = \frac{\text{Res}_P(\omega')}{s_0} = r_i, i = 1, \ldots, m$. Clearly $\omega_1 \in \Gamma(X, \omega_X(\Sigma_{i=1}^d D_i + \Sigma_{i=1}^d D_{i,f_i} - 2E))$.

**Theorem 4.13.** Let $w \in k^m$ be defined by $w_i = \text{Res}_P(\omega_1)$ where $\omega_1$ is the differential form chosen as in Corollary 4.12. Let $C = C(X, E, \mathcal{P})^\perp$ defined as in 4.3.1. Then $C \supseteq C_\omega^\perp$.

If $q = 2^n$ (for some $n > 0$), any element of $\mathbb{F}_q$ is a square, in particular, $w_i = v_i^2$ for some $v_i \in \mathbb{F}_q^*$. Let $v = (v_1, \ldots, v_n)$ and let $g_2$ denote the coordinate-wise multiplication by $v = (v_1, \ldots, v_n)$. Then the code $C' = g_2(C)$ (which is equivalent to $C$) has the property $C' \supseteq C_\omega^\perp$ with respect to the standard inner product on $\mathbb{F}_q^n$.

**Proof.** Since the second assertion is clear, we will only prove the first. If $g_1, g_2 : \Gamma(X, L)$, then

\[ \omega g_1,g_2 \in \Gamma(X, \omega(D_1 + \cdots + D_d + \Sigma_{i=1}^d D_{i,f_i})). \]

Observe that the intersection of the supports of the divisors $\cap_{i=1}^d |D_i| = \cap_{i=1}^d |D_i|$ is still the original set of rational points as in 3.3. Now $D_1 + \cdots + D_d + \Sigma_{i=1}^d D_{i,f_i} = \Sigma_{i=1}^d D_i$. It follows that if $g_1,g_2$ denote sections of $C = C(X, E, \mathcal{P})$, i.e. sections of $\Gamma(X, \mathcal{L})$ that vanish at the points $P_0, \ldots, P_M$:

\[ \Sigma_{i=1}^M \text{Res}_P(\omega) \frac{g_1(P_i)g_2(P_i)}{g_1(P_i)} = \Sigma_{i=1}^M \text{Res}_P(\omega) \frac{g_1(P_i)g_2(P_i)}{g_1(P_i)} = \Sigma_{i=1}^M \text{Res}_P(\omega) g_2(P_i) = 0. \]

Since $g_1(P_i) = g_2(P_i) = 0$ for all $i = m+1, \ldots, M$, we may observe that the last equality implies

\[ \Sigma_{i=1}^M \text{Res}_P(\omega) g_2(P_i) = 0. \]
4.4. Estimation of the parameters. For the rest of the paper we will assume that \( q = 2^n \) for some \( n > 0 \). Next we proceed to estimate the parameters of the codes \( C = C(X,E,\mathcal{P})^\perp \). For the sake of simplicity we will restrict to the case where \( X \) is a toric surface: the higher dimensional case will be dealt with elsewhere. Clearly the length of all these codes is \( m \) the number of chosen rational points. The dimensions of these codes may be estimated as follows: given a line bundle \( \mathcal{L} = \mathcal{O}_X(E) \) (associated to the divisor \( E \) and) generated by global sections, one may readily compute the dimension of its global sections as the number of lattice points in the corresponding polytope \( P \). Let this be denoted \(|P|\). Recall the vector space \( C(X,E,\mathcal{P}) \) is the subspace \( \{ s \in \Gamma(X,\mathcal{L}) | s(P_i) = 0, i = m + 1, \ldots, M \} \). Since the map \( s \mapsto s(P_i) \) is a \( k \)-linear map of \( k \)-vector spaces, one may then estimate the dimension of \( C(X,E,\mathcal{P}) \) as follows:

\[
|P| \geq \dim(C(X,E,\mathcal{P})) \geq |P| - (M - m)
\]

Therefore, the dimension of the dual code \( C = C(X,E,\mathcal{P})^\perp \) may be estimated as

\[
\dim(C) \geq |P| - |P| = m - |P|
\]

Finally one makes use of Theorem 3.5 to compute the distance of the code \( C \). In view of the above results the distance of the code \( C \) is bounded below by the distance of the code \( C(X,\omega_X,E,\mathcal{P}) \). Therefore, it suffices to show that the hypotheses of Theorem 3.5 are in fact satisfied by the code \( C(X,\omega_X,E,\mathcal{P}) \). We proceed to show this presently.

Let \( \mathrm{cl}(\mathcal{Z}(t_i-a_i)) \) denote the closure of \( \mathcal{Z}(t_i-a_i) \) in \( X \). Observe that the curves \( C_i \) as in Theorem 3.5 that contain the rational points are given by \( C_{a_i} = \mathrm{cl}(\mathcal{Z}(t_i-a_i)) \) for \( a_i \in k^* \). Clearly there are \( c \) possible choice of these points and hence such curves. (We are stating the following proposition to be applicable for higher dimensions so that we use \( d \) to denote the dimension of the toric variety. For toric surfaces as considered in this paper, clearly \( d = 2 \).)

**Proposition 4.14.** Assume the 1-dimensional rays \( \rho_i \), for \( i = d + 1, \ldots, N \) (in the fan of \( X \)) belong to the region of \( \mathbb{N}^d \cong \mathbb{R}^d \) with the co-ordinate \( x_1 \) non-positive as in the hypothesis 3.4 (7). Let \( C \) denote any of the curves \( C_{a_i} \) as above. (i) Then the intersection numbers \( C \bullet Z(x_i) \geq 0 \) for all \( i = 1, \ldots, N \) and \( C \bullet Z(x_2) > 0 \). (ii) Consequently the intersection numbers \( C \bullet (D - E + K) > 0 \) provided \( c \) is sufficiently large in comparison with \( e_3, \ldots, e_N \) and is chosen as in 3.4. Therefore, in this case, the hypotheses of Theorem 3.5 are satisfied by the code \( C(X,\omega_X,E,\mathcal{P}) \).

**Proof.** In view of Lemma 3.8, it suffices to consider the intersection numbers \( C \bullet Z(x_i) = Z(x_1) \bullet Z(x_i) \). Now we make use of the computation of the intersection numbers as in the example in [23, p. 80]. In case \( i \geq 2 \), then these are either 0 or 1 depending on if the rays corresponding to the toric divisors \( Z(x_1), Z(x_i) \) form a 2-dimensional cone in the fan of \( X \) or not. Therefore, if \( i \geq 2 \), the above intersection numbers are clearly non-negative. Now it suffices to consider the case where \( i = 1 \). Using the standard conventions used for defining the homogeneous coordinate ring of a projective toric variety (see [4]) we will use the variable \( x_1 \) also to denote the corresponding 1-dimensional ray in the fan. In this case the computation of these intersection numbers proceeds by finding one dimensional cones \( \rho' \) and \( \rho'' \) so that the cones \( x_1 + \rho' \) and \( x_1 + \rho'' \) are both 2-dimensional cones in the fan of \( X \) so that \( n(\rho') + n(\rho'') + a_1 n(x_1) = 0 \). Here, \( n(\eta) \) denotes the primitive element in the lattice \( \mathbb{N} \) along the 1-dimensional cone \( \eta \) and \( a_1 \) is an integer. Observe that at most one of the two cones \( \rho' \) and \( \rho'' \) can be the cone \( x_2 \). Therefore, the other cone must be one of \( x_{d+1}, x_{d+2}, \ldots, x_N \). At this point, the first hypothesis in the proposition implies that the integer \( a_1 \) above must be non-negative. Since the intersection number \( Z(x_1) \bullet Z(x_i) \) identifies with the number \( a_1 \) (see [23, p. 80]), and since \( Z(x_1) \bullet Z(x_2) = 1 \) by the hypotheses in 3.4(3), the first conclusion of the proposition follows.

Next we consider the second statement. For this, observe first that the dimension of \( X \) (i.e. \( d \) in the above theorem) is now 2 and that the number of rational points \( \{ P_i \} \) is \( m \geq (c/2)^2 \).

