

Toric Varieties Hirzebruch Surfaces and Error-Correcting Codes

Johan P. Hansen

Department of Mathematics, Ny Munkegade, 8000 Aarhus C, Denmark
 (e-mail: matjph@mi.aau.dk)

Received: August 21, 2000; revised version: September 3, 2002

Abstract. For any integral convex polytope in \mathbb{R}^2 there is an explicit construction of an error-correcting code of length $(q - 1)^2$ over the finite field \mathbb{F}_q , obtained by evaluation of rational functions on a toric surface associated to the polytope. The dimension of the code is equal to the number of integral points in the given polytope and the minimum distance is determined using the cohomology and intersection theory of the underlying surfaces. In detail we treat Hirzebruch surfaces.

1 Toric codes

Let $M \simeq \mathbb{Z}^2$ be a free \mathbb{Z} -module of rank 2 over the integers \mathbb{Z} . Let \square be an integral convex polytope in $M_{\mathbb{R}} = M \otimes_{\mathbb{Z}} \mathbb{R}$, i.e. a compact convex polyhedron such that the vertices belong to M .

Let q be a prime power and let $\xi \in \mathbb{F}_q$ be a primitive element. For any i such that $0 \leq i \leq q - 1$ and any j such that $0 \leq j \leq q - 1$, we let $P_{ij} = (\xi^i, \xi^j) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$. Let m_1, m_2 be a \mathbb{Z} -basis for M . For any $m = \lambda_1 m_1 + \lambda_2 m_2 \in M \cap \square$, we let $\mathbf{e}(m)(P_{ij}) = (\xi^i)^{\lambda_1} (\xi^j)^{\lambda_2}$.

Definition 1.1. The toric code C_{\square} associated to \square is the linear code of length $n = (q - 1)^2$ generated by the vectors

$$\{(\mathbf{e}(m)(P_{ij}))_{i=0, \dots, q-1; j=0, \dots, q-1} \mid m \in M \cap \square\}. \quad (1)$$

In [3] we presented a general method to obtain the dimension and a lower bound for the minimal distance of a toric code. We obtained the following results.

Theorem 1.2. Let d be a positive integer and let \square be the polytope in $M_{\mathbb{R}}$ with vertices $(0, 0)$, (d, d) , $(0, 2d)$, see figure 1. Assume that $2d \leq q - 1$. The toric code C_{\square} has length equal to $(q - 1)^2$, dimension equal to $\#(M \cap \square) = (d + 1)^2$ (the number of lattice points in \square) and minimal distance is equal to $(q - 1)^2 - 2d(q - 1)$.

Theorem 1.3. Let d be a positive integer and let \square be the polytope in $M_{\mathbb{R}}$ with vertices $(0, 0)$, $(d, 0)$, $(0, d)$, see Fig. 1. Assume that $d < q - 1$. The toric code C_{\square} has length equal to $(q - 1)^2$, dimension equal to $\#(M \cap \square) = \frac{(d+1)(d+2)}{2}$ (the number of lattice points in \square) and minimal distance is equal to $(q - 1)^2 - d(q - 1)$.

Theorem 1.4. Let d, e be positive integers and let \square be the polytope in $M_{\mathbb{R}}$ with vertices $(0, 0)$, $(d, 0)$, (d, e) , $(0, e)$, see Fig. 1. Assume that $d < q - 1$ and that $e < q - 1$. The toric code C_{\square} has length equal to $(q - 1)^2$, dimension equal to $\#(M \cap \square) = (d + 1)(e + 1)$ (the number of lattice points in \square) and minimal distance is equal to $(q - 1)^2 - (d(q - 1) + (q - 1 - d)e) = (q - 1 - d)(q - 1 - e)$.

