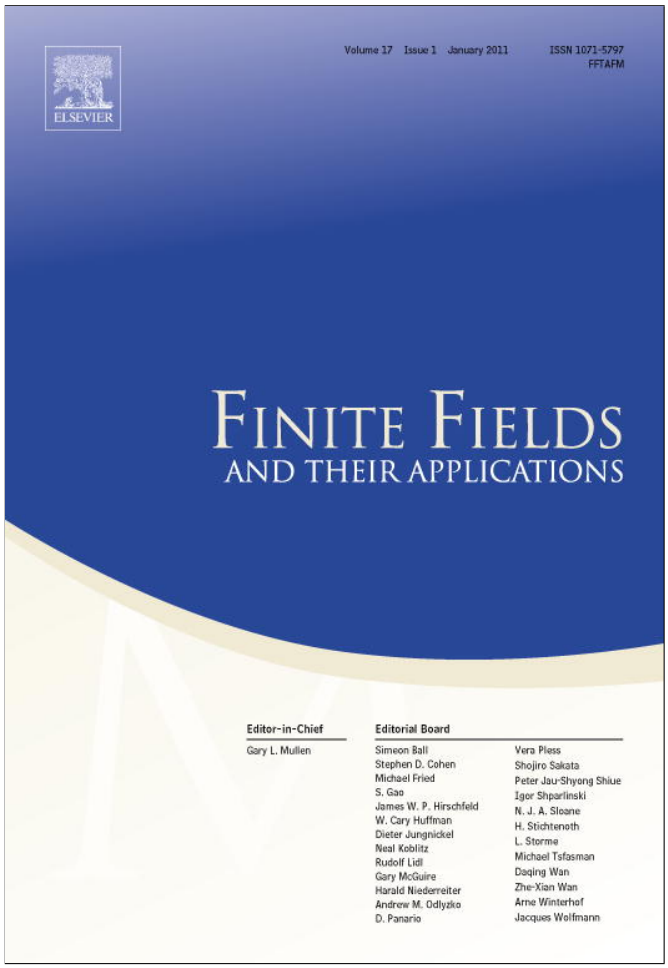
Provided for non-commercial research and education use.
Not for reproduction, distribution or commercial use.



This article appeared in a journal published by Elsevier. The attached copy is furnished to the author for internal non-commercial research and education use, including for instruction at the authors institution and sharing with colleagues.

Other uses, including reproduction and distribution, or selling or licensing copies, or posting to personal, institutional or third party websites are prohibited.

In most cases authors are permitted to post their version of the article (e.g. in Word or Tex form) to their personal website or institutional repository. Authors requiring further information regarding Elsevier's archiving and manuscript policies are encouraged to visit:

http://www.elsevier.com/copyright

Author's personal copy

Finite Fields and Their Applications 17 (2011) 15–50

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Toric residue codes: I

Roy Joshua [a,*,1], Reza Akhtar [b]

[a] Department of Mathematics, Ohio State University, Columbus, OH 43210, USA
[b] Department of Mathematics, Miami University, Oxford, OH 45056, USA

ARTICLE INFO

Article history:
Received 20 April 2009
Revised 11 July 2010
Accepted 4 October 2010
Communicated by W. Cary Huffman

MSC:
14G50
14C17
94B40

Keywords:
Toric varieties
Residues

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.

© 2010 Elsevier Inc. All rights reserved.

Contents

1. Introduction 16
2. Review of basic techniques 18
3. Toric residue codes 21
4. Duality results and estimation of parameters 27
5. Examples 37
6. Application I: The construction of quantum stabilizer codes from toric varieties 47
7. Application II: Decryption of toric evaluation codes 49
Acknowledgments 49
Appendix A. Frobenius splitting 49
References 50

* Corresponding author.
E-mail addresses: joshua@math.ohio-state.edu (R. Joshua), reza@calico.mth.muohio.edu (R. Akhtar).

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

1071-5797/$ – see front matter © 2010 Elsevier Inc. All rights reserved.
doi:10.1016/j.ffa.2010.10.001

Author's personal copy

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 [4], and studied extensively by several authors: see [8,10] and [22]. The present paper started with an attempt 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 [14] and [15]. 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 4.9 and Corollary 4.11.
- 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 4.14.

In the present paper we make a start in this direction, by developing the general theory for toric varieties and performing explicit computations for various toric surfaces. We hope to consider higher dimensional cases such as toric threefolds in future work. A major motivation for us in studying toric residue codes is to construct quantum stabilizer codes from toric varieties. It perhaps needs to be pointed out that so far, the only algebraic geometry codes that have been used to produce such quantum stabilizer codes are codes based on curves: our techniques seem to open up a way to produce such codes not only from toric surfaces, but also from higher dimensional projective smooth toric varieties.

The main ideas of the paper are now outlined. We begin with *evaluation codes* in Section 2. If X is a toric variety, defined over the finite field k, E is a divisor on X and $\mathcal{P} = \{P_1, \ldots, P_m\}$ is a set of k-rational points on X not contained in the polar part of E, then evaluation codes may be constructed by evaluating sections of the line bundle $\mathcal{O}_X(E)$ at the points in $\mathcal{P}$. The parameters of such codes have been analyzed, mainly for toric surfaces, using intersection theory: see [14].

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 local residues of these forms at the given k-rational points $\mathcal{P} = \{P_1, \ldots, P_m\}$. 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 codes may be constructed 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. Let D_i, $i = 1, \ldots, d$ denote d effective ample divisors on X and let $\bigcap_{i=1}^{d} |D_i| = \{R_i\}$ denote a set of*

Author's personal copy

k-rational points. Assume, in addition to the above situation, 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 $\eta \in \Gamma(X, \omega(\sum_i D_i))$ 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 [12, (3.8) Theorem]. The main difference is that such a statement in not true in general in positive characteristic – see [21]; 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, $C(X, \omega_X, E, \mathcal{P})$ where X is a smooth toric variety defined over a finite field k, E is divisor on X, ω_X is the sheaf of top-differential forms on X, and $\mathcal{P}$ is a given set of k-rational points on X. The code $C(X, \omega_X, E, \mathcal{P})$ is obtained by taking the residue of differential forms that satisfy certain conditions along E as defined more precisely in Section 3, at the k-rational points in $\mathcal{P}$. We prove that such codes, while not strictly the dual of evaluation codes, are nevertheless useful in estimating the parameters of the duals of toric evaluation codes. This is the content of Proposition 4.9 and Corollary 4.11, and these may be incorporated into the following main result.

Theorem 1.2. *Let X denote a smooth projective toric variety defined over a finite field k with X satisfying the basic hypotheses in* 3.4. *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* 3.3.

(i) *Then the modified residue code $C(X, \omega_X, E, \mathcal{P})$, defined as in* 4.3, *maps surjectively onto the dual code $C(X, E, \mathcal{P})^{\perp}$.*
(ii) *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 4.14 then shows how to obtain codes containing their dual codes this way which would be useful in constructing quantum stabilizer codes on toric surfaces.

We discuss several examples in detail in Section 5: 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. Quantum stabilizer codes for the usual $\mathbb{P}^2$ cannot be constructed; nevertheless, toric residue codes may be produced from this example which we analyze in depth. 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. The following is a summary of the results obtained for the construction of quantum stabilizer codes from the above examples. In both of these examples the field k will be $\mathbb{F}_2^{2t}$ for some t so that $c = |k^*| = 2^{2t} - 1$. 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'. (At the beginning of Section 6, 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

Author's personal copy

$$k_Q = 2t\big(k + k' - n\big) \geqslant 2t\big((14/60)c^2 - (434/60)c\big),$$
$$d_Q = \min\big(d, 3/2d'\big) \geqslant c^2/2 + (1/6)c + 2. \tag{1.0.1}$$

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

$$k_Q = 2t\big(k + k' - n\big) \geqslant 2t\big((10/24)c^2 - (271/30)c\big),$$
$$d_Q = \min\big(d, 3/2d'\big) \geqslant c^2/2 + (13/12)c + 4. \tag{1.0.2}$$

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 [14], for estimating their parameters using methods of intersection theory. We also quickly review rational differential forms on toric varieties and their residues following [4].

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 $\mathcal{L}_{P_i} \otimes_{\mathcal{O}_{X,P_i}} k(P_i) \cong k$ 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

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

It is customary to assume the map α is *injective* and this will be important in computing the parameters of the code. In case $\mathcal{L} = \mathcal{O}_X(E) =$ the line bundle associated to the divisor E, and the given points $P_1, P_2, \ldots, P_M$ are not contained in 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. 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. Now $\Gamma(X, \mathcal{L}) = \{f \in K(X) \mid (f) + E \geqslant 0, \text{ or } f = 0\}$ where $K(X)$ is the function field of X.

3. By replacing E by an appropriately selected linearly equivalent divisor, one may ensure that none of the points $\{P_i \mid i\}$ are contained in the polar part of E; this may require a finite extension of the base field: see [24, p. 134, Theorem 1]. We will henceforth always assume that this hypothesis is satisfied.

Terminology: For the rest of the paper, if $Y \subseteq \mathbb{P}^n$ is a projective variety and f is an element of the homogeneous coordinate ring of Y, we denote by $Z(f)$ the set $\{y \in Y\colon\ f(y) = 0\}$.

Author's personal copy

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

Theorem 2.3. *(See [14, Theorem 5.9].) Suppose X is a smooth and projective variety over k, $d = \dim X \geqslant 2$, 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. Assume there are $\leqslant b$ 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 $G \bullet C_i \geqslant 0$ for all i. Let*

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

where $Z(s)$ is the divisor of zeros of s, s being a section of $\mathcal{L}$.

(i) *Then the code $C(X, \mathcal{L})$ has length M and minimum distance*

$$d \geqslant M - lb - \sum_{i=1}^{n} G \bullet C_i.$$

(ii) *If $G \bullet C_i = \delta \leqslant N$ for all i, then*

$$d \geqslant M - lb - (n - l)\delta.$$

(iii) *In particular, if X is a non-singular surface and H is a* nef *divisor on X with $H \bullet C_i > 0$, then*

$$l \leqslant \frac{D \bullet H}{\min_i\{C_i \bullet H\}}.$$

Thus if $G \bullet H < C_i \bullet H$ for all i, then $l = 0$ and $d \geqslant M - \sum_{i=1}^{n} G \bullet C_i$. Moreover if $d > 0$, then the evaluation map α in Definition 2.1 *is injective.*

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 the treatment in [4] in these.

Let $f_0, \ldots, f_d$ denote homogeneous polynomials of degree n in variables $x_0, \ldots, x_d$ which do not vanish simultaneously on k^{d+1} except at the origin, and let g be a homogeneous polynomial of degree $\rho = (d+1)(n-1)$. Then we consider the d-form

$$\Omega = \sum_{i=0}^{d} (-1)^i x_i\, dx_0 \wedge \cdots \wedge \widehat{dx_i} \wedge \cdots \wedge dx_d. \tag{2.2.1}$$

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 ω_g. The affine open sets

$$U_i = \{x \in \mathcal{P}^d\colon\ f_i(x) \neq 0\}$$

Author's personal copy

clearly form an open cover $\mathcal{U}$ of $\mathbb{P}^d$, and ω_g is regular on $U_0 \cap \cdots \cap U_d$, so it is a Čech co-chain in $C^d(\mathcal{U}, \Omega^n_{\mathbb{P}^d})$. Further, since $\mathcal{U}$ has $d+1$ elements, ω_g is a Čech co-cycle and thus defines a class

$$[\omega_g] \in \check{H}^d\big(\mathcal{U}, \Omega^d_{\mathbb{P}^d}\big) \cong H^d\big(\mathbb{P}^d, \Omega^d_{\mathbb{P}^d}\big).$$

Observe that on the open affine subscheme where $x_0 \neq 0$, the form Ω reduces to $d(\frac{x_1}{x_0}) \wedge \cdots \wedge d(\frac{x_n}{x_0})$ since $\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}$ form a local system of parameters on this subscheme.

We will next consider a d-dimensional projective toric variety X over the fixed field k. X is now determined by a complete fan $\sum$ in $\mathbb{N}_{\mathbb{R}} = \mathbb{R}^d$. As usual, $\mathbb{M}$ will denote the dual lattice of $\mathbb{N} = \mathbb{Z}^d$ (= the lattice of characters of the dense torus T), and $\Sigma(1)$ will denote the set of 1-dimensional cones in Σ. Each $\rho \in \Sigma(1)$ determines a divisor D_ρ on X and a generator $n_\rho \in \mathbb{N} \cap \rho$. (Standard references for toric varieties are [13] 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 coordinates. One takes the polynomial ring S over the base field k in variables x_ρ corresponding to each of the faces ρ of the polytope. Two monomials $\prod_{\rho_i} x_{\rho_i}^{a_i}$ and $\prod_{\rho_i} x_{\rho_i}^{b_i}$ are identified if there exists a character $m \in \mathbb{M}$ so that $a_{\rho_i} = \langle m, n_{\rho_i}\rangle + b_{\rho_i}$ for all ρ_i where n_{ρ_i} is the primitive generator in $\mathbb{N}$ of the half-line $\mathbb{R}_+.\rho_i$. Therefore, the degree of the monomial $\prod_{\rho_i} x_{\rho_i}^{a_i}$ is given by the class of the corresponding divisor $\sum_i a_{\rho_i} D_{\rho_i} \in CH_1(X)$ where D_{ρ_i} is the divisor corresponding to the face ρ_i and $CH_i(X)$ denotes the Chow group of dimension i-cycles modulo rational equivalence.

As explained in [5], X has the homogeneous coordinate ring $S = k[x_\rho]$, which is graded by the Chow group $A_{d-1}(X)$ so that a monomial $\prod_{\rho_i} x_{\rho_i}^{a_{\rho_i}}$ has degree defined above. Given a class $\alpha \in A_{d-1}(X)$, we let S_α denote the graded piece of S in degree α; 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 $I = \{\rho_1, \ldots, \rho_d\} \subset \Sigma(1)$ consisting of d elements, we let

$$\det(n_I) = \det\big(\langle m_i, n_{\rho_j}\rangle_{1 \leqslant i,j \leqslant d}\big).$$

Here n_{ρ_j} denote the primitive vectors in the lattice $\mathbb{M}$ along the rays ρ_j. Also set $dx_I = dx_{\rho_1} \wedge \cdots \wedge dx_{\rho_d}$ and $\hat{x}_I = \prod_{\rho \notin I} x_\rho$. 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 Ω by the formula

$$\Omega = \sum_{|I|=d} \det(n_I)\hat{x}_I\, dx_I \tag{2.2.2}$$

where the sum is over all d-element subsets $I \subset \Sigma(1)$. This form is well defined up to ± 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 $\widehat{\Omega}^d_S = S \cdot \Omega$, where Ω is considered to have degree

$$\beta_0 = \sum_\rho \deg(x_\rho) = \left[\sum_\rho D_\rho\right] \in A_{d-1}(X).$$

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

$$H^0\big(X, \boldsymbol{\omega}_X(Y)\big) = \left\{ g\frac{\Omega}{f} \colon\ g \in S_{\alpha-\beta_0} \right\} \simeq S_{\alpha-\beta_0}.$$

Author's personal copy

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

$$\omega_g = g\frac{\Omega}{f_0 \cdots f_d} \in \boldsymbol{\omega}_X(U_0 \cap \cdots \cap U_d).$$

Here U_i is the complement in X of the zero locus of f_i. Hence $[\omega_g]$ defines a class in the Čech cohomology $\check{H}^d(X, \boldsymbol{\omega}_X) \cong H^d(X, \boldsymbol{\omega}_X)$ for all g. Moreover, if $D_i = Z(f_i)$, then $Z(f_0 \cdots f_d) = \sum_{i=0}^{d} D_i = D$. Therefore, the same ω_g defines an element of $\Gamma(X, \boldsymbol{\omega}_X(D))$: see Definition 3.1 below. The *toric residue* of such an ω_g is defined in [4] to be the image of this element under the trace map $\mathrm{Tr} : H^d(X, \boldsymbol{\omega}_X) \to k$.