The divisor \( F + F' \) in Theorem 3.5 is now given by \( D - E = \Sigma i=1 D_i - E (D - E + K', \) respectively). Since \( K \) is linearly equivalent to \( K', C \bullet (D - E + K') = C \bullet (D - E + K) \).

Recall \( D = D_1 + D_2 \), where \( D_1 \), \( i = 1, 2 \) is defined by either (3.3.1) or (3.3.2). In either case, one may see readily that \( C \bullet (D - E + K) \geq (c/2)(C \bullet (Z(x_1)) + C \bullet (Z(x_2))) - \Sigma i=3 N(i+1)(C \bullet Z(x_i)) \). Now the intersection numbers above may be computed using (i): observe that \( C \bullet Z(x_i) \) for \( i = 3, \ldots, N \) are either 0 or 1, all of \( C \bullet Z(x_i) \geq 0 \) for \( i = 1, 2 \) with at least one of them positive. Moreover, \( Z(x_1) \bullet Z(x_2) > 0 \) for only one of \( x_1, i = 3, \ldots, N \). Therefore, the intersection number \( C \bullet (D - E + K) > 0 \) if \( c \) is sufficiently large in comparison with \( e_3, \ldots, e_N \). This completes the proof of the proposition. \( \square \)
To complete the determination of the distance of the code \( C(X, \omega_X, E, P) \), it suffices to estimate the number \( l \) in Theorem 3.5 and the intersection numbers \( C_{a_i} \bullet (D - E + K) \). Apart from the following general techniques that we will use in computing the parameter \( l \), this will be handled on a case by case basis and several examples are worked out in detail in the next section.

**Proposition 4.15.** Assume the basic hypothesis in 3.4 and that \( X \) is a toric surface. (i) Let \( R, S \) denote two effective divisors on \( X \) so that if \( R = \Sigma_{i=1}^p R_i, S = \Sigma_{j=1}^p S_j \) with \( R_i, S_j \) the corresponding irreducible components, the \( \{R_i\} \) are all distinct from the \( \{S_j\} \). Let \( f \in \Gamma(X, \mathcal{O}_X(S - R)) \) so that it vanishes identically on the irreducible curves \( C_1, \ldots, C_p \) in \( X \), and so that all the \( C_i \)'s are distinct from the prime divisors \( R_j \). Then \( f \in \Gamma(X, \mathcal{O}_X(S - R - s_i (C_j)) \).

(ii) Let \( F' = D + K' \), where \( K' = K + \text{div}(g) \), and where \( g \) is the homogenization of the rational function \( \frac{J(q_1, \ldots, q_d)_{t_1, \ldots, t_d}}{g_1 \cdots g_d} \). Let \( f \in \Gamma(X, \mathcal{O}_X(F' - E)) \) so that it vanishes identically on the irreducible curves \( C_1, \ldots, C_p \) in \( X \), and so that all the \( C_i \)'s are distinct from the prime divisors \( E_j \) and the prime divisors in \( K \). Then the rational function \( f g \in \Gamma(X, \mathcal{O}_X(D - \Sigma_{i=1}^p (C_i - E + K)) \) (and hence also in \( \Gamma(X, \mathcal{O}_X(D - E + K)) \).

**Proof.** (i) The main observation is that the following conditions are satisfied: (i) since \( f \) vanishes identically on the curves \( C_i \), \( \text{div}(f)_{S_0} = B + \Sigma_{j=1}^p C_i \) where \( B \) is an effective divisor, and (ii) \( S - \text{div}(f)_{S_0} \geq 0 \). These, together with the hypothesis that the curves \( C_i \) are all distinct from the divisors \( R_j, S \), show that the \( R_j, S \) are getting cancelled with prime divisors in \( B \) or in \( S - \text{div}(f)_{S_0} \), and not with the \( C_i \)'s appearing in \( \text{div}(f)_{S_0} \). This implies \( \text{div}(f) - \Sigma_{i=1}^p C_j + S - R \geq 0 \) and proves (i).

(ii) Recall from 3.2.1 that the rational function \( g \) is the homogenization of \( \frac{J(q_1, \ldots, q_d)_{t_1, \ldots, t_d}}{g_1 \cdots g_d} \). Since the \( g_i \)'s are all distinct from in Proposition 3.2, one may observe that \( D = \text{div}(g)_{S_0} \). Therefore, \( \text{div}(f) + D + K' - E = \text{div}(f) + D + K + \text{div}(g) - E = \text{div}(f)_0 - \text{div}(f)_{S_0} + D - \text{div}(f)_{S_0} + \text{div}(g)_0 + K - \text{div}(f)_0 + K - \text{div}(g)_0 - \text{div}(f)_{S_0} \geq 0 \). Since the divisors \( C_i \) do not appear as prime divisors in \( E \) or \( K \), and since \( f \) vanishes identically on \( C_i, i \neq \frac{1}{1, \ldots, p} \), it follows that \( \text{div}(f)_0 - \Sigma_{i=1}^p C_i + E + \text{div}(g)_0 - \text{div}(f)_{S_0} \geq 0 \) and \( \text{div}(g)_0 \geq \text{div}(f)_{S_0} \). This proves \( \text{div}(f)_0 - \text{div}(f)_{S_0} + \text{div}(g)_0 - \text{div}(g)_{S_0} - \Sigma_{i=1}^p C_i + D + K - E \geq 0 \), i.e., \( \text{div}(f)_0 - \Sigma_{i=1}^p C_i + D + K - E \geq 0 \).

**Remark 4.16.** In [17], a variant of this result is used when \( E \) was trivial, i.e., \( F - E \) is effective. Then there are no assumptions on the curves. In the present formulation, we need to assume that the curves \( C_i \) are all distinct from the divisors \( E_j \) so that there is no possible cancellation among these.

**Lemma 4.17.** (i) Let \( R = \Sigma_{i=1}^p Z(x_i - a_i(j) \phi_i), \bar{R} = \text{div}(Z(x_i)) \) and \( S \) denote any divisor on \( X \). Then the assignment \( f \mapsto f \mid_{\Pi_{j \neq i=1}^{p}(x_i - a_i(j) \phi_i)} \) defines a bijection \( \Gamma(X, \mathcal{O}_X(S - R)) \rightarrow \Gamma(X, \mathcal{O}_X(S - \bar{R})) \).

(ii) Let \( R = \Sigma_{j=1}^N e_j Z(x_j - h_j \psi_j) \), \( \bar{R} = e_j Z(x_j) + \Sigma_{j=1}^N e_j Z(x_j - h_j \psi_j) \) and \( S \) denote any divisor on \( X \). Then the assignment \( f \mapsto f \mid_{\Pi_{j \neq i}^{N}(x_j - h_j \psi_j)} \) defines a bijection \( \Gamma(X, \mathcal{O}_X(S - R)) \rightarrow \Gamma(X, \mathcal{O}_X(S - \bar{R})) \).

(iii) Let \( S = \Sigma_{j=1}^m Z(x_j - a_j(j) \phi_j), \bar{S} = m_j Z(x_j) + m_j Z(x_j - a_j(j) \phi_j) \) and \( R \) denote any divisor on \( X \). Then the assignment \( f \mapsto \Pi_{j \neq i=1}^{m} (x_j - a_j(j) \phi_j) \mid_{\Pi_{j \neq i}^{m}(x_j - a_j(j) \phi_j)} \) defines a bijection \( \Gamma(X, \mathcal{O}_X(S - R)) \rightarrow \Gamma(X, \mathcal{O}_X(S - \bar{R})) \).

**Proof.** (i) If \( g = f \mid_{\Pi_{j \neq i=1}^{p}(x_i - a_i(j) \phi_j)} \), then it is clear that \( \text{div}(f) = \text{div}(g) - \text{div}(Z(x_i)) + \Sigma_{j=1}^p Z(x_i - a_i(j) \phi_j) \). Now substituting this into \( \text{div}(f) + S - R \geq 0 \) proves that \( \text{div}(g) + S - \bar{R} \geq 0 \). This proves (i).