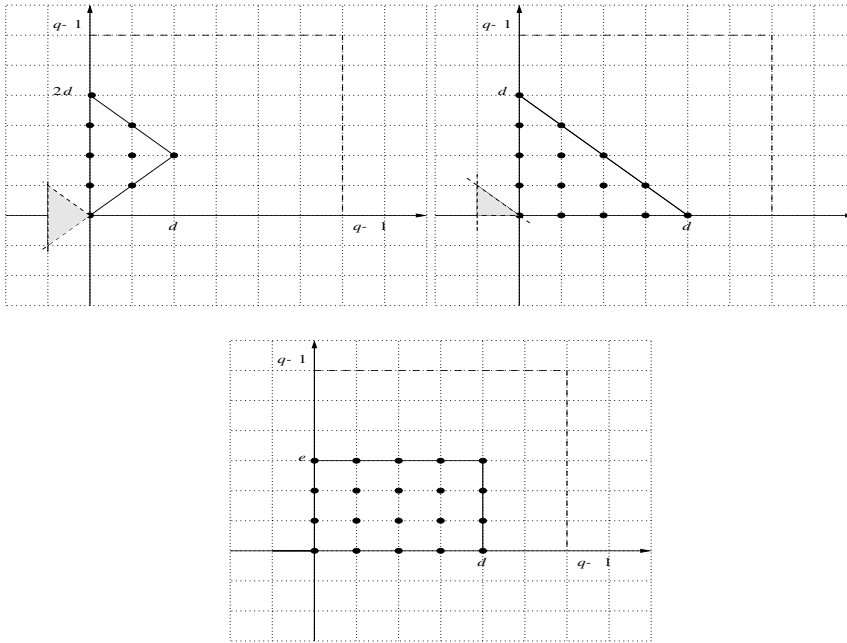


Fig. 1. The polytope of Theorem 1.2 is the left triangle with vertices $(0, 0)$, (d, d) , $(0, 2d)$. The polytope of Theorem 1.3 is the right triangle with vertices $(0, 0)$, $(d, 0)$, $(0, d)$. The polytope of Theorem 1.4 is the square with vertices $(0, 0)$, $(d, 0)$, (d, e) , $(0, e)$

Theorem 1.5. *Let d, e, r be positive integers and let \square be the polytope in $M_{\mathbb{R}}$ with vertices $(0, 0), (d, 0), (d, e+rd), (0, e)$, see Fig. 2. Assume that $d < q-1$, that $e < q-1$ and that $e+rd < q-1$. The toric code C_{\square} has length equal to $(q-1)^2$, dimension equal to $\#(M \cap \square) = (d+1)(e+1) + r\frac{d(d+1)}{2}$ (the number of lattice points in \square) and minimal distance is equal to $\text{Min}\{(q-1-d)(q-1-e), (q-1)(q-1-e-rd)\}$.*

In Fig. 3, we have plotted for $q = 16$ and $q = 32$ the usual xy -diagrams for the codes obtained, where x for a given code is the rate of the code, that is the fraction $\frac{\text{dimension}}{\text{length}}$, and y is the relative minimal distance $\frac{\text{minimal distance}}{\text{length}}$.

Extensive MAGMA calculations by D. Joyner [6] suggested that the bounds for the minimal distances in the theorems obtained in an earlier version of this paper [4] were in fact the true minimum distances. His calculations also helped identify a mistake in the formulation of Theorem 1.5.

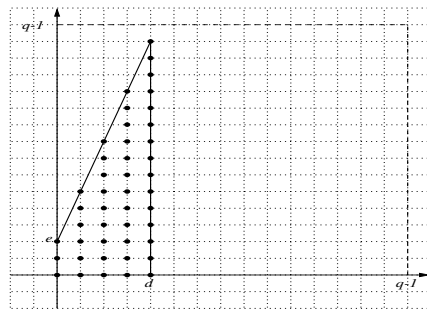


Fig. 2. The polytope of Theorem 1.5 is the polytope with vertices $(0, 0), (d, 0), (d, e+rd), (0, e)$