2.3. Cartier divisors associated to rational differential forms

Recall a *rational differential form* is a global section of the sheaf $K(X) \otimes_{\mathcal{O}_X} \boldsymbol{\omega}_X$. Choosing a local trivialization of $\boldsymbol{\omega}_X$ by the open cover $\{U_i \mid i\}$ of X with transition functions given by $g_{i,j} \in \Gamma(U_i \cap U_j, \mathcal{O}_X^*)$, this means a rational differential form on X is given by a collection $\{(V_i, f_i) \mid f_i \in K(V_i), i\}$, where $\{V_i \mid i\}$ is an open cover of X possibly refining $\{U_i \mid i\}$ so that on $U_i \cap U_j$, $f_i = g_{i,j}.f_j$. See [20]. 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 ω is a rational differential form, (ω) will denote the associated Cartier divisor.

By taking the covering $\{V_i \mid i\}$ to be also a refinement of the affine open cover defined by the fan, one may see that ω_g above is a rational differential form, and that conversely any rational differential form may be expressed as ω_g 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 [5]: see especially [5, Lemma 2.2].)

Definition 2.4. In particular we let $\omega_{can} = \frac{\Omega}{\prod_{\rho \in \Sigma(1)} x_\rho}$. The associated Cartier divisor is clearly the *canonical divisor* $K = -\sum_{\rho \in \Sigma(1)} D_\rho$.

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 $c = |k^*|$. Assume that $\{D_i \mid i = 1, \ldots, d\}$ are d effective divisors whose intersection of supports contains the discrete set of k-rational points $\mathcal{P} = \{P_i \mid i = 1, \ldots, m\}$. If E is a divisor and $\mathcal{L} \cong \mathcal{O}(E)$ is the associated line bundle, $\boldsymbol{\omega}_X(E)$ will denote $\boldsymbol{\omega}_X \otimes \mathcal{L}$. Now

$$\Gamma\big(X, \boldsymbol{\omega}_X(E)\big) = \big\{\omega \in \Gamma\big(X, K(X) \otimes_{\mathcal{O}_X} \boldsymbol{\omega}_X\big) \;\big|\; (\omega) + E \geqslant 0, \text{ or } \omega = 0\big\}. \tag{3.1.1}$$

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 ω to $(Res_{P_1}(\omega), \ldots, Res_{P_m}(\omega))$. Here $Res_{P_i}(\omega)$ denotes the local Grothendieck residue of ω at P_i. We will assume throughout the paper that this map is *injective* and the parameters of the code will be computed under this assumption. *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 $\{P_i \mid i = 1, \ldots, m\}$ of rational points are all in the dense orbit and all their coordinates are nonzero. We begin with the following observation (see [8, (0.4)]) on residues of rational functions on an n-dimensional split torus:

Author's personal copy

Proposition 3.2. *Let $g_1, \ldots, g_d, h \in k[t_1, \ldots, t_d]$ so that the following holds. Let $u < |k^*|$. 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 $\mathbf{f} = (f_1, \ldots, f_d) \in (k^*)^d$ 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 two following ways*:

(i) $g_i(t_1, \ldots, t_d) = \prod_{j=1}^{u}(t_i - a_i(j))$;
(ii) $g_i(t_1, \ldots, t_d) = \prod_{j=1}^{u}(t_i - a_i(j)) \prod_{j \neq i}(t_j - f_j)$.

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 $J(g_1, \ldots, g_d)(P) \neq 0$, where P denotes any of the above points. Therefore, the local residue of the form $\omega_0 = \frac{h dt_1 \wedge \cdots \wedge dt_d}{g_1 \cdots g_d}$ at each of the above points P is given by $\frac{h(P)}{J(g_1, \ldots, g_d)(P)}$. In particular this is nonzero 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 ω_0 is 1. The differential form $\omega_0 = \frac{J(g_1, \ldots, g_d) t_1 \cdots t_d \, dt_1 \wedge \cdots \wedge dt_d}{g_1 \cdots g_d . t_1 \cdots t_d}$ may be homogenized by substituting everywhere for the variables t_i in terms of the homogeneous coordinates $x_1, \ldots, x_N$ and by observing that the form $\frac{dt_1 \wedge \cdots \wedge dt_d}{t_1 \cdots t_d}$ homogenizes to $\frac{\Omega}{x_1 \cdots x_N}$. Here $N = |\Delta(1)| =$ the number of 1-dimensional rays in the fan Δ. (See [7, Theorem 4].) (Observe that the multi-degree in $(t_1, \ldots, t_d)$ of $J(g_1, \ldots, g_d) t_1 \cdots t_d = \deg(g_1 . \cdots g_d)$.) Thus the above form ω_0 defines a global rational differential form, which we denote by $\overline{\omega}_0$. Clearly ω_{can} is also a global rational differential form and $\overline{\omega}_0 = g\omega_{can}$ where g is the rational function obtained by homogenizing $\frac{J(g_1, \ldots, g_d) t_1 \cdots t_d}{g_1 \cdots g_d}$. It follows that the divisors associated to the form ω_{can} and $\overline{\omega}_0$ are linearly equivalent. The latter restricts to ω_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 $Res_P(\omega_{can}) = 1$ for any of the u^d rational points P chosen above. However, the two forms $\bar{\omega}_0$ and ω_{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 $\omega_X(D + \mathrm{div}(g)) \cong \mathcal{O}_X(D + K + \mathrm{div}(g))$. This observation will be used in working with the polytopes for the examples considered in Section 5. The divisor $K + \mathrm{div}(g)$ will be denoted K' henceforth.

For any divisor F on X, recall the definitions

$$\Gamma\big(X, \mathcal{O}_X(F)\big) = \big\{ f \in K(X) \;\big|\; \mathrm{div}(f) + F \geqslant 0, \text{ or } f = 0 \big\} \quad \text{and}$$
$$\Gamma\big(X, \boldsymbol{\omega}_X(F)\big) = \big\{ \omega \in \Gamma\big(X, K(X) \otimes \boldsymbol{\omega}_X\big) \;\big|\; (\omega) + F \geqslant 0, \text{ or } \omega = 0 \big\}.$$

Proposition 3.4. *Multiplication by the differential form $\bar{\omega}_0$ induces an isomorphism $\Gamma(X, \mathcal{O}_X(F + K')) \to \Gamma(X, \boldsymbol{\omega}_X(F))$. Moreover, if $F = D - E$ (where $D = \mathrm{div}(g)_\infty$) for some effective divisor E and $f \in \Gamma(X, \mathcal{O}_X(F + K'))$, $Res_{P_i}(f . \bar{\omega}_0) = f(P_i)$, $i = 1, \ldots, m$.*

Proof. Let $f \in \Gamma(X, \mathcal{O}_X(F + K'))$. Then $\mathrm{div}(f) + K' + F \geqslant 0$. But K' is the Cartier divisor associated to $\bar{\omega}_0$, so that $(f . \bar{\omega}_0) + F = \mathrm{div}(f) + (\bar{\omega}_0) + F \geqslant 0$. It follows that multiplication by $\bar{\omega}_0$ sends $f \in \Gamma(X, \mathcal{O}_X(F + K'))$ to $f\bar{\omega}_0 \in \Gamma(X, \omega_X(F))$. 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

$$\mathrm{div}(f)_0 - \mathrm{div}(f)_\infty + D - E + K + \mathrm{div}(g)_0 - \mathrm{div}(g)_\infty = \mathrm{div}(f)_0 - E + K + \mathrm{div}(g)_0 - \mathrm{div}(f)_\infty$$

since $D = \mathrm{div}(g)_\infty$. Therefore, the hypothesis that $\mathrm{div}(f) + D - E + K' \geqslant 0$ implies that $\mathrm{div}(f)_\infty$ is contained in $\mathrm{div}(g)_0$ which is disjoint from the points $\{P_i \mid i = 1, \ldots, m\}$. Therefore, $Res_P(f\bar{\omega}_0) =$

Author's personal copy

$f(P).Res_P(\bar{\omega}_0) = f(P)$ since $Res_P(\bar{\omega}_0) = 1$ for all the chosen points P. This proves the second assertion. □

The proposition above shows that the residue $Res_P(f\bar{\omega}_0) = 0$ 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 $d = \dim X \geqslant 2$. $C_1, C_2, \ldots, C_n$ are irreducible curves on X with k-rational points $P_1, P_2, \ldots, P_m$ 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 at most b points on each C_i, these points are all contained in the dense orbit, and have all coordinates different from zero. For each $i = 1, \ldots, d$, let D_i denote the divisor defined by the closure of*

$$Z\big(g_i(t_1, \ldots, t_d)\big) = \big\{(x_1, \ldots, x_d) \in \mathbb{G}_m^d \;\big|\; g_i(x_1, \ldots, x_d) = 0\big\}.$$

(*Note that $\bigcap_{i=1}^{d} |D_i|$ clearly contains the rational points $\mathcal{P} = \{P_1, \ldots, P_m\}$.*)

Assume the following hypotheses as well:

(i) *Let F be a divisor on X and let $F' = F + K'$, where $K' = K + \operatorname{div}(g)$ is the divisor considered above in Proposition* 3.4.

(ii) *Let $Z(s) = \{P \in X \mid s(P) = 0\}$ where $s \in \Gamma(X, \mathcal{O}_X(F'))$, and let*

$$l = \sup_{s \in \Gamma(X, \mathcal{O}_X(F'))} \#\big\{i\colon\ C_i \subseteq Z(s)\big\}.$$

(iii) *Assume $F' \bullet C_i \geqslant 0$ for all $i = 1, \ldots, m$.*

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

$$d \geqslant m - lb - \sum_{i=1}^{m} F' \bullet C_i.$$

If $F' \bullet C_i = \delta \leqslant N$ for all i, then

$$d \geqslant m - lb - (n - l)\delta.$$

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

$$l \leqslant \frac{F' \bullet H}{\min_i\{C_i \bullet H\}}.$$

Thus if $F' \bullet H < C_i \bullet H$ for all i, then $l = 0$ and $d \geqslant m - \sum_{i=1}^{n} F' \bullet C_i$. Moreover if $d > 0$ the residue map $\Gamma(X, \boldsymbol{\omega}_X(E)) \to k^m$ in Definition 3.1 *is injective.*

Proof. The proof reduces to the original form of Hansen's theorem quoted above if one makes use of the equality that $Res_{P_i}(s.\bar{\omega}_0) = s(P_i)$ at all the points P_i, $i = 1, \ldots, m$ proved in the last proposition. □

Author's personal copy

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 [15]. 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 coordinate 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 $\mathrm{div}(t_i - a)$ 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 $|J_i'| \geqslant |k^*|/2$. In the case $D_{i,a}$ is ample for each i and any $a \in k^*$, we let

$$D_1 = \sum_{a \in k^* | a \neq f_1} D_{1,a} + \sum_{j=2}^{d} D_{j,f_j}, \quad \text{where } f_1 = 1 \quad \text{and}$$
$$D_i = \sum_{a \in k^* | a \neq f_i} D_{i,a}, \quad i = 2, \ldots, d. \tag{3.3.1}$$

(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* with $c = |k^*|$, whereas the intersection $\bigcap_{i=1}^d |D_i|$ has more points. This intersection always contains the point $\mathbf{f} = (f_1, \ldots, f_d)$ when D_i is defined by (3.3.2).

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

$$D_{i,a} \bullet V(\rho) \geqslant 0, \quad i = 1, \ldots, d,$$
$$\left(\sum_{i=1}^{d} D_{i,a} \right) \bullet V(\rho) > 0 \quad \text{and}$$
$$\bigcap_{i=1}^{d} |D_i| \quad \text{is finite} \tag{3.3.3}$$

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

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 nonempty subvariety. Therefore, the set of points on the union of these divisors lying outside the dense orbit is finite.

Author's personal copy

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 $D_i = \sum_{a\in k^*|a\neq f_i} D_{i,a}$. 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,

$$D_i \bullet V(\rho) = D_{J_i'} \bullet V(\rho) + \sum_{j\neq i} D_{j,f_j} \bullet V(\rho)$$

$$= \left|J_i'\right| D_{i,a} \bullet V(\rho) + \sum_{j\neq i} D_{j,a} \bullet V(\rho) = \left(\sum_i D_{i,a}\right) \bullet V(\rho) + \left(\left|J_i'\right| - 1\right) D_{i,a} \bullet V(\rho)$$

where $a \in k^*$ is any point. Since $(\sum_i D_{i,a}) \bullet V(\rho) > 0$ by our hypothesis (3.3.3), it follows that $D_i \bullet V(\rho) > 0$ 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} = the closure of $Z(t_i - a_i)$ in X, where t_i denotes the i-th coordinate on the torus $T = \mathbb{G}_m^d$. On homogenizing, this divisor becomes $Z(x_i - a_i\phi_i)$ where ϕ_i are chosen as in 3.4(4) below. Multiplying by the rational function $\frac{x_i}{(x_i - a_i\phi_i)}$, 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. The hypotheses in (3.3.3) are merely convenient hypotheses that will ensure ampleness of the divisors D_i as proved above. Moreover, these hypotheses seem to be verified in the examples of surfaces considered in Section 5 and also several higher dimensional examples.

We let D' denote the divisor $\sum_{i=1}^n D_i'$ and D denote the divisor $\sum_{i=1}^n D_i$. We let

$$\mathcal{P} = \{P_i \mid i = 1, \ldots, m\} \tag{3.3.4}$$

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 on the shape of the corresponding polytope, while* (4) *is a condition on the Euler form and* (5), (6) *are conditions on the line bundle.*

(0) Given an n-dimensional toric variety defined over a field k, by taking a finite extension of the field, we may assume all the orbits are in fact split tori. Therefore, we will assume, without loss of generality that for all toric varieties that we consider all the orbits are in fact split tori. The divisor of zeros of a homogeneous polynomial p (i.e. an element of the homogeneous coordinate ring of the toric variety: see [5]) will be denoted $Z(p)$.

(1) The cardinality of k^* is denoted c. (Observe that, if $k = \mathbb{F}_{p^s}$ for some prime p and $s \geqslant 1$, then $c = p^s - 1$.)