(ii) If \( g = f \mid_{\Pi_{j \neq i}^{N}(x_j - h_j \psi_j)} \), then it is clear that \( \text{div}(f) = \text{div}(g) - e_j(Z(x_j)) + e_j Z(x_j - h_j \psi_j) \). Now substituting this into \( \text{div}(f) + S - R \geq 0 \) proves \( \text{div}(g) + S - \bar{R} \geq 0 \). This proves (ii), and the proof of (iii) is similar.

**Remark 4.18.** In case \( e_1 = x_1 \) and \( \phi_1 = x_3 \) (as occurs in the second and third examples considered in the next section), one may choose \( h_1 = 1 \). Since we have already assumed \( h_1 \) is different from all the \( a_1(j) \), this will ensure that the \( \{E_i\} \) and \( \{F_j\} \) are all distinct as required in the Proposition 4.15 above.

**5. Examples**

In this section we consider several examples of toric surfaces: projective spaces of dimension 2 blown up at a point and Hirzebruch surfaces. In all of these cases, we will let \( X \) denote the toric surface over which the code is defined, \( E \) will be an effective divisor and \( P = \{P_1, \ldots, P_n\} \) will be a collection of \( k \)-rational points all chosen as before. We will let the ground field \( k = \mathbb{F}_2 \) for some \( n \). The goal of this section is to complete the explicit determination of the parameters of the dual code \( C = C(X, E, \mathcal{P})^\perp \) in the above examples.
Recall that that the cardinality of $k^*$ is $c$ by assumption. In the first example, there are exactly $(c-1)^2$ rational points $P_i$ at which one takes the residues of the sections $s \in \mathcal{O}_X(E)$. Therefore, the length of the code is $(c-1)^2$.

An important observation that we use in computing the various intersection numbers is the following toric Nakai criterion: see [23, Theorem 2.18].

**Theorem 5.1.** Let $X$ denote a non-singular projective toric variety over a field $k$ of dimension $d$. Then a divisor $D$ on $X$ is ample if and only if the intersection number $(D \cdot V(\tau)) > 0$ for the closed sub-variety $V(\tau)$ of $X$ associated to a $d-1$-dimensional cone in the fan of $X$.

We will verify the criterion (3.3.3) in each of the following cases for the divisors defined there: in view of the above theorem it will follow that the divisors $D_i$, $i = 1, 2$ are ample.

**Example 5.2.** $\mathbb{P}^2$ with $\mathcal{L} = \mathcal{O}_{\mathbb{P}^2}(r) = \mathcal{O}_{\mathbb{P}^2}(E)$. Here the fan is given by $e_1 = \left(\begin{array}{c}1 \\ 0 \end{array}\right)$, $e_2 = \left(\begin{array}{c}0 \\ 1 \end{array}\right)$, and $e_3 = -e_1 - e_2$. The homogeneous co-ordinate ring has three variables $x_i$ corresponding to each of the $e_i$, which are divisors. We will denote the divisor associated to $e_i$ by $E_i$. We choose the polytope with vertices given by the vectors $v_1 = \left(\begin{array}{c}0 \\ 0 \end{array}\right)$, $v_2 = \left(\begin{array}{c}r \\ 0 \end{array}\right)$ and $v_3 = \left(\begin{array}{c}0 \\ r \end{array}\right)$ for a fixed positive integer $n$. Now the inward normals to the faces of the above polytope will be the vectors $e_1$, $e_2$, and $e_3 = -e_1 - e_2$. This polytope corresponds to the line bundle $O_{\mathbb{P}^2}(r)$ on $\mathbb{P}^2$ so that $\dim(\Gamma_2, \mathcal{L}) = \# \text{points}$ which are divisors. We see $\mathcal{O}_{\mathbb{P}^2}(1)$ is ample if and only if the intersection number $a_i = 1$ for each $i = 1, 2$, and $a \in k^*$. Therefore, the hypotenses in (3.3.3) are satisfied.

Observe that $E = rZ(x_2)$, $D_1 = \Sigma_{j=1}^{c-1}Z(x_1 - a_jx_3) + Z(x_2 - f_2x_3)$, $D_2 = \Sigma_{j=1}^{c-1}Z(x_2 - 2) + \Sigma_{j=1}^{c-1}Z(x_2)$ where $a_j = \{a_i(j)| j = 1, \cdots, c\}$, i.e. $a_i(c) = f_i$, $i = 1, 2$. Observe that $K = -Z(x_1) - Z(x_2) - Z(x_3)$. One may also observe that $|D_1| \cap |D_2| = \{x_1 = 0\}$ so that $M = m+1$ in this case.

One may verify readily that the hypotheses in (3.4) (0) through (3), (5), and (7) are satisfied. We let $s_0 = \frac{(x_2 - a_2x_3)^2}{x_3}$; one can verify readily this satisfies 3.4.(6). The form $\frac{dt_1 \wedge dt_1}{x_3}$ when homogenized becomes \[ \frac{x_1^{a_1+a_2+a_3}}{x_3} \] which shows the hypothesis in 3.4(4) is also satisfied.

We let $s = \frac{(x_2 - a_2x_3)^2}{x_3}$. Now $\text{div}(s_0) = 2D_{2,j_2}$ and $\text{div}(s) = E$. Now it is straightforward to verify that $Res_{P_i}(s_0) = 0$ for any point $P_i$, $i = 1, \cdots, m$. It follows that the above section satisfies the hypotheses in Corollary 4.5. In order to verify the hypothesis in 4.4, we let $s = \frac{(x_2 - a_2x_3)^2}{x_3}$. In this case $\text{div}(s_0) = 2D_{2,j_2}$ and $\text{div}(s) = E$.

Next observe that $D = \Sigma_{j=1}^{c-1}Z(x_1 - a_jx_3) + \Sigma_{j=1}^{c-1}Z(x_2 - a_2x_3)$. Therefore, $D + K - E$ is linearly equivalent to $(c-2)Z(x_1) + (c-1)Z(x_2) + (r+1)Z(x_3)$. Therefore, the corresponding support function $h$ (see [23, p. 72]) is given by $h(e_1) = -(c-2) - c+2$, $h(e_2) = -(c-1) = -c+1$, and $h(e_3) = r+1$. It follows that the corresponding polytope is given by $P = \{m \in \mathbb{N}_c | m, e_1 \geq -c+2, m, e_2 \geq -c+1, m, e_3 \geq r+1\}$. Therefore, $P$ has as faces the lines $x_1 = -c+2$, $x_2 = -c+1$, and $-x_1 - x_2 = r+1$: see figure below.
Next we proceed to compute the intersection numbers \((D + K - E - lZ(x_1)) \bullet (Z(x_1))\). As observed above that \(D + K - E\) is linearly equivalent to \((c - 2)Z(x_1) + (c - 1)Z(x_2) - (r + 1)Z(x_3)\). Therefore, one may compute the intersection number \(((D + K - E - lZ(x_1)) \bullet (Z(x_1)))\) to be \((c - 2 - 1) + (c - 1) - (r + 1)\). It follows that the number of zeroes of \(f\) is bounded above by

\[ l(c + c - l - 2)(c - 1) - (r + 1) \leq l(c + c - l - 2) + c - r - 2 = l(c - 1) + 2c - r - 4 \leq 2c^2 - rc - 4. \]

Next we will let \(r\) and \(c\) be such that

\[ 5/4(c - 1) \geq r \geq 9/8(c - 1). \]

Therefore, one may compute the dimension and distance to be bounded below by

\[ \text{dimension}(C) \geq (c - 1)^2 - (r + 1)(r + 2)/2 \geq 7/32(c - 1)^2 - 15/8(c - 1) - 1 \]

\[ \text{distance}(C) \geq 1/8c^2 - 25/8c + 5. \]

In order to obtain a good family of codes, we may proceed as follows. Now we choose a fixed algebraic closure \(k\) of \(k\) and run through all finite extensions of \(k\) inside \(k\). Recall \(c\) denotes the number nonzero elements in the ground field \(k\): we can let \(c \to \infty\) by running through all finite sub-fields of \(k\). At the same time we also let \(r \to \infty\) with \(r\) and \(c\) satisfying the relations in (5.0.6). Therefore, the ratio \(\text{dimension}(C)/\text{length}(C)\) is bounded below by \(7/32\) which is also the limit

\[ \lim_{\text{length}(C) \to \infty} \frac{\text{dimension}(C)}{\text{length}(C)} = 7/32. \]

Similarly the ratio \(\text{distance}(C)/\text{length}(C)\) is bounded below by \(1/8\).
which is also the limit $\lim_{\text{length}(C) \to \infty} \frac{\text{dimension}(C)}{\text{length}(C)} = 1/8$. Therefore, it is easy to see that we obtain a good family of codes this way, just from $\mathbb{P}_2$.