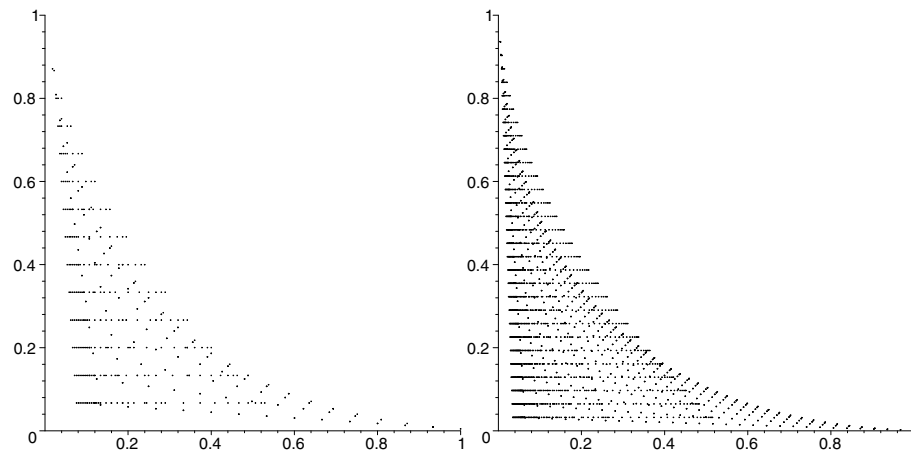


Fig. 3. For all possible codes obtained by Theorem 1.5 a point is marked in the usual xy -diagram, where x for a given code is the rate of the code, that is the fraction $\frac{\text{dimension}}{\text{length}}$, and y is the relative minimal distance $\frac{\text{minimal distance}}{\text{length}}$. The left diagram is for the case $q = 16$ and the right is for the case $q = 32$

2 The Method of Toric Varieties

The toric codes are obtained from evaluating certain rational functions in rational points on toric varieties. For the general theory of toric varieties we refer to [1] and [7]. Here we will be using toric surfaces and we recollect their theory.

In 2.2 we present the method using toric varieties, their cohomology and intersection theory to obtain bounds for the number of rational zeroes of a rational function. In 2.3 this is used to prove the theorems on dimension and minimal distance of the codes C_{\square} presented above.

2.1 Toric Surfaces and Their Cohomology

Let M be an integer lattice $M \simeq \mathbb{Z}^2$. Let $N = \text{Hom}_{\mathbb{Z}}(M, \mathbb{Z})$ be the dual lattice with canonical \mathbb{Z} -bilinear pairing $\langle \cdot, \cdot \rangle: M \times N \rightarrow \mathbb{Z}$. Let $M_{\mathbb{R}} = M \otimes_{\mathbb{Z}} \mathbb{R}$ and $N_{\mathbb{R}} = N \otimes_{\mathbb{Z}} \mathbb{R}$ with canonical \mathbb{R} -bilinear pairing $\langle \cdot, \cdot \rangle: M_{\mathbb{R}} \times N_{\mathbb{R}} \rightarrow \mathbb{R}$.

Given a 2-dimensional integral convex polytope \square in $M_{\mathbb{R}}$. The support function $h_{\square}: N_{\mathbb{R}} \rightarrow \mathbb{R}$ is defined as $h_{\square}(n) := \inf\{\langle m, n \rangle \mid m \in \square\}$ and \square can be reconstructed:

$$\square_h = \{m \in M \mid \langle m, n \rangle \geq h(n) \quad \forall n \in N\}. \quad (2)$$

The support function h_{\square} is piecewise linear in the sense that $N_{\mathbb{R}}$ is the union of a non-empty finite collection of strongly convex polyhedral cones in $N_{\mathbb{R}}$ such that h_{\square} is linear on each cone. A fan is a collection Δ of strongly convex polyhedral cones in $N_{\mathbb{R}}$ such that every face of $\sigma \in \Delta$ is contained in Δ and $\sigma \cap \sigma' \in \Delta$ for all $\sigma, \sigma' \in \Delta$.