Author's personal copy

(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 $P \subseteq \mathbb{M}_{\mathbb{R}}$. Let $\Sigma(1) = \{\rho_i \mid i = 1, \ldots, N\}$ denote the 1-dimensional cones in the fan, and let $\{x_i \mid i = 1, \ldots, N\}$ denote the corresponding variables in the associated homogeneous coordinate ring of X. *We will often denote the divisor $Z(x_i)$ by B_i.*

(3) We will assume that $d = \dim_k X = \dim_{\mathbb{R}}(\mathbb{M}_{\mathbb{R}})$. We will also assume that d faces of the polytope P *lie* on the coordinate 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 coordinates on the dense torus $T = \mathbb{G}_m^d$. On homogenizing the differential form

$$\frac{dt_1 \wedge \cdots \wedge dt_d}{\prod_{j=1}^{n_1-1}(t_1 - b_1(j)) \cdots \prod_{j=1}^{n_d-1}(t_d - b_d(j))}$$

using the technique in [7, Theorem 4] in terms of the variables $x_1, \ldots, x_N$, we obtain a differential form of the form

$$\frac{\Omega}{\prod_{j=1}^{n_1-1}(x_1 - b_1(j)\phi_1) \cdots \prod_{j=1}^{n_d-1}(x_d - b_d(j)\phi_d) x_{d+1}^{r_{n+1}} \cdots x_N^{r_N}}.$$

Here each $b_i(j) \in k^*$. ϕ_i is a product of non-negative powers of the variables $x_{d+1}, \ldots, x_N$ and each $r_i \in \mathbb{Z}$. We also require that the weight of $x_i =$ the weight of ϕ_i. In particular, this means, on the dense orbit, the coordinates $(t_1, \ldots, t_d)$ are given by $t_i = x_i/\phi_i$, $i = 1, \ldots, d$. Moreover, this involves calculating the dt_i using the quotient rule: we are assuming implicitly that the characteristic of the field is such that the above differential form in homogeneous coordinates is not identically zero.

(5) We will also assume that the given line bundle $\mathcal{L} = \mathcal{O}_X(E)$, where

$$E = e_{d+1}\big(Z(x_{d+1} - h_{d+1}\psi_{d+1})\big) + \cdots + e_N\big(Z(x_N - h_N\psi_N)\big)$$

with the variables (i.e. faces) $x_{d+1}, \ldots, x_N$ *distinct* from the variables x_i, $i = 1, \ldots, d$, and where ψ_j is a polynomial in the variables different from x_j with weight of $\psi_j =$ the weight of x_j. Moreover, $h_i \in k$ are chosen so that the intersection $|E| \cap (\bigcap_{i=1}^d |D_i|)$ is empty. We also require $e_i > 0$ for all i and that $\sum_{i=d+1}^N e_i \geqslant d$.

(6) In addition, we require that there exists a section $s_0 \in \Gamma(X, \mathcal{L})$ of the following form:
(a) If the divisors D_i are chosen as in (3.3.1), we require this to be given by

$$\frac{(x_2 - f_2\phi_2)^{g_2} \cdots (x_d - f_d\phi_d)^{g_d}}{(x_{d+1} - h_{d+1}\psi_{d+1})^{e_{d+1}} \cdots (x_N - h_N\psi_N)^{e_N}}.$$

(b) If the divisors D_i are chosen as in (3.3.2), we require this to be given by

$$\frac{(x_1 - f_1\phi_1)^{g_1} \cdots (x_d - f_d\phi_d)^{g_d}}{(x_{d+1} - h_{d+1}\psi_{d+1})^{e_{d+1}} \cdots (x_N - h_N\psi_N)^{e_N}},$$

where the f_i are chosen as in 3.3 and the g_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 coordinates different from f_i, $i = 1, \ldots, d$.

(7) A generic point on the 1-dimensional rays ρ_i, for $i = d+1, \ldots, N$ belongs to the region of $\mathbb{N}_{\mathbb{R}} \cong \mathbb{R}^d$ with all the coordinates $x_1, \ldots, x_d$, *non-positive*.

From the examples worked out in Section 5, one may see that these hypotheses are in fact satisfied in many cases. Observe also that since $\{P_i \mid i = 1, \ldots, M\} \subseteq \bigcap_{i=1}^d |D_i|$, $|E| \cap \{P_i \mid i = 1, \ldots, M\}$ is *empty*,

Author's personal copy

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 = the closure of $Z(g_i)$ in X, $i = 1, \ldots, d$, and the divisors D_i, $i = 1, \ldots, d$, have as intersection the same finite set of points $\{P\} = \bigcap_{j=1}^d Z(g_i)$. In particular, X may be chosen 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 attempt to produce more examples of such varieties by blowing up along smooth toric subvarieties contained in the complement of the dense open orbit.

Proposition 3.11. *Let $\pi : \widetilde{X} \to X$ denote the blow up of a projective smooth d-dimensional toric variety over k along some closed T-stable subvariety, where T is the dense torus in X. Let D_i, $i = 1, \ldots, d$, denote the closure of $Z(g_i)$ in X, where the g_i are defined as in Proposition* 3.2. *Let $\widetilde{D}_i$ denote the closure of $Z(\pi^*(g_i))$ in $\widetilde{X}$. If the intersection $\bigcap_{i=1}^d |D_i|$ is contained in T, so is the intersection $\bigcap_{i=1}^d |\widetilde{D}_i|$.*

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 π is the dense torus in $\widetilde{X}$. □

4. Duality results and estimation of parameters

4.1. Duality results

The following theorem is well known over the complex numbers even when the divisors are not ample. (See [12,6].) 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 Theorem 4.3.

Theorem 4.1. *Let X denote a smooth projective toric variety defined over a field k. Let $d = \dim_k(X)$. Let $D_1, \ldots, D_d$ denote n effective ample Cartier divisors whose intersection is a finite set of k-rational points. Let ω denote a differential form in $\Gamma(X, \boldsymbol{\omega}_X(D_1 + \cdots + D_n))$, i.e. ω has poles contained in $\sum_{i=1}^d D_i$. Then*

$$\sum_{x \in \bigcap_{i=1}^d |D_i|} Res_x(\omega) = 0$$

where $Res_x(\omega)$ denotes the local residue of the differential form ω at x.

Author's personal copy

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 $x_1, \ldots, x_d, x_{d+1}$ are the homogeneous coordinates on $\mathbb{P}^d$.

For each $i = 1, \ldots, d$ let d_i denote a *positive* integer $\leqslant c$ and let $B_i = \sum_{j=1}^{d_i} Z(x_i - a_i(j)x_{d+1})$. Let $\{R_\ell \mid \ell\}$ denote all the k-rational points that lie in the intersection of the supports of all B_i, $i = 1, \ldots, d$.

Lemma 4.2. *(See [27, pp. 36–37].) Let $R_1 = (R_{1,1}, \ldots, R_{1,d})$, $R_2 = (R_{2,1}, \ldots, R_{2,d})$ denote two arbitrarily chosen distinct points from the set $\{R_\ell \mid \ell\}$ above. Then there exists a differential form $\eta_{1,2} \in \Gamma(X, \omega(\sum_i B_i))$ so that $Res_{R_1}(\eta_{1,2}) = 1$, $Res_{R_2}(\eta_{1,2}) = -1$, and $Res_{R_\ell}(\eta_{1,2}) = 0$ for all $\ell \neq 1, 2$.*

Proof. We let

$$\eta_{1,2} = \left(\frac{1}{(x_1/x_{d+1} - R_{1,1}) \cdots (x_d/x_{d+1} - R_{1,d})} - \frac{1}{(x_1/x_{d+1} - R_{2,1}) \cdots (x_d/x_{d+1} - R_{2,d})} \right) d(x_1/x_{d+1}) \wedge \cdots \wedge d(x_d/x_{d+1}).$$

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 Ω/x_{d+1}^{d+1}. Next the term $\frac{1}{(x_1/x_{d+1} - R_{1,1}) \cdots (x_d/x_{d+1} - R_{1,d})}$ simplifies to $\frac{x_{d+1}^d}{(x_1 - R_{1,1}x_{d+1}) \cdots (x_d - R_{1,d}x_{d+1})}$ and the term $\frac{1}{(x_1/x_{d+1} - R_{2,1}) \cdots (x_d/x_{d+1} - R_{2,d})}$ simplifies to $\frac{x_{d+1}^d}{(x_1 - R_{2,1}x_{d+1}) \cdots (x_d - R_{2,d}x_{d+1})}$.

Now a key point here is the following: the terms in the numerator that do not contain x_{d+1}^{d+1} as a factor will cancel out when the difference

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

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}^{d+1} as a factor, and this will cancel with the x_{d+1}^{d+1} in the denominator of Ω/x_{d+1}^{d+1}. Therefore, $\eta_{1,2}$ is identified with the form:

$$\frac{\Omega g}{(x_1 - R_{1,1}x_{d+1})(x_1 - R_{2,1}x_{d+1}) \cdots (x_d - R_{1,d}x_{d+1})(x_d - R_{2,d}x_{d+1})} \tag{4.1.1}$$

where g is some homogeneous polynomial in the variables $x_1, \ldots, x_d, x_{d+1}$. 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_1 and R_2 and observe these are 1 and -1, respectively. The residues at the other points R_ℓ, $\ell \neq 1, 2$ 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, $i = 1, \ldots, d$ is a set of effective ample divisors on X and $\bigcap_{i=1}^d |D_i| = \{R_\ell \mid \ell = 1, \ldots, M\}$ where each R_ℓ is a k-rational point of X. Assume that for each point R_ℓ, one is given $v_\ell(R_\ell) \in k^*$ so that the sum $\sum_\ell v_\ell(R_\ell) = 0$. Then there exists a differential form $\eta \in \Gamma(X, \omega_X(\sum_i D_i))$ so that $Res_{R_\ell}(\eta) = v_\ell(R_\ell)$.*

Proof. A corresponding result is proven for the special case when $X = \mathbb{P}^d$ in [27, 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. Recall M denotes the total number of the given rational

Author's personal copy

points $\{R_\ell \mid \ell\}$. For each pair of points R_{i_1}, R_{i_2} among the given rational points, let η_{i_1,i_2} denote the differential form constructed in the last lemma. We show there exists a rational linear combination of these differential forms, $\eta = \sum_{i_1,i_2} x_{i_1,i_2}\eta_{i_1,i_2}$ satisfying the required properties. Here the x_{i_1,i_2} are the variables and there are altogether $N = \binom{M}{2} = \frac{M(M-1)}{2}$ such variables. Taking the residues of the form η at the given points $\{R_\ell \mid \ell\}$ provides us with the following system of M-linear equations in the above variables:

$$\begin{aligned}
&\sum_{i_1,i_2} Res_{R_1}(\eta_{i_1,i_2})x_{i_1,i_2} = v_1(R_1)\\
&\qquad\vdots\\
&\sum_{i_1,i_2} Res_{R_m}(\eta_{i_1,i_2})x_{i_1,i_2} = v_M(R_M).
\end{aligned} \tag{4.1.2}$$

Since each fixed point R_ℓ appears along with every other point R_m as a pair (R_ℓ, R_m), and $Res_{R_\ell}(\eta_{\ell,m}) = 1$, $Res_{R_m}(\eta_{\ell,m}) = -1$, 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 [12, (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 [3, Chapter 1]. (Though they state their results over algebraically closed fields, one may see that the same arguments as in the proof of [3, 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 Appendix A.)

One begins with the observation that, Serre duality provides the isomorphism:

$$H^d(X, \omega_X) \cong k, \qquad H^i\big(X^*, \omega_X\big) = 0, \quad i \geqslant d \tag{4.1.3}$$

where $X^* = X - (\bigcap_i |D_i|) = \bigcup_i (X - |D_i|)$. Therefore, one obtains the exact sequence:

$$H^{d-1}\big(X^*, \omega_X\big) \to H^d_{\bigcap_i |D_i|}(X, \omega_X) \to H^d(X, \omega_X) \cong k \to 0. \tag{4.1.4}$$

By excision, the term $H^d_{\bigcap_i |D_i|}(X, \omega_X)$ is identified with $\bigoplus_{R_i} H^d_{R_i}(X, \omega_X)$. Moreover, the map $H^d_{R_i}(X, \omega_X) \to k$ identifies with taking the residue at the point R_i. The exactness of the sequence in (4.1.4) now shows that if $v_i \in k$, $i = 1, \ldots, M$ are such that $\sum_i v_i = 0$, then there exists a class $\phi \in H^{d-1}(X^*, \omega_X)$ so that if $\bar{\phi}_i$ denotes the image of ϕ in $H^d_{R_i}(X, \omega_X)$, then the local residue of $\bar{\phi}_i$ at R_i equals v_i, $i = 1, \ldots, m$. Therefore, in order to complete the proof of the theorem it suffices to show that there exists a global differential d-form $\Omega \in H^0(X, \omega_X(\sum_{i=1}^d D_i))$ that maps to the class ϕ 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 [3, Chapter 6]), this implies that

$$H^i\big(X, \omega_X(D_{i_1} + \cdots + D_{i_p})\big) = 0, \quad i > 0 \tag{4.1.5}$$

Author's personal copy

for any subset $\{i_1, \ldots, i_p\}$ of p-elements in $1, \ldots, d$. Next we make a complex out of

$$\left\{\omega_X(D_{i_1} + \cdots + D_{i_p}) \;\middle|\; 1 \leqslant i_1, \ldots, i_p \leqslant d\right\}$$

as follows: the term in degree q, $1 \leqslant q \leqslant d$, is given by

$$\bigoplus_{i_j \in S,\, |S|=q} \omega_X(D_{i_1} + \cdots + D_{i_q})$$

where the sum varies over subsets S of $\{1 \leqslant i_1, \ldots, i_q \leqslant d\}$ with cardinality q. The differential

$$\delta : \bigoplus_{i_j \in S,\, |S|=q} \Gamma\big(U, \omega_X(D_{i_1} + \cdots + D_{i_q})\big) \to \bigoplus_{j_k \in T,\, |T|=q+1} \Gamma\big(U, \omega_X(D_{j_1} + \cdots + D_{j_q} + D_{j_{q+1}})\big)$$

is given by $\delta(\alpha_{i_1,\ldots,i_q})_{j_1,\ldots,j_{q+1}} = \sum_{k=1}^{q+1} (-1)^k \alpha_{j_1,\ldots,\hat{j_k},\ldots,j_{q+1}}$ with the form $\alpha_{j_1,\ldots,\hat{j_k},\ldots,j_{q+1}}$ viewed as a form with poles contained in $D_{j_1} + \cdots + D_{j_q} + D_{j_{q+1}}$. Since the above argument already appears in [12, (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 $\omega_X(D_\bullet)$.