We conclude this example by computing the dimension of the code $\Gamma(X, \omega_X(D - E))$ explicitly and comparing that with the dimension of the code dual to $\Gamma(X, \mathcal{O}_X(E))$, provided we assume $k = \mathbb{C}$. Though this is not needed for estimation of the parameters of the code, we hope that this computation will shed some insight into the duality results we obtained earlier in this section. First observe that $D - E$ is linearly equivalent to $(c - 1)B_1 + cB_2 - rB_2$, where $B_i = Z(x_i)$. By Serre-duality, one observes that $\Gamma(X, \omega_X(D - E)) \cong H^2(X, \mathcal{O}_X(rB_3 - (c - 1)B_1 + cB_2))^\vee \cong \oplus_{m \in \mathbb{M}} (\mathbb{P}^{2})^\vee(e(m))$, where $Z(h, m) = \{n \in \mathbb{N}| m \geq h(n)\}$, and $h$ is the support function associated to the divisor $rB_3 - (c - 1)B_1 + cB_2$. (See [23, p. 75].) Therefore, $H^2_{\mathbb{P}^2}(\mathbb{P}^{2} ; \mathbb{C})$ to be non-trivial, one needs $Z(h, m) = \{0\}$, and in this case, $H^2_{\mathbb{P}^2}(\mathbb{P}^{2} ; \mathbb{C}) \cong \mathbb{C}$. Now observe that the support function $h$ associated to the line bundle $\mathcal{O}_X(rB_3 - (c - 1)B_1 + cB_2)$ is given by $h(e_1) = c - 1$, $h(e_2) = c$, and $h(e_3) = -r$. Therefore, on the cone $\sigma_1$ (spanned by $e_1$ and $e_2$), $h(ae_1 + be_2) = c + c = c(e_1^2) + c(e_2)^2, a + b = -a + b$. Similarly on $\sigma_2$ (spanned by $e_2$ and $e_3$) $h(ae_2 + b e_3) = ac + rb$ and in the cone $\sigma_3$ spanned by $e_3$ and $e_1$, $h(ae_3 + be_1) = -ar + bc - b$. If $m = xe_1' + ye_2'$, one may compute $<m, ae_1 + be_2 >= ax + by, <m, ae_2 + be_3 >= -b(x + y) + ay$, and $<m, ae_3 + be_1 >= -a(x + y) + bx$. Therefore, in order that the condition $Z(h, m) = \{0\}$, we need the following three inequalities to be satisfied for all $a > 0$ or $b > 0$:

\begin{align*}
ax + by &< ac + cb - a, \text{ in the cone } \sigma_1 \\
ay - bx + y &< ac + rb, \text{ in the cone } \sigma_2 \\
-a(x + y) + bx &< -ra + bc - b, \text{ in the cone } \sigma_3 
\end{align*}

Clearly we may choose $0 < x < c - 1$ and $0 < y < c$ so that the first inequality is satisfied. We may let $b = 0$ to conclude from the second inequality that $y < c$ and by letting $a = 0, b \neq 0$ there to conclude $r < x + y$. From the third inequality we may conclude similarly that $x < c$ and that $r < x + y$. The required region satisfying all the above inequalities is now the triangle with vertices $(c - 1, c), (r - c, c)$ and $(c - 1, r - c + 1)$. Therefore, one may conclude that the dimension of the $k$-vector space $\Gamma(X, \omega_X(D - E)) = \frac{(2r - c + 1)^2}{2}$. On the other hand, the dimension of the $k$-vector space which is the dual code of $\Gamma(X, \mathcal{O}_X(E))$ is given by $(c - 1)^2 - \frac{(c - 1)(c + 2)}{2}$. It follows that if $c$ is sufficiently large in comparison with $r$, the dimension of the dual code is smaller than the dimension of the code $\Gamma(X, \omega_X(D - E))$, though both are $O(c^2)$. (This also provides an independent confirmation that the residue code computed using $\Gamma(X, \omega_X(D - E))$ is in general larger than the dual code: we had proved earlier in Theorem 1.2 that the first maps surjectively to the latter.)

Example 5.3. Next we consider a projective space of dimension 2 with a point blown up as follows. Now we will consider the refined normal fan consisting of the vectors $u_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, u_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, u_3 = \begin{pmatrix} -1 \\ -1 \end{pmatrix}, \text{ and } u_4 = \begin{pmatrix} 0 \\ -1 \end{pmatrix}$.

We next consider the polytope with vertices $v_1 = \begin{pmatrix} 0 \\ 0 \end{pmatrix}, v_2 = \begin{pmatrix} r \\ 0 \end{pmatrix}, v_3 = \begin{pmatrix} r - s \\ s \end{pmatrix}, \text{ and } v_4 = \begin{pmatrix} 0 \\ s \end{pmatrix}$. Here $r, s \geq 0, \text{ and } r \geq s$. Accordingly, each of the four faces of this polytope corresponds to a variable in the homogeneous co-ordinate ring with $x_i$ corresponding to the ray $u_i$. The toric variety $X$ is obtained by blowing up a point on the projective space $\mathbb{P}_2$. One may compute $CH_1(X) = \mathbb{Z} \oplus \mathbb{Z}$. Therefore, in the homogeneous co-ordinate ring of the toric variety, the variables have the following weights:

\begin{align*}
\text{weight of } x_1 \text{ and } x_3 &= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\
\text{weight of } x_2 &= \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \text{ and } \\
\text{weight of } x_4 &= \begin{pmatrix} -1 \\ 1 \end{pmatrix}
\end{align*}

Clearly the basic hypotheses in 3.3 are satisfied.

Next observe that $h(u_i) = 0$ for $i = 1, 2, \text{ and } h(u_3) = < r - s, -1 > = -r, h(u_4) = < 0, 0 > = -s$. Therefore, $E = rZ(x_3) + sZ(x_4)$. 

TORIC RESIDUE CODES I 19
We proceed to verify that the basic hypotheses in 3.3 and 3.4 are satisfied. Observe that $n = 2$ and $N = 4$ in this example. We replace the above divisor by the linearly equivalent divisor given by $rZ(x_3 - h_1 x_1) + sZ(x_4)$, where $h_3 \in k^*$ is a fixed element: henceforth we will denote this divisor by $E$. (We will use $h_3 = 1$.) Observe that since this is linearly equivalent to the divisor $rZ(x_3) + sZ(x_4)$, the global sections of the corresponding line bundle are isomorphic to the global sections of the line bundle corresponding to the latter. We require $r + s \geq 2$. In this case the irrelevant ideal is generated by $x_3 x_4, x_1 x_2, x_1 x_2$, and $x_2 x_3$. The only points of intersection for two divisors $Z(x_1 - cx_3)$ and $Z(x_2 - dx_3 x_4)$ are in the dense orbit. Two divisors $Z(x_1 - cx_3)$ and $Z(x_2 - dx_3 x_4)$ for $c \neq d$ do not intersect. The only point of intersection for two divisors of the form $Z(x_2 - ax_1 x_3)$ and $div(x_2 - bx x_3 x_4)$ are the points with homogeneous co-ordinates $x_2 = 0 = x_3$ and $x_1 = 0, x_4 = 0$. By the action of the torus $\mathbb{G}_m^2$, these identity with a single point in the toric-variety under consideration. The intersection $|D_1| \cap |D_2|$ has exactly this point in addition to the points in the dense torus, so that $M = m + 1$, in this example. In this case we choose the subsets $J_1^* = k^* - \{f_1, h_3\}$ and $J_2^* = k^* - \{f_2\}$. (i.e. We need to remove two points $x_1 = f_1$ and $x_1 = h_3$ (i.e. in terms of the co-ordinates on the dense torus, $t_1 = h_3$) from the $x_1$-axis. We only remove the point $x_2 = f_2$ from the $x_2$-axis (i.e. in terms of the co-ordinates on the dense torus, $t_2 = f_2$.) Observe as a result, that $m = (c - 2)(c - 1) = c^2 - 3c + 2$ in this example.