The *normal fan* Δ is the coarsest fan such that h_{\square} is linear on each $\sigma \in \Delta$, i.e. for all $\sigma \in \Delta$ there exists $l_{\sigma} \in M$ such that

$$h_{\square}(n) = \langle l_{\sigma}, n \rangle \quad \forall n \in \sigma. \quad (3)$$

The 1-dimensional cones $\rho \in \Delta$ are generated by unique primitive elements $n(\rho) \in N \cap \rho$ such that $\rho = \mathbb{R}_{\geq 0}n(\rho)$.

Upon refinement of the normal fan, we can assume that two successive pairs of $n(\rho)$'s generate the lattice and we obtain *the refined normal fan*. The refined normal fans of the polytopes in Fig. 1 are shown in Fig. 4.

Example 2.1. Consider the polytope of Theorem 1.2. We have that $n(\rho_1) = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $n(\rho_2) = \begin{pmatrix} -1 \\ 1 \end{pmatrix}$, $n(\rho_3) = \begin{pmatrix} -1 \\ 0 \end{pmatrix}$ and $n(\rho_4) = \begin{pmatrix} -1 \\ -1 \end{pmatrix}$. Let σ_1 be the cone generated by $n(\rho_1)$ and $n(\rho_2)$, σ_2 be the cone generated by $n(\rho_2)$ and $n(\rho_3)$, σ_3 the cone generated by $n(\rho_3)$ and $n(\rho_4)$ and σ_4 the cone generated by $n(\rho_4)$ and $n(\rho_1)$.

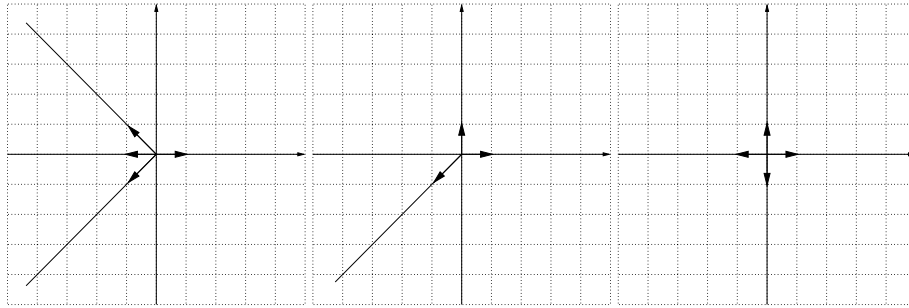


Fig. 4. The refined normal fans of the polytopes in Fig. 1

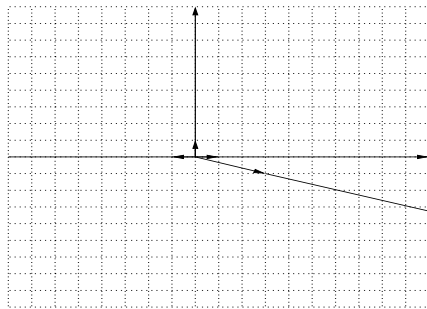


Fig. 5. The normal fan of the polytope in Fig. 2

The support function is:

$$h_{\square} \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} = \begin{cases} \begin{pmatrix} 0 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{if } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_1, \\ \begin{pmatrix} d \\ d \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{if } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_2, \\ \begin{pmatrix} d \\ d \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{if } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_3, \\ \begin{pmatrix} 0 \\ 2d \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{if } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_4. \end{cases}$$

Example 2.2. Next consider the polytope of Theorem 1.3. We have that $n(\rho_1) = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $n(\rho_2) = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $n(\rho_3) = \begin{pmatrix} -1 \\ -1 \end{pmatrix}$. Let σ_1 be the cone generated by $n(\rho_1)$ and $n(\rho_2)$, σ_2 be the cone generated by $n(\rho_2)$ and $n(\rho_3)$ and σ_3 the cone generated by $n(\rho_3)$ and $n(\rho_1)$. The support function is:

$$h_{\square} \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} = \begin{cases} \begin{pmatrix} 0 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{if } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_1, \\ \begin{pmatrix} d \\ 0 \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{if } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_2, \\ \begin{pmatrix} 0 \\ d \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{if } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_3. \end{cases}$$