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 $\omega_X(D_\bullet)$ provides a resolution of the sheaf $j_*(\omega_{|X^*})$, where $j : X^* \to X$ denotes the obvious open immersion. Let x denote a fixed point of X^*, and let t denote an index $1 \leqslant t \leqslant d$ so that $x \in X - |D_t|$. Let $\alpha \in \bigoplus_{i_j \in S,\, |S|=q} \Gamma(U, \omega_X(D_{i_1} + \cdots + D_{i_q}))$, where $U \subset X - |D_t|$ is an open neighborhood of x. Let $\theta(\alpha) \in \bigoplus_{i_j \in T,\, |T|=q-1} \Gamma(U, \omega_X(D_{i_1} + \cdots + D_{i_{q-1}}))$ be defined by

$$\theta(\alpha)_{l_1,\ldots,l_{q-1}} = \alpha_{t,l_1,\ldots,l_{q-1}}. \tag{4.1.6}$$

Observe that the form $\alpha_{t,l_1,\ldots,l_{q-1}} \in \Gamma(U, \omega_X(D_t + D_{l_1} + \cdots + D_{l_{q-1}})) \cong \Gamma(U, \omega_X(D_{l_1} + \cdots + D_{l_{q-1}}))$ since $U \subseteq X - |D_t|$. Therefore, θ defines a map

$$\theta : \bigoplus_{i_j \in S,\, |S|=q} \Gamma\big(U, \omega_X(D_{i_1} + \cdots + D_{i_q})\big) \to \bigoplus_{i_j \in T,\, |T|=q-1} \Gamma\big(U, \omega_X(D_{i_1} + \cdots + D_{i_{q-1}})\big).$$

Now it suffices to show that $d \circ \theta + \theta \circ d = id$: this is readily checked using the definition of θ. 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 $\Gamma(X, \omega_X(D_\bullet))$ computes the cohomology $H^i(X^*, \omega_X)$. Since the complex $\omega_X(D_\bullet)$ terminates with $\omega(\sum_{i=1}^d D_i)$, it follows that one has a surjection

$$H^0\left(X, \omega_X\left(\sum_{i=1}^d D_i\right)\right) \to H^{d-1}\big(X^*, \omega_X\big) \to 0. \tag{4.1.7}$$

This completes the proof of the theorem. □

Proof of Theorem 4.1. Let ω denote a differential form in $\Gamma(X, \boldsymbol{\omega}_X(D_1 + \cdots + D_d))$, i.e. ω has poles contained in $\sum_{i=1}^d D_i$. As shown above ω defines a class in $H^{d-1}(X^*, \omega_X)$ which maps to $\bigoplus_{P_i} H^d_P(X, \omega_X)$. The latter map is sending ω to $(Res_{P_\ell}(\omega) \mid \ell)$. The proof of the last theorem (see the exact sequence in (4.1.4)), now also shows that the sum $\sum_\ell Res_{P_\ell}(\omega) = 0$. This completes the proof of Theorem 4.1. □

Author's personal copy

Remark 4.4. The statement that global residue is zero for an ω as in Theorem 4.1 will follow from the definition of the residue as a Čech form as in [4], but the statement that the sum of the local residues is also zero does not seem to follow this way. The authors are not aware of any other proof of this statement that holds in all characteristics.

Throughout the remainder of this section, we will assume that the basic hypotheses 3.3 *and* 3.4 *hold.* In particular $\{P_1, \ldots, P_m\}$ will denote the points chosen as in (3.3.4).

4.2. The example of projective spaces

Proposition 4.5. *Assume in addition to the above hypotheses that $N = d + 1$, where N is the number of variables in the homogeneous coordinate ring of X as in* 3.4(2)*, the divisor $E = e_{d+1}Z(x_{d+1} - x_1)$, 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*

$$D_1 = \sum_{a \in k^* | a \neq f_1} D_{1,a} + \sum_{j=2}^{d} D_{j,f_j}, \qquad D_i = \sum_{a \in k^* | a \neq f_i} D_{i,a}, \quad i = 2, \ldots, d.$$

(*This situation occurs in the first example considered in Section* 5.)

Then there exists a section $s \in \Gamma(X, \mathcal{L})$ so that the following conditions are satisfied:

(1) $\operatorname{div}(s)_0 \subseteq |D_{d,f_d}|$,
(2) *s is regular at all the points $\{P_i \mid i = 1, \ldots, m\}$ and*
(3) $\operatorname{div}(s)_\infty = E$.

If $e_{d+1} \geqslant d$, there exists a section $s \in \Gamma(X, \mathcal{L})$ so that instead of (1) *above,* $\operatorname{div}(s)_0 \subseteq |D_{2,f_2} + \cdots + D_{d,f_d}|$.

Proof. It follows readily that each $\phi_i = x_{d+1}$, where ϕ_i is as in 3.4(4). We let $s = \frac{(x_d - f_d x_{d+1})^{e_{d+1}}}{(x_{d+1} - x_1)^{e_{d+1}}}$. In this case it is clear that $s(P_i) \neq 0$ at all the chosen points P_i, $i = 1, \ldots, m$, $\operatorname{div}(s)_0 \subseteq |D_{d,f_d}|$ and that $\operatorname{div}(s)_\infty = E$. Alternatively one may choose $s = \frac{(x_2 - f_2 x_{d+1})^{g_2} \ldots (x_d - f_d x_{d+1})^{g_d}}{(x_{d+1} - x_1)^{e_{d+1}}}$ with $g_i \geqslant 1$ chosen in such a way that $\sum_{i=2}^{d} g_i = e_{d+1}$. In this case one may also verify that the intersection $\bigcap_{i=1}^{d} |D_i|$ has only one point outside the dense orbit which is the point with homogeneous coordinates $[1 : 0 : \ldots : 0]$. This point is not in the support of E. This is discussed in more detail in the first example considered in Section 5, for the case $d = 2$. □

Corollary 4.6. *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* $\operatorname{div}(t)_\infty = 2E$.
(ii) *There exists an $\omega \in \Gamma(X, \omega(\sum_i D_i + 2D_{d,f_d} - 2E))$ so that $Res_{P_i}(\omega) \neq 0$ 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 $\omega' \in \Gamma(X, \omega(\sum_{i=1}^{d} D_i))$ chosen as in the proof of Theorem 4.3 so that $Res_{P_i}(\omega') \neq 0$ for all the points P_i, $i = 1, \ldots, m$. Let t denote a section of $\mathcal{L}$ chosen as in (i). Now we let

$$\omega = \frac{\omega'}{t} = \frac{\omega'}{s^2}. \tag{4.2.1}$$

Author's personal copy

In view of Proposition 4.5 clearly ω belongs to $\Gamma(X, \boldsymbol{\omega}_X(D_1 + \cdots + D_d + 2D_{d,f_d} - 2E))$. Since the support of E is disjoint from the support of $\{P_i \mid i = 1, \ldots, m\}$, t is regular at all points of $\{P_i \mid i\}$. $t(P_i)$ is nonzero by assumption at the points P_i. Therefore, $Res_{P_i}(\omega) = Res_{P_i}(\frac{\omega'}{s^2}) = \frac{Res_{P_i}(\omega')}{s(P_i)^2} \neq 0$ at each P_i, i.e. $Res_{P_i}(\omega) \neq 0$ for each point P_i. □

We will return to the general situation, i.e., where the divisors D_i are chosen as in (3.3.2), for the remainder of this section.

4.3. The modified evaluation and residue codes associated to an effective divisor E

Let $\mathcal{L}$ denote an ample line bundle on X associated to an *effective* divisor E. Now $\mathcal{L} = \mathcal{O}(E)$. Let s denote a *section* of $\mathcal{L}$. We send any such section s to $(s(P_0), s(P_1), \ldots, s(P_m), s(P_m), s(P_{m+1}), \ldots, s(P_M)) \in k^M$. Letting $\mathcal{P} = \{P_1, \ldots, P_m\}$, we define the code $C(X, E, \mathcal{P})$ to be the image in k^M by the evaluation map $s \mapsto (s(P_1), \ldots, s(P_m), \ldots, s(P_M))$, of the k-subspace $\{s \in \Gamma(X, \mathcal{L}) \mid s(P_i) = 0,\ i = m+1, \ldots, M\}$. In view of the fact that the last $M - m$ coordinates are zero, one may view the code $C(X, E, \mathcal{P})$ as a subspace of k^m.

Assume that the divisors D_i, $i = 1, \ldots, d$ are chosen as in (3.3.1). In this case we let $\bar{D}_1 = D_1 + \sum_{i=2}^{d} D_{i,f_i}$, and $\bar{D}_i = D_i$, $i = 2, \ldots, d$. Therefore, the sum $\sum_i D_i + \sum_{i=2}^{d} D_{i,f_i} = \sum_i \bar{D}_i$ and $|\bar{D}_i| = |D_i|$, for each i so that $\bigcap_{i=1}^{d} |\bar{D}_i| = \bigcap_{i=1}^{d} |D_i|$. Consider

$$C(X, \boldsymbol{\omega}_X, E, \mathcal{P}) = \left\{ \alpha \in \Gamma\big(X, K(X) \otimes_{\mathcal{O}_X} \boldsymbol{\omega}_X\big) \;\middle|\; (\alpha) + D + \sum_{i=2}^{d} D_{i,f_i} - E \geqslant 0 \right\},$$

where $\boldsymbol{\omega}_X$ denotes, as before, the sheaf of top-degree differential forms on X. We call this the *modified residue code* in this case.

Assume next that the divisors D_i, $i = 1, \ldots, d$, are chosen as in (3.3.2). Let σ denote a permutation of $1, \ldots, n$ so that $\sigma(i) \neq i$ for all i. Now let $\bar{D}_i = D_i + D_{\sigma(i),f_{\sigma(i)}}$, $i = 1, \ldots, d$. Therefore, $\sum_{i=1}^{d} \bar{D}_i = \sum_{i=1}^{d} D_i + \sum_{i=1}^{d} D_{i,f_i}$ and $|\bar{D}_i| = |D_i|$, for each i so that $\bigcap_{i=1}^{d} |\bar{D}_i| = \bigcap_{i=1}^{d} |D_i|$. In this case we let

$$C(X, \boldsymbol{\omega}_X, E, \mathcal{P}) = \left\{ \alpha \in \Gamma\big(X, K(X) \otimes_{\mathcal{O}_X} \boldsymbol{\omega}_X\big) \;\middle|\; (\alpha) + D + \sum_{i=1}^{d} D_{i,f_i} - E \geqslant 0 \right\},$$

where $\boldsymbol{\omega}_X$ denotes, as before, the sheaf of top-degree differential forms on X. We call this the *modified residue code* in this case.

Definition 4.7. We define $Res : C(X, \omega_X, E, \mathcal{P}) \to k^m \subseteq k^M$ by sending

$$\alpha \in C(X, \omega_X, E, \mathcal{P}) \mapsto \big(Res_{P_1}(\alpha), \ldots, Res_{P_m}(\alpha), 0, \ldots, 0\big).$$

Definition 4.8. Let $w \in (k^*)^m$. For a code $C \subseteq k^m$, we define

$$C_w^{\perp} = \left\{ x \in k^m \;\middle|\; \sum_i w_i x_i y_i = 0 \text{ for any } y \in C \right\}. \tag{4.3.1}$$

In case $w_i = 1$, for all i, we will denote $C_w^{\perp}$ by $C^{\perp}$.

Proposition 4.9. *Assume the above situation. Then Theorem* 4.1 *implies that the image of the code* $C(X, \boldsymbol{\omega}_X, E, \mathcal{P})$ (*defined above*) *under the residue map Res above is contained in* $C(X, E, \mathcal{P})^{\perp}$.

Author's personal copy

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 cases $|\bar{D}_i| = |D_i|$ for all $i = 1, \ldots, d$. Let $f \in C(X, E, \mathcal{P})$. Recall from above that $f(P_i) = 0$, for all $i = m+1, \ldots, M$. If $\alpha \in C(X, \boldsymbol{\omega}_X, E, \mathcal{P})$, then the product $f\alpha$ has poles contained in $\bigcup_{i=1}^n |\bar{D}_i| = \bigcup_{i=1}^n |D_i|$, so that Theorem 4.1 and the observation above show the sum

$$\sum_{p \in \bigcap_{i=1}^n |\bar{D}_i|} Res_p(f\alpha) = \sum_{p \in \bigcap_{i=1}^n |D_i|} Res_p(f\alpha)$$
$$= \sum_{p \in \bigcap_{i=1}^n |D_i|} f(p) Res_p(\alpha) = 0. \tag{4.3.2}$$

In particular, we may replace $Res_{P_i}(\alpha)$ by 0 for all $i = m+1, \ldots, M$. The required conclusion follows. □

Remark 4.10. 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 4.11.

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

$$\sum_j f(p_j) r_j = 0 \quad \textit{for any global section } f \in C(X, E, \mathcal{P}),$$

there exists a differential form $\omega' \in C(X, \boldsymbol{\omega}_X, E, \mathcal{P})$ *so that* $Res_{P_i}(\omega') = r_i$, $i = 1, \ldots, m$. (*The divisor* D_{i,f_i} *is defined in* 3.3.)

(ii) *Therefore, the residue map of Definition* 4.7 *sends* $C(X, \boldsymbol{\omega}_X, E, \mathcal{P})$ *onto* $C(X, E, \mathcal{P})^{\perp}$.

Proof. Consider the sequence $\{r_i s_0(P_i) \mid i = 1, \ldots, m\}$, where s_0 is the chosen section in $\Gamma(X, \mathcal{L})$, chosen as in 3.4(6), i.e. $s_0(P_i) \neq 0$ 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 $\mathrm{div}(s_0) + E \geqslant 0$, where $\mathcal{L} = \mathcal{O}_X(E)$. Since $r_j = 0$ for all $j = m+1, \ldots, M$, clearly the sum $\sum_j r_j s_0(P_j) = 0$, where the sum is taken over all the k-rational points in the intersection $\bigcap_{i=1}^d |D_i|$, so that by Theorem 4.3, there exists a differential form $\omega \in \Gamma(X, \boldsymbol{\omega}_X(\sum_{i=1}^d D_i))$ with $Res_{P_i}(\omega) = r_i s_0(P_i)$, $i = 1, \ldots, M$. 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 $Res_{P_i}(\omega') = Res_{P_i}(\frac{\omega}{s_0}) = \frac{Res_{P_i}(\omega)}{s_0(P_i)} = r_i$, $i = 1, \ldots, m$. The hypotheses on ω and s_0 show that $\omega' \in \Gamma(X, \omega_X(\sum_{i=1}^d D_i + \sum_{i=2}^d D_{i,f_i} - E)) = C(X, \boldsymbol{\omega}_X, E, \mathcal{P})$ in case the divisors D_i are defined as in (3.3.1), and that $\omega' \in \Gamma(X, \boldsymbol{\omega}_X(\sum_{i=1}^d D_i + \sum_{i=1}^d D_{i,f_i} - E)) = C(X, \boldsymbol{\omega}_X, E, \mathcal{P})$ in case the divisors D_i are defined as in (3.3.2). This proves the first statement, and the second is clear. □

Remarks 4.12. 1. Even if the residue map in Definition 4.7 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 $f \in \Gamma(X, \mathcal{L})$ so that $f(P_i) = 0$, 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 coordinates, and assume both the evaluation and residue maps map into k^m.

Author's personal copy

Corollary 4.13. *Under the basic hypotheses as in* 3.4 *and* 3.3 *there exists a differential form*

$$\omega_1 \in C(X, \boldsymbol{\omega}_X, 2E, \mathcal{P})$$

so that $Res_{P_i}(\omega_1) \neq 0$ *at all the chosen rational points* $\{P_i \mid i = 1, \ldots, m\}$.

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

$$\omega_1 \in \Gamma\left(X, \omega\left(\sum_{i=1}^{d} D_i + \sum_{i=1}^{d} D_{i,f_i} - 2E\right)\right). \qquad \square$$

Theorem 4.14. *Let* $w \in k^m$ *be defined by* $w_i = Res_{P_i}(\omega_1)$ *where* ω_1 *is the differential form chosen as in Corollary* 4.13. *Let* $C = C(X, E, \mathcal{P})_w^{\perp}$ *defined as in* (4.3.1). *Then* $C \supseteq C_w^{\perp}$.