Now one may compute the intersection numbers $Z(x_1) \bullet Z(x_1) = 0, Z(x_2) \bullet Z(x_1) = 1, Z(x_1) \bullet Z(x_2) = 1, Z(x_1) \bullet Z(x_3) = 0, Z(x_2) \bullet Z(x_3) = 1, Z(x_3) \bullet Z(x_2) = 0, Z(x_4) \bullet Z(x_3) = 0, Z(x_4) \bullet Z(x_3) = 1$ and $Z(x_4) \bullet Z(x_4) = -1$. It follows that the conditions in (3.3.3) are satisfied.

Next one may readily verify all the hypotheses (1) through (3) in 3.4 are satisfied. Observe that $|J_i^*| = |k^*| - 2$ and $|J_2^*| = |k^*| - 1$ in the definition of the divisors $D_i$, $i = 1, 2$. Denoting by $(t_1, t_2)$ the co-ordinates on the torus $\mathbb{T} = \mathbb{G}_m^2$, and homogenizing using the technique in [7, Theorem 4], one sees that the differential form

$$\frac{dt_1 dt_2}{\prod_{i=1}^{n}(x_1 - a_i(x_1 x_2))}$$

transforms to

$$\frac{x_1^{2-\epsilon} dx_1}{\prod_{i=1}^{n}(x_1 - a_i(x_1 x_2) x_3 x_4)}.$$  

Moreover, one may verify that the weight of $x_1 = \text{the weight of } x_3$, and the weight of $x_2$ is the weight of $x_3 x_4$. The weight of $x_3 x_4 = \binom{r-s}{s}$ which is also equal to the weight of $(x_1 - a_1 x_3)^{2-\epsilon} (x_2 - a_2 x_3 x_4)^{s}$. These verify the hypothesis (4) in 3.4. Now we may choose $s_0 = \binom{(x_1 - f_1 x_3)^{2-\epsilon} (x_2 - f_2 x_3 x_4)^s}{(x_3 - h_3 x_1) x_4}$, where $f_1 \in k^*$ and $h_3 \in k^*$ denote the chosen points, with $h_3$ chosen to be distinct from all the $a_1(j)$, $j = 1, \ldots, c - 2$. Clearly this section does not vanish at any of the points $P_i, i = 1, \ldots, m$ since the co-ordinates of these points are all different from $f_i$. Recall also that $r + s \geq 2$ by our assumption. Moreover, the arguments in the paragraph above show that indeed the intersection $\cap_{i=1}^{c}|D_i| \cap |E|$ is empty. We have therefore verified the hypotheses (5) and (6) in 3.4. The hypothesis (7) there is obviously satisfied since the rays corresponding to $x_3$ and $x_4$ are chosen as above. Therefore, it suffices to estimate the parameters of the resulting codes in this example.

Now one may compute the number of lattice points in the above polytope to be $(s + 1)(r - s/2 + 1)$.

Next we consider the divisor $D$: we will choose this as in (3.3.2). Let $T$ denote the two dimensional split torus $\mathbb{G}_m^2$ and we will denote $(t_1, t_2)$ denote co-ordinates on this torus. The divisor $D$ will be of the form:

$$\Sigma_{j=1}^{c-2}\delta(cZ(t_1 - a_1(j) x_3)) + \delta(Z(t_2 - f_2) + \delta(Z(t_2 - a_2(j)) + \delta(Z(t_1 - f_1)))$$

Upon homogenizing using the technique in [7, Theorem 4], and making use of the weights of the variables as in (5.0.9), we obtain the following formulae for the divisor obtained by taking the closures of each $Z(t_i - a_i(j))$, $i = 1, 2$ and $j = 1, \ldots, c$, respectively:

$$\Sigma_{j=1}^{c-2}Z(x_1 - a_1(j) x_3) + Z(x_2 - f_2 x_3 x_4) + \Sigma_{j=1}^{c-2}Z(x_2 - a_2(j) x_3 x_4) + Z(x_1 - f_1 x_3)$$

As shown above this is linearly equivalent to

$$(c - 1).Z(x_1) + cZ(x_2)$$

The divisor $D + K - E = D_1 + D_2 + K - E$ is linearly equivalent to $(c - 2)Z(x_1) + (c - 1)Z(x_2) - (r + 1)Z(x_3) - (s + 1)Z(x_4)$. Using the computation of the intersection numbers between the various toric divisors above, one may compute the intersection number $(D + K' - E) \bullet Z(x_1) = (D + K - E) \bullet Z(x_1)$ to be $c - 1 - (s + 1)$.

Next we proceed to estimate the parameter $l$ as in Theorem 3.5. Therefore, suppose there are $l$ (0 $\leq l \leq c$) curves $Z(x_3 - a_i(j) x_3)$, $j = 1, \ldots, l$ (with $a_i(j) \in k$) so that a rational function $f \in \Gamma(X, \mathcal{O}_X(D + K' - E))$ vanishes identically on these curves. i.e.

$$\text{div}(f)_0 - Z(x_3 - a_i(j) x_3) \geq 0$$
for all \( j = 1, \ldots, l \). First an application of Proposition 4.15(ii) will show that \( \Gamma(X, \mathcal{O}_X(D + K - E - Z_{j=1}x_1 - a_1(j)\phi_1)) \neq \{0\} \). Now an application of Lemma 4.17(i) with \( E = Z_{j=1}x_1 - a_1(j)\phi_1, E = lZ(x_1) \) and \( F = D + K - E \) will show that \( \Gamma(X, \mathcal{O}_X(D + K - E - lZ(x_1))) \neq \{0\} \). Next we apply Lemma 4.17(iii) with \( F = D + D_1, E = K - E - lZ(x_1) \) and \( F = (c - 1)Z(x_1) + cZ(x_2) \) to conclude that \( \Gamma(X, \mathcal{O}_X((c - 1)Z(x_1) + cZ(x_2) + K - E - lZ(x_1))) \neq \{0\} \). Another application of Lemma 4.17 (iii) with \( F = (c - 1)Z(x_1) + cZ(x_2) + K - lZ(x_1) \), \( E = rZ(x_3 - h_3x_1) + sZ(x_4) \), and \( E = rZ(x_3) + sZ(x_4) \) shows that

\[
\Gamma(X, \mathcal{O}_X((c - 2)Z(x_1) + (c - 1)Z(x_2) - (r + 1)Z(x_3) - (s + 1)Z(x_4) - lZ(x_1))) \neq \{0\}
\]

Next we proceed to compute the support function associated to the divisor \((c - 2)Z(x_1) + (c - 1)Z(x_2) - (r + 1)Z(x_3) - (s + 1)Z(x_4)\). This support function \( h \) (see [23, p. 72]) is given by \( h(e_1) = -(c - 2) = -c + 2 \), \( h(e_2) = -(c - 1) = -c + 1 \), \( h(e_3) = r + 1 \), and \( h(e_4) = s + 1 \). It follows that the corresponding polytope is bounded by the faces which are the lines \( x_1 = -c + 2 \), \( x_2 = -c + 1 \), \( x_2 = -s - 1 \), and \(-x_1 - x_2 = r + 1\): see figure below.