Example 2.3. Also consider the polytope of Theorem 1.4. We have that $n(\rho_1) = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $n(\rho_2) = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $n(\rho_3) = \begin{pmatrix} -1 \\ 0 \end{pmatrix}$ and $n(\rho_4) = \begin{pmatrix} 0 \\ -1 \end{pmatrix}$. Let σ_1 be the cone generated by $n(\rho_1)$ and $n(\rho_2)$, σ_2 be the cone generated by $n(\rho_2)$ and $n(\rho_3)$, σ_3 the cone generated by $n(\rho_3)$ and $n(\rho_4)$ and σ_4 the cone generated by $n(\rho_4)$ and $n(\rho_1)$. The support function is:

$$h_{\square} \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} = \begin{cases} \begin{pmatrix} 0 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{if } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_1, \\ \begin{pmatrix} d \\ 0 \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{if } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_2, \\ \begin{pmatrix} d \\ e \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{if } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_3, \\ \begin{pmatrix} 0 \\ e \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{if } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_4. \end{cases}$$

Example 2.4. Finally consider the polytope of Theorem 1.5. We have that $n(\rho_1) = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $n(\rho_2) = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $n(\rho_3) = \begin{pmatrix} -1 \\ 0 \end{pmatrix}$ and $n(\rho_4) = \begin{pmatrix} r \\ -1 \end{pmatrix}$. Let σ_1 be the cone generated by $n(\rho_1)$ and $n(\rho_2)$, σ_2 be the cone generated by $n(\rho_2)$ and $n(\rho_3)$, σ_3 the cone generated by $n(\rho_3)$ and $n(\rho_4)$ and σ_4 the cone generated by $n(\rho_4)$ and $n(\rho_1)$. The support function is:

$$h_{\square} \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} = \begin{cases} \begin{pmatrix} 0 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{if } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_1, \\ \begin{pmatrix} d \\ 0 \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{if } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_2, \\ \begin{pmatrix} d \\ e + rd \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{if } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_3, \\ \begin{pmatrix} 0 \\ e \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{if } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_4. \end{cases}$$

The 2-dimensional *algebraic torus* $T_N \simeq \overline{\mathbb{F}}_q^* \times \overline{\mathbb{F}}_q^*$ is defined by $T_N := \text{Hom}_{\mathbb{Z}}(M, \overline{\mathbb{F}}_q^*)$. The multiplicative character $\mathbf{e}(m)$, $m \in M$ is the homomorphism $\mathbf{e}(m) : T \rightarrow \overline{\mathbb{F}}_q^*$ defined by $\mathbf{e}(m)(t) = t(m)$ for $t \in T_N$. Specifically, if $\{n_1, n_2\}$ and $\{m_1, m_2\}$ are dual \mathbb{Z} -bases of N and M and we denote $u_j := \mathbf{e}(m_j)$, $j = 1, 2$, then we have an isomorphism $T_N \simeq \overline{\mathbb{F}}_q^* \times \overline{\mathbb{F}}_q^*$ sending t to $(u_1(t), u_2(t))$. For $m = \lambda_1 m_1 + \lambda_2 m_2$ we have

$$\mathbf{e}(m)(t) = u_1(t)^{\lambda_1} u_2(t)^{\lambda_2}.$$

The *toric surface* X_{\square} associated to the refined normal fan Δ of \square is

$$X_{\square} = \bigcup_{\sigma \in \Delta} U_{\sigma}$$

where U_{σ} is the $\overline{\mathbb{F}}_q$ -valued points of the affine scheme $\text{Spec}(\overline{\mathbb{F}}_q[S_{\sigma}])$, i.e.

$$U_{\sigma} = \{u : S_{\sigma} \rightarrow \overline{\mathbb{F}}_q \mid u(0) = 1, u(m + m') = u(m)u(m') \forall m, m' \in S_{\sigma}\},$$

where S_{σ} is the additive subsemigroup of M

$$S_{\sigma} = \{m \in M \mid \langle m, y \rangle \geq 0 \forall y \in \sigma\}.$$

The *toric surface* X_{\square} is irreducible, non-singular and complete, see [7, Chapter 1]. If $\sigma, \tau \in \Delta$ and τ is a face of σ , then U_{τ} is an open subset of U_{σ} . Obviously $S_{\emptyset} = M$ and $U_{\emptyset} = T_N$ such that the algebraic torus T_N is an open subset of X_{\square} .