If $q = 2^n$, *for some* $n > 0$, *then 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_v *be coordinate-wise multiplication by* $v = (v_1, \ldots, v_n)$. *Then the code* $C' = g_v(C)$ (*which is equivalent to* C) *has the property* $C' \supseteq C'^{\perp}$ *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 $g_1, g_2 \in \Gamma(X, \mathcal{L})$, then

$$\omega.g_1.g_2 \in \Gamma\left(X, \boldsymbol{\omega}\left(D_1 + \cdots + D_d + \sum_{i=1}^{d} D_{i,f_i}\right)\right).$$

Observe that the intersection of the supports of the divisors $\bigcap_{i=1}^{d} |\bar{D}_i| = \bigcap_{i=1}^{d} |D_i| =$ the original set of rational points as in 3.3. Now $D_1 + \cdots + D_d + \sum_{i=1}^{d} D_{i,f_i} = \sum_{i=1}^{d} \bar{D}_i$. 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 $P_{m+1}, \ldots, P_M$,

$$\sum_{i=1}^{M} Res_{P_i}(\omega)\big[g_1(P_i)g_2(P_i)\big] = \sum_{P_i \in \bigcap_{i=1}^{d} |D_i|} Res_{P_i}(\omega)\big[g_1(P_i)g_2(P_i)\big] = \sum_{P_i \in \bigcap_{i=1}^{d} |D_i|} Res_{p_i}(\omega.g_1.g_2) = 0.$$

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

$$\sum_{i=1}^{m} Res_{P_i}(\omega)\big[g_1(P_i)g_2(P_i)\big] = 0. \qquad \square$$

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

Author's personal copy

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 $\{s \in \Gamma(X, \mathcal{L}) \mid s(P_i) = 0,\ i = m+1, \ldots, M\}$. 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:

$$|P| \geqslant \dim\big(C(X, E, \mathcal{P})\big) \geqslant |P| - (M - m). \tag{4.4.1}$$

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

$$\dim(C) \geqslant |\mathcal{P}| - |P| = m - |P|. \tag{4.4.2}$$

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 $cl(Z(t_i - a_i))$ denote the closure of $Z(t_i - a_i)$ in X. Observe that the curves C_i as in Theorem 3.5 that contain the rational points are given by $C_{a_1} = cl(Z(t_1 - a_1(j_1)))$ for $a_i(j) \in k^*$. Clearly there are c possible choices of these points and hence such curves.

Proposition 4.15. *Assume the* 1*-dimensional rays* ρ_i*, for* $i = 3, \ldots, N$ *in the fan of* X*, belong to the region of* $\mathbb{N}_{\mathbb{R}} \cong \mathbb{R}^2$ *with the coordinate* 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* $C \bullet Z(x_i) \geqslant 0$ *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* $C(X, \boldsymbol{\omega}_X, E, \mathcal{P})$*.*

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 $i \geqslant 2$, 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 $i \geqslant 2$, the above intersection numbers are clearly non-negative. Recall also that $Z(x_1) \bullet Z(x_2) = 1$ by the hypotheses in 3.4(3). 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 [5]) we will use the variable x_i 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 ρ' and ρ'' 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 η and a_1 is an integer. Observe that at most one of the two cones ρ' and ρ'' can be the cone x_2. Therefore, the other cone must be one of $x_3, x_4, \ldots, x_N$. At this point, the first hypothesis in the proposition implies that the integer a_1 above must be non-negative. Since the intersection number $Z(x_1) \bullet Z(x_1)$ equals the number a_1 (see [23, p. 80]) 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 by 3.3, the number of rational points $\{P_i\}$ is $m \geqslant (c/2)^2$.

The divisor F (F') in Theorem 3.5 is now given by $D - E = \sum_{i=1}^{2} D_i - E$ ($D - E + K'$, 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_i, $i = 1, 2$ is defined by either (3.3.1) or (3.3.2). In either case, one may see readily that $C \bullet (D - E + K) \geqslant (c/2)(C \bullet (Z(x_1) + C \bullet (Z(x_2)))) - \sum_{i=3}^{N} (e_i + 1)(C \bullet Z(x_i))$. 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 $C \bullet Z(x_i) \geqslant 0$ for $i = 1, 2$ with at least one of them positive. Moreover, $Z(x_1) \bullet Z(x_i) > 0$ for only one of x_i, $i = 3, \ldots, N$. 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. □

Author's personal copy

To complete the determination of the distance of the code $C(X, \boldsymbol{\omega}_X, E, \mathcal{P})$, it suffices to estimate the number l in Theorem 3.5 and the intersection numbers $C_{a_1} \bullet (D - E + K)$. 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 4.16. *Assume the basic hypotheses in* 3.4 *and that X is a toric surface.*

(i) *Let R, S denote two effective divisors on X so that if* $R = \sum_{i=1}^{l} R_i$ *and* $S = \sum_{j=1}^{m} S_j$ *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 *are distinct from the prime divisors* R_j*s. Then* $f \in \Gamma(X, \mathcal{O}_X(S - R - \sum_{j=1}^{p} C_j))$.

(ii) *Let* $F' = D + K'$, *where* $K' = K + \operatorname{div}(g)$, *and where g is the homogenization of the rational function* $\frac{J(g_1,\ldots,g_d)t_1\cdots t_d}{g_1\cdots g_d}$. *Suppose* $f \in \Gamma(X, \mathcal{O}_X(F' - E))$ *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 *in E and the prime divisors in K. Then the rational function* $fg \in \Gamma(X, \mathcal{O}_X(D - \sum_{i=1}^{p} C_i - E + K))$, *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 and on the components of the divisor R, and the curves C_i are all assumed to be distinct from the divisors R_j, $\operatorname{div}(f)_0 = B + \sum_{i=1}^{p} C_i + R$ where B is effective, and $S - \operatorname{div}(f)_\infty \geqslant 0$. Therefore, $\operatorname{div} f - \sum_{j=1}^{p} C_j - R + S = \operatorname{div}(f)_0 - \operatorname{div}(f)_\infty - \sum_{j=1}^{p} C_j - R + S \geqslant B \geqslant 0$. This proves (i).

(ii) Recall from 3.2.1 that the rational function g is the homogenization of $\frac{J(g_1,\ldots,g_d)t_1\cdots t_d}{g_1\cdots g_d}$. Since the g_i are defined as in Proposition 3.2, one may observe that $D = \operatorname{div}(g)_\infty$. Therefore,

$$\begin{aligned}\operatorname{div}(f) + D + K' - E &= \operatorname{div}(f) + D + K + \operatorname{div}(g) - E \\ &= \operatorname{div}(f)_0 - \operatorname{div}(f)_\infty + D - \operatorname{div}(g)_\infty + \operatorname{div}(g)_0 + K - E \\ &= \operatorname{div}(f)_0 + K - E + \operatorname{div}(g)_0 - \operatorname{div}(f)_\infty \geqslant 0.\end{aligned}$$

Since the divisors C_i do not appear as prime divisors in E or K, and since f vanishes identically on C_i, $i = 1, \ldots, p$, it follows that $\operatorname{div}(f)_0 - \sum_{i=1}^{p} C_i + K - E + \operatorname{div}(g)_0 - \operatorname{div}(f)_\infty \geqslant 0$ and $\operatorname{div}(g)_0 \geqslant \operatorname{div}(f)_\infty$. This proves $\operatorname{div}(f)_0 - \operatorname{div}(f)_\infty + \operatorname{div}(g)_0 - \operatorname{div}(g)_\infty - \sum_{i=1}^{p} C_i + D + K - E \geqslant 0$, i.e. $\operatorname{div}(fg) - \sum_{i=1}^{p} C_i + D + K - E \geqslant 0$. □

Remarks 4.17. In [15], a variant of (i) in the last Proposition is used when R is trivial, i.e. $S - R$ 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 R_j so that there is no possible cancellation among these.

The above proposition may clearly be adapted to higher dimensional toric varieties by replacing the irreducible curves C_i by prime divisors.

Lemma 4.18.

(i) *Let* $R = \sum_{j=1}^{l} Z(x_1 - a_1(j)\phi_1)$, $\bar{R} = lZ(x_1)$ *and let S denote any divisor on X. Then the assignment* $f \mapsto f.\frac{x_1^l}{\prod_{j=1}^{l}(x_1 - a_1(j)\phi_j)}$ *defines a bijection* $\Gamma(X, \mathcal{O}_X(S - R)) \to \Gamma(X, \mathcal{O}_X(S - \bar{R}))$.

(ii) *Let* $R = \sum_{j=3}^{N} e_j Z(x_j - h_j\psi_j)$, $\bar{R} = e_3 Z(x_3) + \sum_{j=4}^{N} e_j Z(x_j - h_j\psi_j)$ *and S denote any divisor on X. Then the assignment* $f \mapsto f.\frac{x_3^{e_3}}{(x_3 - h_3\psi_3)^{e_3}}$ *defines a bijection* $\Gamma(X, \mathcal{O}_X(S - R)) \to \Gamma(X, \mathcal{O}_X(S - \bar{R}))$.

Author's personal copy

(iii) *Let* $S = \sum_{j=1}^{m_1} Z(x_1 - a_1(j)\phi_1) + \sum_{j=1}^{m_2} Z(x_2 - a_2(j)\phi_2)$, $\bar{S} = m_1 Z(x_1) + m_2 Z(x_2)$ *and let* R *denote any divisor on* X. *Then the assignment* $f \mapsto f.\frac{\prod_{j=1}^{m_1}(x_1 - a_1(j)\phi_1)\prod_{j=1}^{m_2}(x_2 - a_2(j)\phi_2)}{x_1^{m_1}x_2^{m_2}}$ *defines a bijection* $\Gamma(X, \mathcal{O}_X(S+R)) \to \Gamma(X, \mathcal{O}_X(\bar{S}+R))$.

Proof. (i) If $g = f.\frac{x_1^l}{\prod_{j=1}^{l}(x_1 - a_1(j)\phi_j)}$, then it is clear that $\operatorname{div}(f) = \operatorname{div}(g) - lZ(x_1) + \sum_{j=1}^{l} Z(x_1 - a_1(j)\phi_j)$. Now substituting this into $\operatorname{div}(f) + S - R \geqslant 0$ proves that $\operatorname{div}(g) + S - \bar{R} \geqslant 0$. This proves (i).

(ii) If $g = f.\frac{x_3^{e_3}}{(x_3 - h_3\psi_3)^{e_3}}$, then it is clear that $\operatorname{div}(f) = \operatorname{div}(g) - e_3(Z(x_3)) + e_3 Z(x_3 - h_3\psi_3)$. Now substituting this into $\operatorname{div}(f) + S - R \geqslant 0$ proves $\operatorname{div}(g) + S - \bar{R} \geqslant 0$. This proves (ii), and the proof of (iii) is similar. □

Remark 4.19. In case $\psi_3 = x_1$ and $\phi_1 = x_3$ as occurs in the second and third examples considered in the next section, one may choose $h_3 = 1$. Since we have already assumed h_3 is different from all the $a_1(j)$, this will ensure that the $\{E_i\}$ and $\{F_j\}$ are all distinct as required in Proposition 4.16 above. Clearly this result extends to higher dimensional toric varieties.

5. Examples

In this section we consider several examples of toric surfaces: projective spaces of dimension 2, 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 $\mathcal{P} = \{P_1, \ldots, P_m\}$ will be a collection of k-rational points all chosen as before. The ground field k be an arbitrary finite field unless explicitly stated otherwise. 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 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 $s \in \omega_X(E)$. 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 nonsingular 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* $(D \bullet V(\tau)) > 0$ *for the closed subvariety* $V(\tau)$ *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 $\mathbf{e}_1 = \binom{1}{0}$, $\mathbf{e}_2 = \binom{0}{1}$, and $\mathbf{e}_3 = -\mathbf{e}_1 - \mathbf{e}_2$. The homogeneous coordinate ring has three variables x_i corresponding to each of the $\mathbf{e}_i$ which are divisors. We choose the polytope with vertices given by the vectors $\mathbf{v}_1 = \binom{0}{0}$, $\mathbf{v}_2 = \binom{r}{0}$ and $\mathbf{v}_3 = \binom{0}{r}$ for a fixed *positive integer* r. Now the inward normals to the faces of the above polytope will be the vectors $\mathbf{e}_1$, $\mathbf{e}_2$, and $\mathbf{e}_3 = -\mathbf{e}_1 - \mathbf{e}_2$. This polytope corresponds to the line bundle $\mathcal{O}_{\mathbb{P}_2}(r)$ on $\mathbb{P}_2$ so that $\dim \Gamma(\mathbb{P}_2, \mathcal{L}) =$ the number of lattice points contained in the above polytope including its boundary. Clearly this will work out to be $(r+1)(r+2)/2$. Therefore, the dimension of the resulting code denoted $C(X, E, \mathcal{P})$ above is bounded below by $(r+1)(r+2)/2 - 1$.

We proceed to verify the basic hypotheses in 3.4 and 3.3 are satisfied. We first compute the intersection numbers:

$$Z(x_1) \bullet Z(x_1) = Z(x_2) \bullet Z(x_2) = 1, \qquad Z(x_i) \bullet Z(x_j) = 1 \quad \text{if } i \neq j.$$

Author's personal copy

It follows readily from this computation that the divisor $D_{i,a} = Z(x_i - ax_3)$ is ample for each $i = 1, 2$, and $a \in k^*$. Therefore, the hypotheses in (3.3.3) are satisfied. Observe that $E = rZ(x_3 - x_1)$ (which is linearly equivalent to $\bar{E} = rZ(x_3)$), and that

$$D_1 = \sum_{j=1}^{c-1} Z\big(x_1 - a_1(j)x_3\big) + Z(x_2 - f_2x_3), \qquad D_2 = \sum_{j=1}^{c-1} Z\big(x_2 - a_2(j)x_3\big)$$

where $k^* = \{a_i(j) \mid j = 1, \ldots, c\}$, 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 the only point in $|D_1| \cap |D_2|$ not in the dense orbit is the single point with homogeneous coordinates $[1 : 0 : 0]$, so that $M = m + 1$ in this case. Clearly this point is not in $|E|$.

One may verify readily that the hypotheses in (3.4)(0) through (3), (5), and (7) are satisfied. We let $s_0 = \frac{(x_2 - a_2(c)x_3)^r}{(x_3 - x_1)^r}$: one can verify readily this satisfies 3.4(6). The form

$$\frac{dt_1 \wedge dt_2}{\prod_{j=1}^{n_1-1}(t_1 - a_1(j)).\prod_{j=1}^{n_2-1}(t_2 - a_d(j))}$$

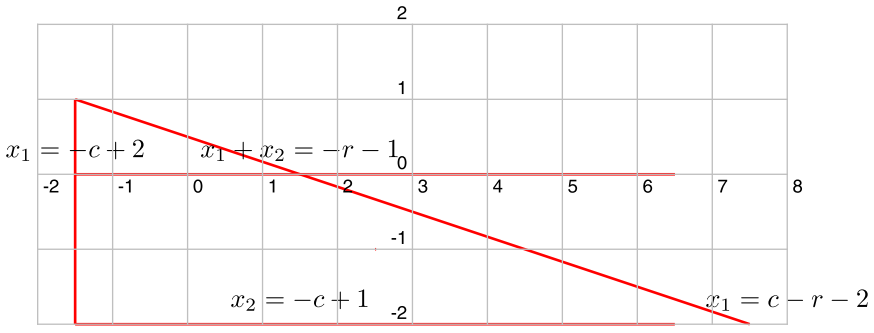
when homogenized becomes

$$\frac{x_3^{n_1+n_2-5}\Omega}{\prod_{j=1}^{n_1-1}(x_1 - a_1(j)x_3).\prod_{j=1}^{n_2-1}(x_2 - a_2(j)x_3)}$$

which shows the hypothesis in 3.4(4) is also satisfied. The same section s_0 provides a section s that satisfies the hypothesis in Proposition 4.5. In this case $\mathrm{div}(s)_0 = D_{2,f_2}$ and $\mathrm{div}(s)_\infty = E$.