The polytope corresponding to the line bundle in (5.0.14) has its first vertical face moved from \( x_1 = -c + 2 \) to \( x_1 = -c + 2 + l \). Since the global sections of the bundle is non-empty as shown by (5.0.14), it follows that \(-c + l + 2 \leq -r - 1 + c - 1 \), and hence that

\[
l \leq 2c - r - 4\]

Therefore, the number of zeroes of \( f \) is bounded above by \( lec + e - s - 2 \leq 2c^2 - rc - 4c + c - s - 2 \leq 2c^2 - rc - 3c - s \). Henceforth we keep \( s, r \) so that \( c/5 > s > 1/6c \) and \( 2c > r \geq 3/2c \); then \( 2c^2 - rc - 3c - s \leq (1/2)c^2 - 3c - 1/6c \) and \( c^2 - 3c + 2 + c - s/2 + 1 \geq (37/60) c^2 - (307/60) c + 1 \). Therefore, we may compute the parameters of the code \( C = C(X, E, P) \) as:

\[
dimension(C) \geq c^2 - 3c + 2 - (s + 1)(r - s/2 + 1) \geq (37/60) c^2 - (307/60) c + 1\]

\[
distance(C) \geq c^2 - 3c + 2 - 2c^2 + rc + 3c + s \geq c^2/2 + (1/6)c + 2\]

One can see that letting \( c \to \infty \) (i.e. taking larger and larger field extensions of \( k \)), and keeping \( r \) and \( s \) as above, we obtain a good family of codes this way.

**Example 5.4.** Next we consider a weighted projective space of dimension 2 where the weights are \((1, 1, 2)\) with the singularity resolved by blowing up the singular point. Observe that the resulting non-singular variety identifies with the Hirzebruch surface \( F_2 \) which is the total space of the \( \mathcal{O}_{P^1}(-2) \)-bundler over \( P^1 \). We will denote this weighted projective space by \( P_2(1,1,2) \). Here the fan is given by \( e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \), \( e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \), and \( e_0 = -e_1 - 2e_2 \). We choose the polytope with vertices given by the vectors \( v_1 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \), \( v_2 = \begin{pmatrix} 2r \\ 0 \end{pmatrix} \), and \( v_3 = \begin{pmatrix} 0 \\ r \end{pmatrix} \) for a fixed positive integer \( r \) which we assume is a multiple of 5. Now the primitive inward normals to the faces of the above polytope will be the vectors \( e_1, e_2, \) and \(-e_1 - 2e_2 \). These correspond to divisors and we introduce variables \( x_i \), corresponding to each of these.

Next we will consider the refined normal fan consisting of the vectors \( u_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \), \( u_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \), \( u_3 = \begin{pmatrix} -1 \\ -2 \\ 0 \end{pmatrix} \), and \( u_4 = \begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix} \).
We consider the polytope with vertices $v_1 = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, $v_2 = \begin{pmatrix} 2r \\ 0 \end{pmatrix}$, $v_3 = \begin{pmatrix} 2r - 2s \\ s \end{pmatrix}$ and $v_4 = \begin{pmatrix} 0 \\ s \end{pmatrix}$. The corresponding variety is the Hirzebruch surface $F_2$. Accordingly each of the faces of this polytope corresponds to a variable in the homogeneous co-ordinate ring of $F_2$ with $x_i$ corresponding to the ray $u_i$. Now one may compute the number of lattice points in the above polytope to be $(s + 1)(2r - s + 1)$. We will let the line bundle on $X$ corresponding to this polytope be denoted $\mathcal{L}$.

Next observe that $h(u_i) = 0$ for $i = 1, 2$, and $h(u_3) = -\left(\begin{pmatrix} 2r - 2s \\ s \end{pmatrix}, -\frac{1}{2}\right) = -2r$, $h(u_4) = -\left(\begin{pmatrix} 0 \\ s \end{pmatrix}, -\frac{1}{2}\right) = -s$. Therefore, the above polytope corresponds to the divisor $2rZ(x_3) + sZ(x_4)$. We will replace this by the linearly equivalent divisor $E = 2r(Z(x_3 - h_3x_1)) + sZ(x_4)$, where $h_3 \in k^*$. Observe that $CH_1(F_2) = \mathbb{Z} \oplus \mathbb{Z}$. Therefore, one may now compute the weights of the variables $x_i$ to be as follows:

$$(5.0.17) \quad \text{weight of } x_1 \text{ and } x_3 = \begin{pmatrix} 1 \\ 0 \end{pmatrix},$$

$$\text{weight of } x_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \text{ and}$$

$$\text{weight of } x_4 = \begin{pmatrix} -2 \\ 1 \end{pmatrix}.$$

Now one may compute the intersection numbers $Z(x_1) \cdot Z(x_1) = 0, Z(x_2) \cdot Z(x_1) = 1, Z(x_1) \cdot Z(x_4) = 1, Z(x_1) \cdot Z(x_3) = 0, Z(x_2) \cdot Z(x_3) = 2, Z(x_3) \cdot Z(x_2) = 1, Z(x_1) \cdot Z(x_2) = 0, Z(x_3) \cdot Z(x_4) = 0, Z(x_4) \cdot Z(x_3) = 1$, and $Z(x_4) \cdot Z(x_2) = -2$. One may show using these computations that the hypothesis in (3.3.3) is satisfied. In this case also we choose the subsets $J_1 = k^* - \{c_1, h_3\}$ and $J_2 = k^* - \{c_2\}$. (i.e. We need to remove two points $x_1 = c_1$ and $x_1 = h_3$ (i.e. in terms of the co-ordinates on the dense torus, $t_1 = h_3$) from the $x_1$-axis. We only remove the point $x_2 = c_2$ from the $x_2$-axis (i.e. in terms of the co-ordinates on the dense torus, $t_2 = c_2$.) Now $|E| \cap |D_1| \cap |D_2| = \phi.$ Moreover, in this case also $m = (c - 2)(c - 1) = c^2 - 3c + 2$ and $M = m + 1$ as in the last example. In view of these, it is clear that all the hypotheses in 3.3 are satisfied.

We proceed to verify that the basic hypotheses in 3.4 are also satisfied. Observe that $n = 2$ and $N = 4$ in this example. We will assume that $r + s \geq 2$ so that all the hypotheses (1) through (4) in 3.4 are satisfied. Denoting by $(t_1, t_2)$ the co-ordinates on the torus $T = \mathbb{G}_m^2$, and homogenizing using the technique in [7, Theorem 4], one sees that the differential form $\frac{dt_1 \wedge dt_2}{(t_1 - a_1)(t_2 - a_2)}$ transforms to $\frac{x_3^{2r - 2s}x_4^{-3s}}{(x_1 - a_1x_3)(x_2 - a_2x_4)}$. Moreover, one may verify that the weight of $x_1$ is the weight of $x_3$ and the weight of $x_2$ is the weight of $x_4$. The weight of $x_3^{2r - 2s}x_4^{-s}$ which is also equal to the weight of $(x_1 - a_1x_3)^{2r - 2s}(x_2 - a_2x_4)^s$. Therefore, we may choose $s_0 = \frac{(x_1 - c_1x_3)^{2r - 2s}(x_2 - c_2x_4)^s}{x_3^{2r - 2s}}$, where $c_1 \in k^*$ denotes the chosen point. Clearly this section does not vanish at any of the points $P_i, i = 1, \cdots, m$ since the co-ordinates of these points are all different from $c_i$.

We have verified the hypotheses (5) and (6) in 3.4. The hypothesis (7) there is obviously satisfied since the rays corresponding to $x_3$ and $x_4$ are chosen as above. Therefore, it suffices to estimate the parameters of the resulting codes in this example.