T_N acts *algebraically* on X_{\square} . On $u \in U_{\sigma}$ the action of $t \in T_N$ is obtained as

$$(tu)(m) := t(m)u(m) \quad m \in S_{\sigma}$$

such that $tu \in U_{\sigma}$ and U_{σ} is T_N -stable. The orbits of this action is in one-to-one correspondance with Δ . For each $\sigma \in \Delta$ let

$$\text{orb}(\sigma) := \{u : M \cap \sigma \rightarrow \overline{\mathbb{F}}_q^* \mid u \text{ is a group homomorphism}\}.$$

Then $\text{orb}(\sigma)$ is a T_N orbit in X_{\square} . Define $V(\sigma)$ to be the closure of $\text{orb}(\sigma)$ in X_{\square} .

A Δ -linear support function h gives rise to the Cartier divisor D_h . Let $\Delta(1)$ be the 1-dimensional cones in Δ then

$$D_h := - \sum_{\rho \in \Delta(1)} h(n(\rho)) V(\rho).$$

In particular

$$D_m = \text{div}(\mathbf{e}(-m)) \quad m \in M.$$

Following [7, Lemma 2.3] we have the lemma.

Lemma 2.5. *Let h be a Δ -linear support function with associated Cartier divisor D_h and convex polytope \square_h defined in (2). The vector space $\mathbf{H}^0(X, \mathcal{O}_X(D_h))$ of global sections of $\mathcal{O}_X(D_h)$, i.e. rational functions f on X_{\square} such that $\text{div}(f) + D_h \geq 0$ has dimension $\#(M \cap \square_h)$ and has $\{\mathbf{e}(m) \mid m \in M \cap \square_h\}$ as a basis.*

Remark 2.6. In Example 2.1

$$D_h := - \sum_{\rho \in \Delta(1)} h(n(\rho)) V(\rho) = d V(\rho_3) + 2d V(\rho_4)$$

and

$$\dim H^0(X, \mathcal{O}_X(D_h)) = (d + 1)^2.$$

In Example 2.2

$$D_h := - \sum_{\rho \in \Delta(1)} h(n(\rho)) V(\rho) = d V(\rho_3)$$

and

$$\dim H^0(X, \mathcal{O}_X(D_h)) = \frac{(d + 1)(d + 2)}{2}.$$

In Example 2.3

$$D_h := - \sum_{\rho \in \Delta(1)} h(n(\rho)) V(\rho) = d V(\rho_3) + e V(\rho_4)$$

and

$$\dim H^0(X, \mathcal{O}_X(D_h)) = (d + 1)(e + 1).$$

In Example 2.4

$$D_h := - \sum_{\rho \in \Delta(1)} h(n(\rho)) V(\rho) = d V(\rho_3) + e V(\rho_4)$$

and

$$\dim H^0(X, \mathcal{O}_X(D_h)) = (d + 1)(e + 1) + r \frac{d(d + 1)}{2}.$$

2.2 Intersection Theory and the Number of Rational Zeroes of a Rational Function

For a fixed linebundle \mathcal{L} on X , given an effective divisor D such that $\mathcal{L} = \mathcal{O}_X(D)$, the fundamental question to answer is: How many points from a fixed set \mathcal{P} of rational points are in the support of D . This question is treated in general in [5] using intersection theory, see [2]. Here we will apply the same methods when X is a toric surface.