Next we let $s = \frac{(x_2 - a_2(c)x_3)^{2r}}{(x_3 - x_1)^{2r}}$. Now $\mathrm{div}(s)_0 = 2D_{2,f_2}$ and $\mathrm{div}(s)_\infty = 2E$. By Corollary 4.6, there exists a differential form $\omega \in \Gamma(X, \omega(D_1 + D_2 + 2D_{2,f_2} - 2E))$. Now it is straightforward to verify that $Res_{P_i}(\omega) \neq 0$ for any point P_i, $i = 1, \ldots, m$. It follows that the above section satisfies the hypotheses in Corollary 4.6.

Next observe that $D = \sum_{j=1}^{c-1} Z(x_1 - a_1(j)x_3) + \sum_{j=1}^{c} Z(x_2 - a_2(j)x_3)$. 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 $h(\mathbf{e}_1) = -(c-2) = -c+2$, $h(\mathbf{e}_2) = -(c-1) = -c+1$, and $h(\mathbf{e}_3) = r+1$. It follows that the corresponding polytope is given by $P = \{m \in \mathbb{M}_{\mathbb{R}} \mid \langle m, \mathbf{e}_1\rangle \geqslant -c+2,\ \langle m, \mathbf{e}_2\rangle \geqslant -c+1,\ \langle m, \mathbf{e}_3\rangle \geqslant r+1\}$. 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.



Recall that there are exactly $(c-1)^2$ rational points P_i at which one takes the residues of the sections $s \in \Gamma(X, \boldsymbol{\omega}_X(D - E))$. Therefore, the length of the code is $(c-1)^2$. The chosen rational points all lie on the curves, $Z(x_1 - a_1(j)x_3)$, $a_1(j) \in k^*$. Next suppose there are l $(0 \leqslant l \leqslant c)$ such divisors so that a *nonzero* rational function $f \in \Gamma(X, \mathcal{O}_X(D + K' - E))$ vanishes identically on these l curves, i.e.

$$\mathrm{div}(f)_0 - Z\big(\big(x_1 - a_1(j)x_3\big)\big) \geqslant 0 \tag{5.0.3}$$

Author's personal copy

for all $j = 1, \ldots, l$. Observe that this is equivalent to $Res_{P_i}(\omega) = 0$ for all k-rational points P_i on these curves, when $\omega = g\omega_{can}$, with $g \in \Gamma(X, \mathcal{O}_X(E))$. First an application of Proposition 4.16(ii) will show that $\Gamma(X, \mathcal{O}_X(D + K - E - \sum_{j=1}^{l} Z(x_1 - a_1(j)x_3))) \neq \{0\}$. Recall that $f_1 = 1$ by our hypotheses, so that all the $a_1(j) \neq 1$ and therefore the hypotheses of this proposition are satisfied.

Now an application of Lemma 4.18(i) with $R = \sum_{j=1}^{l} Z(x_1 - a_1(j)x_3)$, $\bar{R} = lZ(x_1)$, and $S = D + K - E$ will show that $\Gamma(X, \mathcal{O}_X(D + K - E - lZ(x_1))) \neq \{0\}$. Next we apply Lemma 4.18(iii) with $S = D = D_1 + D_2$, $R = K - E - lZ(x_1)$, and $\bar{S} = (c-1)Z(x_1) + cZ(x_2)$ to conclude that

$$\Gamma\big(X, \mathcal{O}_X\big((c-1)Z(x_1) + cZ(x_2) + K - E - lZ(x_1)\big)\big) \neq \{0\}.$$

Another application of Lemma 4.18(ii) with $S = (c-1)Z(x_1) + cZ(x_2) + K - lZ(x_1)$, $R = rZ(x_3 - x_1)$, and $\bar{R} = rZ(x_3)$ will show that $\Gamma(X, \mathcal{O}_X(D + K - \bar{E} - lZ(x_1))) \neq \{0\}$, i.e.

$$\Gamma\big(X, \mathcal{O}_X\big((c-2)Z(x_1) + (c-1)Z(x_2) - (r+1)Z(x_3) - lZ(x_1)\big)\big) \neq \{0\}. \tag{5.0.4}$$

This shows that if f is a section that vanishes on the l lines as in (5.0.3), then there is a global section simultaneously for the line bundle corresponding to the above polytope and also for the line bundle corresponding to the polytope associated to the divisor $(c-2-l)Z(x_1) + (c-1)Z(x_2) - (r+1)Z(x_3)$. The latter is a polytope with the left vertical side on the line $x = -c + 2 + 1$. Therefore, we need $-c + 2 + l \leqslant c - r - 2$ where $(c - r - 2, -c + 1)$ is the right-most vertex of the polytope above. This is equivalent to

$$l \leqslant 2c - r - 4 \leqslant 2c - r. \tag{5.0.5}$$

Next we proceed to compute the intersection numbers $((D + K - E - l.Z(x_1)) \bullet (Z(x_1)))$. As observed above, $D + K - E$ 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 $((D + K - E - l.Z(x_1)) \bullet (Z(x_1)))$ to be $(c-2-1).1 + (c-1) - (r+1)$. It follows that the number of zeroes of f is bounded above by

$$\begin{aligned} l.c + (c - l - 2).1 + (c-1) - (r+1) &\leqslant lc + c - l - 2 + c - r - 2 \\ &= l(c-1) + 2c - r - 4 \leqslant 2c^2 - rc - 4. \end{aligned}$$

Next we will let r and c be such that

$$5/4(c-1) \geqslant r \geqslant 9/8(c-1). \tag{5.0.6}$$

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

$$\begin{aligned} dimension(C) &\geqslant (c-1)^2 - (r+1)(r+2)/2 \geqslant 7/32(c-1)^2 - 15/8(c-1) - 1, \\ distance(C) &\geqslant 1/8c^2 - 25/8c + 5. \end{aligned} \tag{5.0.7}$$

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

$$\lim_{length(C) \to \infty} dimension(C)/length(C) = 7/32.$$

Author's personal copy

Similarly the ratio $distance(C)/length(C)$ is bounded below by $1/8$ and also

$$\lim_{length(C)\to\infty} dimension(C)/length(C) = 1/8.$$

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 $\Gamma(X, \boldsymbol{\omega}_X(D-E))$ explicitly and comparing that with the dimension of the code dual to $\Gamma(X, \mathcal{O}_X(E))$, under the assumption that $k = \mathbb{C}$. 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 $(c-1)B_1 + cB_2 - rB_3$, where $B_i = Z(x_i)$. By Serre duality, one observes that

$$\Gamma\big(X, \boldsymbol{\omega}_X(D-E)\big) \cong H^2\big(X, \mathcal{O}_X(rB_3 - (c-1)B_1 - cB_2)\big)^\vee \cong \bigoplus_{m\in\mathbb{M}} \big(H^2_{Z(h,m)}(\mathbb{N}_\mathbb{R}; \mathbb{C})^\vee\big)\mathbf{e}(m),$$

where $Z(h,m) = \{n \in \mathbb{N}_\mathbb{R} \mid \langle m, n\rangle \geqslant h(n)\}$, and h is the support function associated to the divisor $rB_3 - (c-1)B_1 - cB_2$. (See [23, p. 75].) Therefore, for $H^2_{Z(h,m)}(\mathbb{N}_\mathbb{R}; \mathbb{C})$ to be nontrivial, one needs $Z(h,m) = \{0\}$, and in this case, $H^2_{Z(h,m)}(\mathbb{N}_\mathbb{R}; \mathbb{C}) \cong \mathbb{C}$. Now observe that the support function h associated to the line bundle $\mathcal{O}_X(rB_0 - (c-1)B_1 - cB_2)$ is given by $h(\mathbf{e}_1) = c-1$, $h(\mathbf{e}_2) = c$, and $h(\mathbf{e}_3) = -r$. Therefore, on the cone σ_1 spanned by $\mathbf{e}_1$ and $\mathbf{e}_2$, $h(a\mathbf{e}_1 + b\mathbf{e}_2) = \langle c(\mathbf{e}_1^\vee) + c(\mathbf{e}_2)^\vee, a.\mathbf{e}_1 + b.\mathbf{e}_2\rangle = c(a+b) - a$. Similarly on σ_2 spanned by $\mathbf{e}_2$ and $\mathbf{e}_3$, $h(a\mathbf{e}_2 + b.\mathbf{e}_3) = ac - rb$ and on the cone σ_3 spanned by $\mathbf{e}_3$ and $\mathbf{e}_1$, $h(a\mathbf{e}_3 + b\mathbf{e}_1) = -ar + bc - b$. If $m = x\mathbf{e}_1^\vee + y\mathbf{e}_2^\vee$, one may compute $\langle m, a\mathbf{e}_1 + b\mathbf{e}_2\rangle = ax + by$, $\langle m, a\mathbf{e}_2 + b\mathbf{e}_3\rangle = -b(x+y) + ay$, and $\langle m, a\mathbf{e}_3 + b\mathbf{e}_1\rangle = -a(x+y) + bx$. Therefore, in order that the condition $Z(h,m) = \{0\}$ to hold, we need the three following inequalities to be satisfied for all $a > 0$ or $b > 0$:

$$\begin{aligned} ax + by &< ca + cb - a, \quad \text{in the cone } \sigma_1, \\ ay - b(x+y) &< ac - rb, \quad \text{in the cone } \sigma_2 \quad \text{and} \\ -a(x+y) + bx &< -ra + bc - b, \quad \text{in the cone } \sigma_3. \end{aligned} \tag{5.0.8}$$

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 $\Gamma(X, \boldsymbol{\omega}_X(D-E)) = \frac{(2c-r-1)^2}{2}$. 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 $(c-1)^2 - \frac{(r+1)(r+2)}{2}$. 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 $\Gamma(X, \boldsymbol{\omega}_X(D-E))$, though both are $O(c^2)$. (This also provides independent confirmation that the residue code computed using $\Gamma(X, \boldsymbol{\omega}_X(D-E))$ 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 $\mathbf{u}_1 = \binom{1}{0}$, $\mathbf{u}_2 = \binom{0}{1}$, $\mathbf{u}_3 = \binom{-1}{-1}$, and $\mathbf{u}_4 = \binom{0}{-1}$.

We next consider the polytope with vertices $\mathbf{v}_1 = \binom{0}{0}$, $\mathbf{v}_2 = \binom{r}{0}$, $\mathbf{v}_3 = \binom{r-s}{s}$, and $\mathbf{v}_4 = \binom{0}{s}$. Here $r, s \geqslant 0$, and $r \geqslant s$. As before, each of the four faces of this polytope corresponds to a variable in the homogeneous coordinate ring with x_i corresponding to the ray $\mathbf{u}_i$. The toric variety X is obtained by

Author's personal copy

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 coordinate ring of the toric variety, the variables have the following weights:

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

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

$$\text{weight of } x_4 = \begin{pmatrix} -1 \\ 1 \end{pmatrix}. \tag{5.0.9}$$

Clearly the basic hypotheses in 3.3 are satisfied.

Observe that $h(\mathbf{u}_i) = 0$ for $i = 1, 2$, and $h(\mathbf{u}_3) = \left\langle \binom{r-s}{s}, \binom{-1}{-1} \right\rangle = -r$, $h(\mathbf{u}_4) = \left\langle \binom{0}{s}, \binom{0}{-1} \right\rangle = -s$. Therefore, $\bar{E} = rZ(x_3) + sZ(x_4)$.

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 divisor $\bar{E}$ by the linearly equivalent divisor $rZ(x_3 - x_1) + sZ(x_4)$: henceforth we will denote this divisor by E. 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 $r + s \geqslant 2$. In this case the *irrelevant ideal* is generated by x_3x_4, x_1x_4, x_1x_2, and x_2x_3. Making use of this fact, one may make the following observations: The only points of intersection for two divisors $Z(x_1 - cx_3)$ and $Z(x_2 - dx_3x_4)$, with $c, d \neq 0$ and $c \neq d$ are in the dense orbit. Two divisors $Z(x_1 - cx_3)$ and $Z(x_1 - dx_3)$ for $c \neq d$ *do not intersect*. The only points of intersection for two divisors of the form $Z(x_2 - ax_3x_4)$ and $Z(x_2 - bx_3x_4)$, with $a, b \neq 0$, $a \neq b$ are the points with homogeneous coordinates $x_2 = 0 = x_3$ and $x_1 \neq 0$, $x_4 \neq 0$. 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. The two coordinates on the dense torus will be denoted (t_1, t_2): observe that $t_1 = x_1/x_3$ and $t_2 = x_2/(x_3.x_4)$. In this case we choose the subsets $J_1' = k^* - \{f_1, 1\}$, $f_1 \neq 1$ and $J_2' = k^* - \{f_2\}$, i.e. we need to remove two points $t_1 = f_1$ and $t_1 = 1$ from the t_1-axis. We only remove the point $t_2 = f_2$ from the t_2-axis. Observe as a result, that $m = (c-2)(c-1) = c^2 - 3c + 2$ in this example.