Next we consider the divisor $D$: we will choose this as in 3.3.2. Let $T$ denote the two dimensional split torus $\mathbb{G}_m^2$ and we will denote $(t_1, t_2)$ denote co-ordinates on this torus. The divisor $D$ will be of the form:

$$\Sigma_{j=1}^{c-2} d(Z(t_1 - a_1(j))) + d(Z(t_2 - c_1)) + \Sigma_{j=1}^{c-1} d(Z(t_2 - a_2(j))) + d(Z(t_1 - c_1))$$

Upon homogenizing using the technique in [7, Theorem 4], and making use of the weights of the variables as in (5.0.17) we obtain the following formulae for the divisor obtained by taking the closures of each $Z(t_i - a_i(j)), i = 1, 2$, and $j = 1, \cdots, c$, respectively:

$$\Sigma_{j=1}^{c-2} Z(x_1 - a_1(j)x_3) + Z(x_2 - c_2x_3x_4) + Z(x_3 - a_2(j)x_3x_4) + Z(x_1 - c_1x_3)$$

As shown above this is linearly equivalent to

$$\Sigma_{j=1}^{c-2} Z(x_1 + cZ(x_2))$$
Now $D + K - E = D_1 + D_2 + K - E$ is linearly equivalent to $(c-2)Z(x_1) + (c-1)Z(x_2) - (2r+1)Z(x_3) - (s+1)Z(x_4)$. Now one may compute the intersection number $(D + K' - E) \cdot Z(x_1) = (D + K - E) \cdot Z(x_1)$ to be $c - 1 - (s + 1)$.

Next we proceed to compute the support function associated with the divisor $(c-2)Z(x_1) + (c-1)Z(x_2) - (2r+1)Z(x_3) - (s+1)Z(x_4)$. This support function $h$ (see [23, p. 72]) is given by $h(e_1) = -(c-2) = -c + 2$, $h(e_2) = -(c-1) = -c + 1$, $h(e_3) = 2r + 1$, and $h(e_4) = s + 1$. It follows that the corresponding polytope is bounded by the faces which are the lines $x_1 = -c + 1$, $x_2 = -c + 1$, $x_2 = -s - 1$, and $-x_1 - 2x_2 = 2r + 1$; see figure below.

Next suppose there are $l$ ($0 \leq l \leq c$) curves $Z(x_1 = a_i(j)x_3)$, $j = 1, \cdots, l$ (with $a_i(j) \in k$) so that a rational function $f \in \Gamma(X, \mathcal{O}_X(D + K' - E))$ vanishes identically on these curves. i.e.

\[(5.0.21) \quad \text{div}(f)_0 = Z(x_1 = a_1(j)x_3) \geq 0\]

for all $j = 1, \cdots, l$. Now an argument as in the last example will show that $-c + 2 + l \leq 2c - 2r - 3$, and hence that

\[(5.0.22) \quad l \leq 3c - 2r - 5\]

Therefore, the number of zeroes of $f$ is bounded above by $l(c + c - s - 2) \leq -2c^2 - 2rc - 5c + c - s = 2 - 3c^2 - 2rc - 4c - s - 2$. Henceforth we keep $s$ so that $c/10 > s > (1/12)c$ and $(6/4)c > r > (5/4)c$ so that $c^2 - 3c + 2 - 3c^2 + 2rc + 4c + s + 2 \geq 1/2c^2 + (13/12)c + 4$ and $(c^2 - 3c + 2) - (s + 1)(2r - s + 1) \geq (c^2 - 3c + 2) - (c/12 + 1)(3c - c/12 + 1) = (17/24)c^2 - (361/60)c + 1$. Therefore, we may compute the parameters of the code $C = C(X, \mathcal{L}, \mathcal{P})^\perp$ as:

\[(5.0.23) \quad \text{dimension}(C) \geq (17/24)c^2 - (361/60)c + 1\]

\[\text{distance}(C) \geq c^2 - 3c + 2 - 3c^2 + 2rc + 4c + s + 2 \geq c^2/2 + (13/12)c + 4\]

One can see that letting $c \to \infty$ (i.e. taking larger and larger field extensions of $k$), and keeping $r$ and $s$ as above, we obtain a good family of codes this way.

6. Application I: construction of quantum stabilizer codes from toric varieties

We will begin by reviewing briefly the construction of quantum stabilizer codes from codes containing their dual codes. The construction of quantum codes as stabilizer codes is now a well-developed technique for producing quantum codes: see [13] for a detailed account. Moreover, the technique of producing stabilizer codes starting with a classical code containing its dual is now well-known: this is the so-called Calderbank-Schor-Steane technique as developed in [11] and [27].

We will presently provide a brief outline of some of these to make the paper self-contained. We start with a triple $D' \supset D \supset D''$ of binary codes, i.e. over the field $F_2$, where $D$ is an $[n, k, d]$-code containing its dual $D^*$, and $D'$ is a larger $[n, k']$-code with $k' \geq k + 2$. Let $G$ be a generator matrix of $D$, and let $G'$ be a matrix such that \( \begin{pmatrix} G \\ G' \end{pmatrix} \) is a generator matrix for the code $D'$. Denote by $d'^2$ the second generalized weight of $D'$, i.e., the minimum weight of the bit-wise $OR$ of two different nonzero codewords. Form the code $C \subseteq F_2^{2n}$ with the generator matrix \( \begin{pmatrix} G \\ 0 \\ G' \\ G'' \end{pmatrix} \) where the matrix $G''$ is obtained from $G'$ by permuting its rows so that no row stays on its place. Fix the following $F_2$-linear isomorphism between $F_2^{2n}$ and $F_4^n$ by mapping $(x_1, \ldots, x_n, y_1, \ldots, y_n)$ in $F_2^{2n}$ to
of quantum stabilizer codes given by (6.0.25)

\[ k_F = k + k' \quad \text{and} \quad d_F \geq \min(d, d'_2) \]

Moreover, one defines a symplectic form \( \omega \) on \( F \) as follows. Let \( x = (a_1, \ldots, a_n, b_1, \ldots, b_n) \) and \( x' = (a'_1, \ldots, a'_n, b'_1, \ldots, b'_n) \). We choose the above identification between \( F^n_2 \) and \( F^{2n}_2 \). In the basis of \( F^{2n}_2 \) the form \( \omega \) is defined by \( \omega(x, x') = \sum_{j=1}^{n} a_j b'_j + a'_j b_j \). Then it is shown in [10, section 2] that \( F \supseteq F' = \) the words in \( F^n_4 \) orthogonal to all the words in \( F \) using the form \( \omega \).

The parameters of the corresponding quantum stabilizer codes have been computed in [10, Corollary 1] and they are:

\[ k_Q = k + k' - n, \quad d_Q \geq \min(d, d'_2) \geq \min(d, 3/2d') \]

Next one starts with codes \( C \) and \( C^\perp \) over \( F_{2^t} \) with \( C^\perp \subseteq C \). Symbol-wise expansion, i.e., expressing a point of \( F_{2^{2t}} \) with respect to the standard basis of the \( F_2 \)-vector space \( F_{2^{2t}} \), produces two binary codes \( D \) and \( D^\perp \). Then it is known that \( D^\perp \subseteq D \) and also that \( D^\perp \) is the binary dual of the code \( D \). If the code \( C \) has parameters, \( n, k \) and \( d \), then the parameters of \( D \) are easily seen to be given by \( n_D = 2t, n, k_D = 2t, k \) and \( d_D \geq 2d \).

On the other hand, the technique of producing classical codes starting with algebraic curves defined over a finite field is now well-known, having originally developed by Goppa. A way of combining all of the above to produce quantum stabilizer codes starting with algebraic curves defined over finite fields was worked out in the relatively recent paper [10, section 4]. Here a key role is played by the residue theorem for curves (see [19, Theorem 7.14.2]) to produce classical codes \( D' \supseteq D \supseteq D^\perp \) as needed in the construction of quantum stabilizer codes discussed above.

In the rest of this section we will adapt the standard algebraic-geometry constructions of codes that contain their dual codes and quantum codes: the basic constructions so far have been done only for curves making use of the classical residue theorem for curves (as in [19, Chapter III, Theorem 7.14.2]). In the place of this classical residue theorem, we will make use of the results on toric residues we proved in the last two sections.

What is required is a triple \( C' \supseteq C \supseteq C^\perp \) of codes defined over \( F_{2^t} \) with good parameters.