For a Δ -linear support function h and a 1-dimensional cone $\rho \in \Delta(1)$ we will determine the intersection number $(D_h; V(\rho))$ between the Cartier divisor D_h and $V(\rho) = \mathbb{P}^1$. This number is obtained in [7, Lemma 2.11]. The cone ρ is

the common face of two 2-dimensional cones $\sigma', \sigma'' \in \Delta(2)$. Choose primitive elements $n', n'' \in N$ such that

$$\begin{aligned} n' + n'' &\in \mathbb{R}\rho \\ \sigma' + \mathbb{R}\rho &= \mathbb{R}_{\geq 0}n' + \mathbb{R}\rho \\ \sigma'' + \mathbb{R}\rho &= \mathbb{R}_{\geq 0}n'' + \mathbb{R}\rho \end{aligned}$$

Lemma 2.7. *For any $l_\rho \in M$, such that h coincides with l_ρ on ρ , let $\bar{h} = h - l_\rho$. Then*

$$(D_h; V(\rho)) = -(\bar{h}(n') + \bar{h}(n'')).$$

In the 2-dimensional non-singular case let $n(\rho)$ be a primitive generator for the 1-dimensional cone ρ . There exists an integer a such that

$$n' + n'' + an(\rho) = 0,$$

$V(\rho)$ is itself a Cartier divisor and the above gives the self-intersection number

$$(V(\rho); V(\rho)) = a.$$

More generally the self-intersection number of a Cartier divisor D_h is obtained in [7, Prop. 2.10].

Lemma 2.8. *Let D_h be a Cartier divisor and let \square_h be the polytope associated to h , see (2). Then*

$$(D_h; D_h) = 2 \text{vol}_2(\square_h),$$

where vol_2 is the normalized Lebesgue-measure.

In case of Theorem 1.5 the intersection table becomes

	$V(\rho_1)$	$V(\rho_2)$	$V(\rho_3)$	$V(\rho_4)$
$V(\rho_1)$	$-r$	1	0	1
$V(\rho_2)$	1	0	1	0
$V(\rho_3)$	0	1	r	1
$V(\rho_4)$	1	0	1	0

2.3 Determination of Parameters

We start by exhibiting the toric codes as evaluation codes.

For each $t \in T \simeq \overline{\mathbb{F}}_q^* \times \overline{\mathbb{F}}_q^*$, we can evaluate the rational functions in $H^0(X, O_X(D_h))$

$$\begin{aligned} H^0(X, O_X(D_h)) &\rightarrow \overline{\mathbb{F}}_q^* \\ f &\mapsto f(t). \end{aligned}$$

Let $H^0(X, O_X(D_h))^{\text{Frob}}$ denote the rational functions in $H^0(X, O_X(D_h))$ that are invariant under the action of Frobenius, that is functions that are \mathbb{F}_q linear combinations of the functions $(\mathbf{e})(m)$ of Definition 1.1.

Evaluating in all points in $T(\mathbb{F}_q)$ we obtain the code C_\square :

$$\begin{aligned} H^0(X, O_X(D_h))^{\text{Frob}} &\rightarrow C_\square \subset (\mathbb{F}_q^*)^{\#T(\mathbb{F}_q)} \\ f &\mapsto (f(t))_{t \in T(\mathbb{F}_q)} \end{aligned}$$

and the generators of the code is obtained as the image of the basis:

$$\mathbf{e}(m) \mapsto (\mathbf{e}(m)(t))_{t \in T(\mathbb{F}_q)}.$$

as in (1).

Let $m_1 = (1, 0)$. The \mathbb{F}_q -rational points of $T \simeq \overline{\mathbb{F}_q}^* \times \overline{\mathbb{F}_q}^*$ belong to the $q-1$ lines on X_\square given by $\prod_{\eta \in \mathbb{F}_q} (\mathbf{e}(m_1) - \eta) = 0$. Let $0 \neq f \in H^0(X, O_X(D_h))$ and assume that f is zero along precisely a of these lines. As $\mathbf{e}(m_1) - \eta$ and $\mathbf{e}(m_1)$ have the same divisors of poles, they have equivalent divisors of zeroes, so

$$(\text{div}(\mathbf{e}(m_1) - \eta))_0 \sim (\text{div}(\mathbf{e}(m_1)))_0.$$

Therefore

$$\text{div}(f) + D_h - a(\text{div}(\mathbf{e}(m_1)))_0 \geq 0$$

or equivalently

$$f \in H^0(X, O_X(D_h - a(\text{div}(\mathbf{e}(m_1)))_0)).$$

In the cases of all the theorems this implies that $a \leq d$ according to Lemma 2.5. On any of the other $q-1-a$ lines the number of zeroes of f is according to [5] at most the intersection number:

$$(D_h - a(\text{div}(\mathbf{e}(m_1)))_0; (\text{div}(\mathbf{e}(m_1)))_0). \quad (4)$$