Now one may compute the intersection numbers $Z(x_1) \bullet Z(x_1) = 0$, $Z(x_2) \bullet Z(x_1) = 1$, $Z(x_1) \bullet Z(x_4) = 1$, $Z(x_1) \bullet Z(x_3) = 0$, $Z(x_2) \bullet Z(x_2) = 1$, $Z(x_3) \bullet Z(x_2) = 1$, $Z(x_4) \bullet Z(x_2) = 0$, $Z(x_3) \bullet Z(x_3) = 0$, $Z(x_4) \bullet Z(x_3) = 1$ 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 $|J_1'| = |k^*| - 2$ and $|J_2'| = |k^*| - 1$ in the definition of the divisors D_i, $i = 1, 2$. Denoting by (t_1, t_2) the coordinates on the torus $T = \mathbb{G}_m^2$, and homogenizing using the technique in [7, Theorem 4], one sees that the differential form

$$\frac{dt_1 \wedge dt_2}{\prod_{j=1}^{n_1-1}(t_1 - b_1(j)).\prod_{j=1}^{n_2-1}(t_2 - b_2(j))}$$

transforms to

$$\frac{x_3^{n_1+n_2-5}x_4^{n_2-3}\Omega}{\prod_{j=1}^{n_1-1}(x_1 - b_1(j)x_3)\prod_{j=1}^{n_2-1}(x_2 - b_2(j)x_3x_4)}.$$

Author's personal copy

Moreover, one may verify that x_1 and x_3 have the same weight, and that x_2 and x_3x_4 have the same weight. The weight of $x_3^r x_4^s = \binom{r-s}{s}$ which is also equal to the weight of $(x_1 - a_1x_3)^{r-s}(x_2 - a_2x_3x_4)^s$. These verify the hypothesis (4) in 3.4. Now we may choose

$$s_0 = \frac{(x_1 - f_1x_3)^{r-s}(x_2 - f_2x_3x_4)^s}{(x_3 - x_1)^r x_4^s},$$

where $f_i \in k^*$ and $h_3 \in k^*$ denote the chosen points. Clearly this section does not vanish at any of the points P_i, $i = 1, \ldots, m$ since the coordinates of these points are all different from f_i. Recall also that $r + s \geqslant 2$ by our assumption. Moreover, the arguments in the paragraph above show that indeed the intersection $\bigcap_{i=1}^2 |D_i| \cap |E|$ is empty. We have therefore verified the hypotheses (5) and (6) in 3.4. The hypothesis (7) 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 code 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 by (t_1, t_2) coordinates on this torus. The divisor D will be of the form:

$$\sum_{j=1}^{c-2} cl\big(Z\big(t_1 - a_1(j)\big)\big) + cl\big(Z(t_2 - f_2)\big) + \sum_{j=1}^{c-1} cl\big(Z\big(t_2 - a_2(j)\big)\big) + cl\big(Z(t_1 - f_1)\big). \quad (5.0.10)$$

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:

$$\sum_{j=1}^{c-2} Z\big(x_1 - a_1(j)x_3\big) + Z(x_2 - f_2x_3x_4) + \sum_{j=1}^{c-1} Z\big(x_2 - a_2(j)x_3x_4\big) + Z(x_1 - f_1x_3). \quad (5.0.11)$$

As shown above this is linearly equivalent to

$$(c-1)Z(x_1) + cZ(x_2). \quad (5.0.12)$$

The divisor $D_1 + D_2 + K - E$ 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 $(0 \leqslant l \leqslant c)$ curves $Z(x_1 - a_1(j)x_3)$, $j = 1, \ldots, l$ (with $a_i(j) \in k$) so that a *nonzero* rational function $f \in \Gamma(X, \mathcal{O}_X(D + K' - E))$ vanishes identically on these curves, i.e.

$$\operatorname{div}(f)_0 - Z\big(x_1 - a_1(j)x_3\big) \geqslant 0 \quad (5.0.13)$$

for all $j = 1, \ldots, l$. First an application of Proposition 4.16(ii) shows that

$$\Gamma\left(X, \mathcal{O}_X\left(D + K - E - \sum_{j=1}^{l} Z\big(x_1 - a_1(j)x_3\big)\right)\right) \neq \{0\}.$$

Author's personal copy

(Observe that all the $a_1(j) \neq 1$ so that the hypotheses of this proposition are satisfied.) Now an application of Lemma 4.18(i) with $R = \sum_{j=1}^{l} Z(x_1 - a_1(j)x_3)$, $\bar{R} = lZ(x_1)$ and $S = D + K - E$ will show that

$$\Gamma\big(X, \mathcal{O}_X\big(D + K - E - lZ(x_1)\big)\big) \neq \{0\}.$$

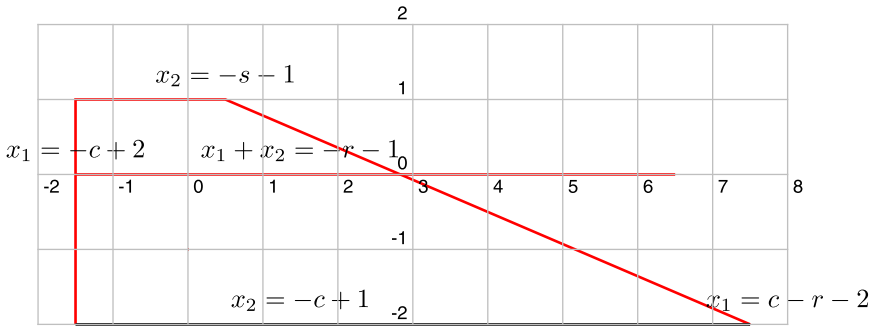
Next we apply Lemma 4.18(iii) with $S = D = D_1 + D_2$, $R = K - E - lZ(x_1)$ and $\bar{S} = (c-1)Z(x_1) + cZ(x_2)$ to conclude that $\Gamma(X, \mathcal{O}_X((c-1)Z(x_1) + cZ(x_2) + K - E - lZ(x_1))) \neq \{0\}$. Another application of Lemma 4.18(ii) with $S = (c-1)Z(x_1) + cZ(x_2) + K - lZ(x_1)$, $R = rZ(x_3 - h_3x_1) + sZ(x_4)$, and $\bar{R} = rZ(x_3) + sZ(x_4)$ shows that

$$\Gamma\big(X, \mathcal{O}_X\big((c-2)Z(x_1) + (c-1)Z(x_2) - (r+1)Z(x_3) - (s+1).Z(x_4) - lZ(x_1)\big)\big) \neq \{0\}. \tag{5.0.14}$$

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 $h(\mathbf{e}_1) = -(c-2) = -c+2$, $h(\mathbf{e}_2) = -(c-1) = -c+1$, $h(\mathbf{e}_3) = r+1$, and $h(\mathbf{e}_4) = s+1$. 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 nonempty as shown by (5.0.14), it follows that $-c+l+2 \leqslant -r-1+c-1$, and hence that

$$l \leqslant 2c - r - 4. \tag{5.0.15}$$

Therefore, the number of k-rational points at which f vanishes is bounded above by

$$lc + c - s - 2 \leqslant 2c^2 - rc - 4c + c - s - 2 \leqslant 2c^2 - rc - 3c - s.$$

Henceforth we keep s, r so that $c/5 > s > c/6$ and $2c > r \geqslant (3/2)c$; then $2c^2 - rc - 3c - s \leqslant (1/2)c^2 - 3c - 1/6c$ and $c^2 - 3c + 2 - (s+1)(r - s/2 + 1) \geqslant (37/60)c^2 - (307/60)c + 1$. Therefore, we may compute the parameters of the code $C = C(X, E, \mathcal{P})^{\perp}$ as:

$$\begin{aligned} \textit{dimension}(C) &\geqslant c^2 - 3c + 2 - (s+1)(r - s/2 + 1) \geqslant (37/60)c^2 - (307/60)c + 1, \\ \textit{distance}(C) &\geqslant c^2 - 3c + 2 - 2c^2 + rc + 3c + s \geqslant c^2/2 + (1/6)c + 2. \end{aligned} \tag{5.0.16}$$

Author's personal copy

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. We begin with $\mathbb{P}_2(1,1,2)$, a weighted projective space of dimension 2 where the weights are $(1,1,2)$. This is a toric variety with one singular point; its fan is given by $\mathbf{e}_1 = \binom{1}{0}$, $\mathbf{e}_2 = \binom{0}{1}$, and $\mathbf{e}_3 = -\mathbf{e}_1 - 2\mathbf{e}_2$. If we resolve the singularity by blowing up the singular point, the resulting nonsingular variety is precisely the Hirzebruch surface F_2, that is, the total space of the $\mathcal{O}_{\mathbb{P}^1}(-2)$-bundle over $\mathbb{P}^1$. This the variety we consider in this example. The fan for $X = F_2$ is the *refined normal fan* consisting of the vectors

$$\mathbf{u}_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad \mathbf{u}_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \qquad \mathbf{u}_3 = \begin{pmatrix} -1 \\ -2 \end{pmatrix} \quad \text{and} \quad \mathbf{u}_4 = \begin{pmatrix} 0 \\ -1 \end{pmatrix}.$$

We consider the polytope with vertices $\mathbf{v}_1 = \binom{0}{0}$, $\mathbf{v}_2 = \binom{2r}{0}$, $\mathbf{v}_3 = \binom{2r-2s}{s}$ and $\mathbf{v}_4 = \binom{0}{s}$. Each of the faces of this polytope corresponds to a variable in the homogeneous coordinate ring of F_2 with x_i corresponding to the ray $\mathbf{u}_i$. 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 $\mathcal{L}$.

Note that $h(\mathbf{u}_i) = 0$ for $i = 1, 2$ and $h(\mathbf{u}_3) = \left\langle \binom{2r-2s}{s}, \binom{-1}{-2} \right\rangle = -2r$, $h(\mathbf{u}_4) = \left\langle \binom{0}{s}, \binom{0}{-1} \right\rangle = -s$. Therefore, the above polytope corresponds to the divisor $2rZ(x_3) + sZ(x_4)$. We will replace this by the linearly equivalent divisor $E = 2rZ(x_3 - x_1) + sZ(x_4)$.

Observe that $CH_1(F_2) = \mathbb{Z} \oplus \mathbb{Z}$. Therefore, one may now compute the weights of the variables x_i as follows:

$$\begin{aligned} \text{weight of } x_1 \text{ and } x_3 &= \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \\ \text{weight of } x_2 &= \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \text{and} \\ \text{weight of } x_4 &= \begin{pmatrix} -2 \\ 1 \end{pmatrix}. \end{aligned} \tag{5.0.17}$$

Now one may compute the intersection numbers

$$Z(x_1) \bullet Z(x_1) = 0, \qquad Z(x_2) \bullet Z(x_1) = 1, \qquad Z(x_1) \bullet Z(x_4) = 1, \qquad Z(x_1) \bullet Z(x_3) = 0,$$
$$Z(x_2) \bullet Z(x_2) = 2, \qquad Z(x_3) \bullet Z(x_2) = 1, \qquad Z(x_4) \bullet Z(x_2) = 0,$$
$$Z(x_3) \bullet Z(x_3) = 0, \qquad Z(x_4) \bullet Z(x_3) = 1, \quad \text{and} \quad Z(x_4) \bullet Z(x_4) = -2.$$

One may show using these computations that the hypothesis in (3.3.3) is satisfied. In this case also we choose the subsets $J_1' = k^* - \{f_1, 1\}$, $f_1 \neq 1$, and $J_2' = k^* - \{f_2\}$, i.e. denoting the coordinates on $\mathbb{G}_m^2$ by (t_1, t_2), with $t_1 = x_1/x_3$ and $t_2 = x_2/(x_3^2 x_4)$, we need to remove two points $t_1 = f_1$ and $t_1 = 1$ from the t_1-axis and the point $t_2 = f_2$ from the t_2-axis. Now $|E| \cap |D_1| \cap |D_2| = \emptyset$ (= the empty set). Moreover, in this case also $m = (c-2)(c-1) = c^2 - 3c + 2$ and $M = m + 1$ as in the last example. Here D_1 (D_2) is given by the sum of the first $(c-1)$-terms in (5.0.18) (the sum of the remaining terms in (5.0.18), respectively). We skip the detailed computation of the intersection $|D_1| \cap |D_2|$ which proceeds as in the last example, since the irrelevant ideal is the same. In view of these, it is clear the basic 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 $r + s \geqslant 2$ so that all the hypotheses (1) through (4) in 3.4

Author's personal copy

are satisfied. Denoting by (t_1, t_2) the coordinates on the torus $T = \mathbb{G}_m^2$, and homogenizing using the technique in [7, Theorem 4], one sees that the differential form

$$\frac{dt_1 \wedge dt_2}{\prod_{j=1}^{n_1-1}(t_1 - b_1(j)) \prod_{j=1}^{n_2-1}(t_2 - b_2(j))}$$

transforms to

$$\frac{x_3^{n_1+2n_2-7} x_4^{n_2-3} \Omega}{\prod_{j=1}^{n_1-1}(x_1 - b_1(j)x_3) \prod_{j=1}^{n_2-1}(x_2 - b_2(j)x_3^2 x_4)}.$$

Moreover, one may verify that x_1 and x_3 have the same weight, and that x_2 and $x_3^2 x_4$ have the same weight. The weight of $x_3^{2r} x_4^s$ is $\binom{2r-2s}{s}$ which is the same as the weight of $(x_1 - a_1 x_3)^{2r-2s}(x_2 - a_2 x_3^2 x_4)^s$. Therefore, we may choose

$$s_0 = \frac{(x_1 - f_1 x_3)^{2r-2s}(x_2 - f_2 x_3^2 x_4)^s}{(x_3 - x_1)^{2r} x_4^s},$$

where $f_i \in k^*$ denotes the chosen point. Clearly this section does not vanish at any of the points P_i, $i = 1, \ldots, m$ since the coordinates of these points are all different from f_i.

We have verified the hypotheses (5) and (6) in 3.4. The hypothesis (7) 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 by (t_1, t_2) coordinates on this torus. The divisor D will be of the form:

$$\sum_{j=1}^{c-2} cl\big(Z\big(t_1 - a_1(j)\big)\big) + cl\big(Z(t_2 - c_1)\big) + \sum_{j=1}^{c-1} cl\big(Z\big(t_2 - a_2(j)\big)\big) + cl\big(Z(t_1 - c_1)\big). \quad (5.0.18)$$

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 $j = 1, \ldots, c$, respectively:

$$\sum_{j=1}^{c-2} Z\big(x_1 - a_1(j)x_3\big) + Z\big(x_2 - c_2 x_3^2 x_4\big) + \sum_{j=1}^{c-1} Z\big(x_2 - a_2(j)x_3^2 x_4\big) + Z(x_1 - c_1 x_3). \quad (5.0.19)$$

As shown above this is linearly equivalent to

$$(c-1)Z(x_1) + cZ(x_2). \quad (5.0.20)$$

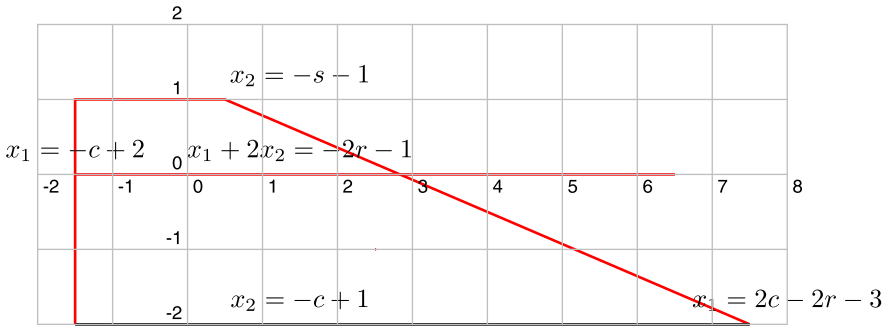
Now $D_1 + D_2 + K - E$ is linearly equivalent to $(c-2)Z(x_1) + (c-1)Z(x_2) - (2r+1)Z(x_3) - (s+1).Z(x_4)$. Then one may compute the intersection number $(D + K' - E) \bullet Z(x_1) = (D + K - E) \bullet Z(x_1)$ to be $c - 1 - (s+1) = c - s - 2$.

Next we proceed to compute the support function associated with the divisor

$$(c-2)Z(x_1) + (c-1)Z(x_2) - (2r+1)Z(x_3) - (s+1)Z(x_4).$$

Author's personal copy

This support function h (see [23, p. 72]) is given by $h(\mathbf{e}_1) = -(c-2) = -c+2$, $h(\mathbf{e}_2) = -(c-1) = -c+1$, $h(\mathbf{e}_3) = 2r+1$, and $h(\mathbf{e}_4) = s+1$. 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 the figure below.