We will choose two effective divisors \( E \) and \( E' \) so that \( E' \leq E \): for example if we choose \( E \) as in 3.4(5), then we may let \( E' = e'_{d+1}Z(x_{d+1} - h_{d+1}v_{d+1}) + \cdots + e'_{n}Z(x_{n} - h_{N}v_{N}) \) where \( e'_i \) is a non-negative integer \( 1 \leq e'_i \leq e_i, \quad i = n + 1, \ldots, N \). Clearly \( C(X, \mathcal{O}_X(E'), \mathcal{P}) \subseteq C(X, \mathcal{O}_X(E), \mathcal{P}) \), and hence \( C(X, \mathcal{O}_X(E'), \mathcal{P})^\perp \supseteq C(X, \mathcal{O}_X(E), \mathcal{P})^\perp \). Therefore, we will then let \( C' = C(X, \mathcal{O}_X(E'), \mathcal{P})^\perp \).

Next we will apply this to the two examples worked out in the last section.

**Example 6.1. The projective space \( \mathbb{P}^2 \) with a point blown-up.** In this case we chose positive integers \( r, r', s, s' \), so that \( 2r > r' \geq 3/2c \) and \( c/5 > s \geq s' > 1/6c \). Therefore, the parameters of the corresponding quantum stabilizer codes are given by

\[ k_Q = 2t(k + k' - n) \geq 2t((226/360)c^2 + (226/360)c^2 - 4c + 2 - (c^2 - 3c + 2)) = 2t(92/360c^2 - 3c + 2) \]

\[ d_Q = \min(d, 3/2d') \geq c^2/2 + (1/6)c + 2 \]

It follows that on letting \( c \to \infty \) and keeping \( r, r', s, s' \) satisfying the above inequalities, one obtains a good family of quantum stabilizer codes.

**Example 6.2. The Hirzebruch surface \( F_2 \).** In this case we chose positive integers \( r, r', s, s' \), so that \( 6/4 > r \geq r' > 5/4c \) and \( c/10 > s \geq s' > 1/12c \). Therefore, the parameters of the corresponding quantum stabilizer codes are given by

\[ k_Q = 2t(k + k' - n) \geq 2t((1019/1440)c^2 + (1019/1440)c^2 - 6c + 4 - (c^2 - 3c + 2)) = 2t(598/1440c^2 - 3c + 2) \]

\[ d_Q = \min(d, 3/2d') \geq c^2/2 + (13/12)c + 4 \]
Proof. \( H \) implies \( H \)

a field \( k \)

all \( i \)

closed fields.

used in the body of the paper. Most of these appear in [2, Chapter 1], where they are only stated over algebraically

be explored fully elsewhere.

generator matrices for the duals of toric evaluation codes. Clearly these are parity check matrices for the toric evaluation code. For the toric evaluation codes themselves, the parity check matrix would arise as a generator matrix for the dual code. The explicit construction of toric evaluation code is the generator matrix for the toric evaluation code. For the toric evaluation codes themselves, one needs to know a parity check matrix for the code in question, which for the dual code associated to a toric

the parity check matrix would arise as a generator matrix for the dual code. The explicit construction of toric evaluation code is the generator matrix for the toric evaluation code. For the toric evaluation codes themselves, the parity check matrix would arise as a generator matrix for the dual code. The explicit construction of toric evaluation code is the generator matrix for the toric evaluation code. For the toric evaluation codes themselves, one needs to know a parity check matrix for the code in question, which for the dual code associated to a toric

7. Application II: Decryption of toric evaluation codes

So far the only decryption technique that seems to be known in the toric context is for the dual codes associated to toric evaluation codes, and not for the toric evaluation codes themselves. The reason for this restriction is that one needs to know a parity check matrix for the code in question, which for the dual code associated to a toric evaluation code is the generator matrix for the toric evaluation code. For the toric evaluation codes themselves, the parity check matrix would arise as a generator matrix for the dual code. The explicit construction of toric evaluation codes provides generator matrices for these toric residue codes. Corollary 4.10 then shows that these provide generator matrices for the duals of toric evaluation codes. Clearly these are parity check matrices for the toric evaluation codes. Now one may apply the standard technique discussed, for example in [18, Chapter 6]. This will be explored fully elsewhere.

8. Appendix: Frobenius splitting

In this section we will summarize some of the key results on Frobenius splitting over finite fields that we have used in the body of the paper. Most of these appear in [2, Chapter 1], where they are only stated over algebraically closed fields.

Let \( X \) denote a regular scheme of finite type over a field \( k \) of characteristic \( p \). Let \( F : X \to X \) denote the absolute Frobenius morphism, i.e. it is the identity on the underlying topological spaces and is the \( p \)-th power map on the structure sheaf. \( X \) is Frobenius split if there is an \( \mathcal{O}_X \)-linear map \( \phi : F_*(\mathcal{O}_X) \to \mathcal{O}_X \) so that the composition \( \phi \circ F^# \) is the identity map of \( \mathcal{O}_X \). (Here \( F^# : \mathcal{O}_X \to F_*(\mathcal{O}_X) \) is the obvious map.) One may observe that the splitting map \( \phi \) is nothing but an endomorphism \( \phi : \mathcal{O}_X \to \mathcal{O}_X \) of the sheaf \( \mathcal{O}_X \), viewed only as an abelian sheaf, and satisfying: (a) \( \phi(f^p,g) = f,\phi(g) \), \( f,g\in \mathcal{O}_X \) and (b) \( \phi(1) = 1 \). If \( Y \) is a closed sub-scheme of \( X \) defined by the sheaf of ideals \( I \), \( \phi \) compatibly splits \( Y \) if \( \phi(F_*(I)) = I \).

Proposition 8.1. (See [2, 1.3.11 Proposition].) Let \( X \) denote a regular and projective scheme of finite type over the field \( k \) and of pure dimension \( d \). If there exists \( \sigma \in H^0(X, \omega_X^{-1}) \) with divisor of zeros \( \sigma_0 = Y_1 + \cdots + Y_d + Z \) where \( Y_1, \cdots, Y_d \) are prime divisors intersecting transversally at a point \( x \), i.e. there exists a regular system of parameters \( t_1, \cdots, t_d \) with \( t_i \) defining \( Y_i \) locally at \( x \) and \( Z \) is an effective divisor not containing \( x \), then \( \sigma^{-p} \epsilon H^0(X, \omega_X^{-1-p}) \) splits \( X \) compatibly with \( Y_1, \cdots, Y_d \).

Corollary 8.2. (See [2, 1.3.E.6].) Let \( X \) denote a regular toric variety over \( k \). Then \( X \) is Frobenius split compatibly with the boundary divisors of \( X \).

Proof. Let \( d = \dim_k(X) \) and let \( t_1, \cdots, t_d \) denote the coordinates on \( T \) coming from the \( d \)-factors \( \mathbb{G}_m \) in \( T \). Let \( \theta = \frac{dt_1 \cdots dt_d}{t_1 \cdots t_d} \epsilon H^0(X, \omega_X(\delta X)) \). Thus \( \sigma = \theta^{-1} \epsilon H^0(X, \omega_X^{-1}) \) and \( \sigma_0 = Y_1 + \cdots + Y_d \) where the \( Y_i \) are the prime divisors in \( \delta X \). Now the last proposition applies.

Corollary 8.3. (Kodaira vanishing: see [2, 1.2.9 Theorem].) Let \( X \) denote a projective, regular toric variety over a field \( k \) and let \( L \) denote an ample line bundle on \( X \). Then \( H^i(X, L \otimes \omega_X) = 0 \) for all \( i \geq 1 \).

Proof. First \( H^i(X, L^{-1}) = 0 \) for all \( \nu > 0 \) and \( i \leq \dim_k(X) - 1 \) by Grothendieck-duality: see [1, (1.3)]. Now Frobenius-splitting implies that \( H^i(X, L^{-1}) \) is a split summand of \( H^i(X, L^{-p}) \) for any positive integer \( \nu \). This implies \( H^i(X, L^{-1}) = 0 \) for all \( i \leq \dim_k(X) - 1 \). Finally Serre-duality (see [1, (1.2)]) shows \( H^i(X, L \otimes \omega_X) = 0 \) for all \( i \geq 1 \).
REFERENCES


Department of Mathematics, Ohio State University, Columbus, Ohio, 43210, USA.
E-mail address: joshua@math.ohio-state.edu

Department of Mathematics, Miami University, Oxford, Ohio, 45056, USA.
E-mail address: reza@calico.mth.muohio.edu