Next suppose there are l $(0 \leqslant l \leqslant c)$ curves $Z(x_1 - a_1(j)x_3)$, $j = 1, \ldots, l$ (with $a_i(j) \in k$) so that a *nonzero* rational function $f \in \Gamma(X, \mathcal{O}_X(D + K' - E))$ vanishes identically on these curves, i.e.

$$\operatorname{div}(f)_0 - Z\big(x_1 - a_1(j)x_3\big) \geqslant 0 \tag{5.0.21}$$

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

$$l \leqslant 3c - 2r - 5. \tag{5.0.22}$$

Therefore, the number of zeroes of f is bounded above by

$$lc + c - s - 2 \leqslant 3c^2 - 2rc - 5c + c - s - 2 = 3c^2 - 2rc - 4c - s - 2.$$

Henceforth we keep s so that $c/10 > s > (1/12)c$ and $(6/4)c > r \geqslant (5/4)c$ so that

$$c^2 - 3c + 2 - 3c^2 + 2rc + 4c + s + 2 \geqslant 1/2c^2 + (13/12)c + 4 \quad \text{and}$$

$$\big(c^2 - 3c + 2\big) - (s+1)(2r - s + 1) \geqslant \big(c^2 - 3c + 2\big) - \left(\frac{c}{10} + 1\right)\left(3c - \frac{c}{12} + 1\right)$$

$$= \frac{17}{24}c^2 - \frac{361}{60}c + 1.$$

Therefore, we may compute the parameters of the code $C = C(X, \mathcal{L}, \mathcal{P})^{\perp}$ as:

$$\begin{aligned} \textit{dimension}(C) &\geqslant (17/24)c^2 - (361/60)c + 1, \\ \textit{distance}(C) &\geqslant c^2 - 3c + 2 - 3c^2 + 2rc + 4c + s + 2 \geqslant c^2/2 + (13/12)c + 4. \end{aligned} \tag{5.0.23}$$

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.

Remark 5.5. One can also apply the same technique to construct similar codes from other Hirzebruch surfaces. For example, for the Hirzebruch surface F_3, we obtain codes with the following parameters:

Author's personal copy

$$\begin{aligned} \textit{dimension}(C) &\geqslant (100/180)c^2 - (584/60)c + 1, \\ \textit{distance}(C) &\geqslant (21/8)c^2 + (37/18)c + 4. \end{aligned} \tag{5.0.24}$$

6. Application I: The 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 [11] 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–Shor–Steane technique as developed in [9,25] and [26].

We will presently provide a brief outline of some of these to make the paper self-contained. We start with a triple $D' \supseteq D \supseteq D^{\perp}$ of *binary codes*, i.e. over the field $\mathbb{F}_2$, where D is an $[n, k, d]$-code containing its dual $D^{\perp}$, and D' is a larger $[n, k']$-code with $k' \geqslant k + 2$. Let G be a generator matrix of D, and let G' be a matrix such that $\binom{G}{G'}$ 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 $C \subseteq \mathbb{F}_2^{2n}$ with the generator matrix $\begin{pmatrix} G & 0 \\ 0 & G \\ G' & G'' \end{pmatrix}$ where the matrix G'' is obtained from G' by permuting its rows so that no row stays in its place. Fix the following $\mathbb{F}_2$-linear isomorphism between $\mathbb{F}_2^{2n}$ and $\mathbb{F}_4^n$ by mapping $(x_1, \ldots, x_n, y_1, \ldots, y_n)$ in $\mathbb{F}_2^{2n}$ to $((x_1, y_1), \ldots, (x_n, y_n))$ in $(\mathbb{F}_2^2)^n$, and then identifying $\mathbb{F}_2^2$ and $\mathbb{F}_4$ by $(0,0) = 0$, $(0,1) = \epsilon$, $(1,0) = \bar{\epsilon}$, $(1,1) = 1$. The image of the code C under this map is $F \subseteq \mathbb{F}_4^n$. Its parameters have been estimated in [2, Section 2]:

$$\begin{aligned} k_F &= k + k' \quad \text{and} \\ d_F &\geqslant \min\bigl(d, d'_2\bigr). \end{aligned} \tag{6.0.25}$$

One defines a symplectic form ω 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 $\mathbb{F}_4^n$ and $\mathbb{F}_2^{2n}$. In the basis of $\mathbb{F}_2^{2n}$ the form ω is defined by the formula $\omega(x, x') = \sum_{j=1}^{n} a_j b'_j + a'_j b_j$. Then it is shown in [2, Section 2] that F contains F^{ω}; the latter is the set of the words in F_4^n orthogonal to all the words in F using the form ω.

The parameters of the corresponding quantum stabilizer codes have been computed in [2, Corollary 1] and they are:

$$k_Q = k + k' - n, \qquad d_Q \geqslant \min\bigl(d, d'_2\bigr) \geqslant \min\left(d, \frac{3d'}{2}\right). \tag{6.0.26}$$

Next one starts with codes C and $C^{\perp}$ over the field $\mathbb{F}_{2^{2t}}$ with $C^{\perp} \subseteq C$. Symbol-wise expansion, i.e. expressing a point of $\mathbb{F}_{2^{2t}}$ with respect to the standard basis of the $\mathbb{F}_2$-vector space $\mathbb{F}_{2^{2t}}$, 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 $n_D = 2tn$, $k_D = 2tk$ and $d_D \geqslant d$.

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 [2, Section 4]. Here a key role is played by the residue theorem for curves (see [17, 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 [17, Chapter III, Theorem 7.14.2]). In the place of this classical residue theorem, we will use the results on toric residues

Author's personal copy

we proved in the last two sections. What is required is a triple $C' \supseteq C \supseteq C^{\perp}$ of codes defined over $\mathbb{F}_{2^t}$ with good parameters.

6.1. Choice of divisors

We will choose two effective divisors E and E' so that $E' \leqslant E$: for example if we choose E as in 3.4(5), then we may let $E' = e'_{d+1}Z(x_{d+1} - h_{d+1}\psi_{d+1}) + \cdots + e'_N Z(x_N - h_N\psi_N)$ where e'_i is a non-negative integer $1 \leqslant e'_i \leqslant e_i$, $i = n+1, \ldots, N$. 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. (In both these cases $c = 2^{2t} - 1$.)

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 $2c > r \geqslant r' > (3/2)c$ and $c/5 > s \geqslant s' > (1/6)c$. Therefore, the parameters of the corresponding quantum stabilizer codes are given by

$$\begin{aligned} k_Q &= 2t.\big(k + k' - n\big) \geqslant 2t\big((37/60)c^2 + (37/60)c^2 - (307/60)c - (307/60)c + 2 - \big(c^2 - 3c + 2\big)\big) \\ &= 2t\big((14/60)c^2 - (434/60)c\big) \quad \text{and} \\ d_Q &= \min\big(d, 3/2d'\big) \geqslant c^2/2 + (1/6)c + 2. \end{aligned} \tag{6.1.1}$$

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

$$\begin{aligned} k_Q &= 2t\big(k + k' - n\big) \geqslant 2t\big((17/24)c^2 + (17/24)c^2 - (361/60)c - (361/60)c + 2 - \big(c^2 - 3c + 2\big)\big) \\ &= 2t\big((10/24)c^2 - (271/30)c\big) \quad \text{and} \\ d_Q &= \min\big(d, 3/2d'\big) \geqslant c^2/2 + (13/12)c + 4. \end{aligned} \tag{6.1.2}$$

Example 6.3. The Hirzebruch surface F_3. In this case the parameters of the corresponding quantum stabilizer codes are given by

$$\begin{aligned} k_Q &= 2t\big(k + k' - n\big) \\ &\geqslant 2t\big((100/180)c^2 + (100/180)c^2 - (584/60)c - (584/60)c + 2 - \big(c^2 - 3c + 2\big)\big) \\ &= 2t\big((20/180)c^2 - (494/30)c\big) \quad \text{and} \\ d_Q &= \min\big(d, 3/2d'\big) \geqslant (21/8)c^2 + (37/18)c + 4. \end{aligned} \tag{6.1.3}$$

Remarks 6.4. 1. Unfortunately, the polytope structure for $\mathbb{P}_2$ seems to be such that no construction of quantum stabilizer codes seems possible using it. Here the main difficulty seems to be the shape of the polytope, which has only three faces: the first formula in (6.0.26) seems to require a bit more flexibility on the polytope so that the parameter k_Q will be positive.

2. The above constructions do not yet yield a *good family of quantum codes*. The difficulty is because $c = 2^{2t} - 1$ in this case, n_Q is essentially the same as $2tc^2$ when t and c are large and because d_Q as above does not involve an extra factor of $2t$. Therefore, while the ratio k_Q/n_Q remains bounded away from 0 as $t \to \infty$, the ratio d_Q/n_Q does go to zero as $t \to \infty$. We plan to pursue these issues in detail elsewhere: see [18] and [19].

Author's personal copy

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 residue codes provides generator matrices for these toric residue codes. Corollary 4.11 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 in [16, Chapter 6]. We plan to explore this idea in more detail in future work.

Acknowledgments

The authors would like to thank David Cox for answering several questions on toric varieties and Michel Brion for pointing out that toric varieties are Frobenius split. They also would like to thank the referee for several helpful comments that have improved the exposition.

Appendix A. 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 [3, 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 ϕ 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 subscheme of X defined by the sheaf of ideals $\mathcal{I}$, ϕ compatibly splits Y if $\phi(F_*(\mathcal{I})) = \mathcal{I}$.

Proposition A.1. *(See [3, 1.3.11 Proposition].) Let X denote a regular and projective scheme of finite type over the finite 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 $Y_1, \ldots, Y_d$ are prime divisors intersecting transversally at a point x (i.e. there exists a regular system of parameters $t_1, \ldots, t_d$ with t_i defining Y_i locally at x) and Z is an effective divisor not containing x, then $\sigma^{p-1} \in H^0(X, \omega_X^{1-p})$ splits X compatibly with $Y_1, \ldots, Y_d$.*

Corollary A.2. *(See [3, 1.3.E.6].) Let X denote a regular toric variety for a torus T over k so that all the T-orbits are split tori. Then X is Frobenius split compatibly with the boundary divisor of X, which will be denoted δX.*

Proof. Let $d = \dim_k(X)$ and let $t_1, \ldots, t_d$ denote the coordinates on T coming from the d-factors $\mathbb{G}_m$ in T. Let $\theta = \frac{dt_1 \wedge \cdots \wedge dt_d}{t_1 \cdots t_d} \in H^0(X, \omega_X(\delta X))$. Thus $\sigma = \theta^{-1} \in H^0(X, \omega_X^{-1})$ and $(\sigma)_0 = Y_1 + \cdots + Y_d$ where the Y_i are the prime divisors in δX. Now the last proposition applies. □

Remark A.3. After a finite base extension of the ground field, we may assume that all T-orbits are split tori, and hence that the above hypotheses are satisfied by all regular toric varieties, after possibly a finite field extension.

Corollary A.4 *(Kodaira vanishing). (See [3, 1.2.9 Theorem].) Let X denote a projective, regular toric variety over a field k so that all the T-orbits are split tori. Then $H^i(X, \mathcal{L} \otimes \omega_X) = 0$ for all $i \geqslant 1$ and all ample line bundles $\mathcal{L}$ on X.*

Author's personal copy

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

References

[1] A. Altman, S. Kleiman, Introduction to Grothendieck Duality Theory, Lecture Notes in Math., vol. 146, Springer, New York, 1970.
[2] A. Ashikhmin, S. Litsyn, M.A. Tsfasman, Asymptotically good quantum codes, preprint, 2004.
[3] M. Brion, S. Kumar, Frobenius Splitting Methods in Geometry and Representation Theory, Progr. Math., vol. 231, Birkhäuser Boston, Inc., Boston, MA, 2005.
[4] D.A. Cox, Toric residues, Ark. Mat. 34 (1996) 73–96.
[5] D.A. Cox, The homogeneous coordinate ring of a toric variety, J. Algebraic Geom. 4 (1995) 17–50.
[6] E. Cattani, D. Cox, A. Dickenstein, Residues in toric varieties, Compos. Math. 108 (1) (1997) 35–76.
[7] E. Cattani, A. Dickenstein, A global view of residues in the torus, J. Pure Appl. Algebra 117/118 (1997) 119–144.
[8] E. Cattani, A. Dickenstein, B. Sturmfels, Computing multidimensional residues, in: Algorithms in Algebraic Geometry and Applications, Santander, 1994, in: Progr. Math., vol. 143, Birkhäuser, Basel, 1996, pp. 135–164.
[9] A.R. Calderbank, P. Shor, Good quantum error correcting codes exist, Phys. Rev. A 54 (1996) 1098–1105.
[10] C. D'Andrea, A. Khetan, Macaulay style formulas for toric residues, Compos. Math. 141 (3) (2005) 713–728.
[11] D. Gottesman, Stabilizer codes and quantum error correction, PhD thesis, CalTech, 1997.
[12] P.A. Griffiths, Variations on a theorem of Abel, Invent. Math. 35 (1976) 321–390.
[13] W. Fulton, Introduction to Toric Varieties, Princeton Univ. Press, Princeton, 1993.
[14] S.H. Hansen, The geometry of Deligne–Lusztig varieties; Higher dimensional AG codes, PhD thesis, University of Aarhus, Department of Mathematical Sciences, July 1999.
[15] J.P. Hansen, Toric varieties, Hirzebruch surfaces and error correcting codes, Appl. Algebra Engrg. Comm. Comput. 13 (2002).
[16] Tom Hoholdt, Jacobus H. van Lint, Ruud Pellikan, Algebraic geometry codes, in: Handbook of Coding Theory, vol. 1, Elsevier, Amsterdam, 1998, pp. 871–961.
[17] R. Hartshorne, Algebraic Geometry, Grad. Texts in Math., vol. 52, Springer-Verlag, New York, Heidelberg, 1977.
[18] R. Joshua, R. Akhtar, Toric evaluation codes from higher dimensional toric varieties, in preparation, 2010.
[19] R. Joshua, Good family of quantum stabilizer codes from toric residues, preprint, 2010.
[20] S. Iitaka, Algebraic Geometry, Grad. Texts in Math., vol. 76, Springer-Verlag, 1981.
[21] N. Lauritzen, A.P. Rao, Elementary counterexamples to Kodaira vanishing in positive characteristics, Proc. Indian Acad. Sci. Math. Sci. 107 (1997) 21–25.
[22] A. Khetan, I. Soprunov, Combinatorial construction of toric residues, Ann. Inst. Fourier (Grenoble) 55 (2) (2005) 511–548.
[23] T. Oda, Convex bodies and algebraic geometry, in: An Introduction to the Theory of Toric Varieties, in: Ergeb. Math. Grenzgeb. (3) (Results in Mathematics and Related Areas (3)), vol. 15, Springer-Verlag, Berlin, 1988, Erg. der Math., Springer, 1987, translated from Japanese.
[24] I. Shafarevich, Basic Algebraic Geometry. 2. Schemes and Complex Manifolds, second edition, Springer-Verlag, Berlin, 1994, translated from the 1988 Russian edition by Miles Reid.
[25] P.W. Shor, Fault-tolerant quantum computation, in: Proc. 35th Ann. Symp. on Fundamentals of Computer Science, IEEE Press, Los Alamitos, 1996, pp. 56–65; http://xxx.lanl.giv/abs/quant-ph/9605011.
[26] A.M. Steane, Enlargement of Calderbank–Shor–Steane quantum codes, IEEE Trans. Inform. Theory 45 (1998) 2492–2495.
[27] A.K. Tsikh, Multidimensional Residues and Their Applications, Amer. Math. Soc., Providence, RI, 1992.