This number can be calculated using Lemma 2.7 and Lemma 2.8. In the situation of Theorem 1.2 the number is $2d - a \cdot 2 \cdot (\frac{1}{2} \cdot 1 \cdot 2) = 2d - 2a$ and in the situation of Theorem 1.3 it is $d - a \cdot 2 \cdot (\frac{1}{2} \cdot 1 \cdot 1) = d - a$ (in both cases the volume-element is shown as gray in figure 1). In the situation of Theorem 1.4 the volume-element is the line segment shown in bold in figure 1 and the number is e . As $0 \leq a \leq d$ the total number of zeroes for f in the three cases is at most:

$$a(q-1) + (q-1-a)(2d-2a) \leq (q-1)2d$$

$$a(q-1) + (q-1-a)(d-a) \leq d(q-1)$$

$$a(q-1) + (q-1-a)e \leq d(q-1) + (q-1-d)e$$

In case of Theorem 1.5 the intersection number (4) is easily calculated using the intersection table above and that $(\operatorname{div}(\mathbf{e}(m_1)))_0 = V(\rho_1) + rV(\rho_4)$. We get

$$(D_h - a(\operatorname{div}(\mathbf{e}(m_1)))_0; (\operatorname{div}(\mathbf{e}(m_1)))_0) = e + (d - a)r.$$

As $0 \leq a \leq d$ the total number of zeroes for f is at most

$$\begin{aligned} & a(q - 1) + (q - 1 - a)(e + (d - a)r) \\ & \leq \max\{d(q - 1) + (q - 1 - d)e, (q - 1)(e + dr)\}. \end{aligned}$$

This implies in all cases that the evaluation maps

$$\begin{aligned} \mathbf{H}^0(X, O_X(D_h))^{\operatorname{Frob}} & \rightarrow C_{\square} \subset (\mathbb{F}_q^*)^{\sharp T(\mathbb{F}_q)} \\ f & \mapsto (f(t))_{t \in T(\mathbb{F}_q)} \end{aligned}$$

are injective and that the dimensions and the lower bounds for the minimal distances of the toric codes are as claimed.

To see that the lower bounds for the minimal distances are in fact the true minimal distances we exhibit codewords of minimal weight.

In the case of Theorem 1.2, we let $b_1, \dots, b_{2d} \in \mathbb{F}_q^*$ be pairwise different elements. Then the function

$$(y - b_1) \cdots (y - b_{2d}) \in \mathbf{H}^0(X, O_X(D_h))^{\operatorname{Frob}}$$

evaluates to zero in the $(q - 1)(2d)$ points

$$(x, b_j), \quad x \in \mathbb{F}_q^*, j = 1, \dots, 2d$$

and gives a codeword of weight $(q - 1)^2 - 2d(q - 1)$.

In the case of Theorem 1.3, we let $b_1, \dots, b_d \in \mathbb{F}_q^*$ be pairwise different elements. Then the function

$$(y - b_1) \cdots (y - b_d) \in \mathbf{H}^0(X, O_X(D_h))^{\operatorname{Frob}}$$

evaluates to zero in the $(q - 1)d$ points

$$(x, b_j), \quad x \in \mathbb{F}_q^*, j = 1, \dots, d$$

and gives a codeword of weight $(q - 1)^2 - 2d(q - 1)$.

In the case of Theorem 1.4 and Theorem 1.5, we let $b_1, \dots, b_{e+rd} \in \mathbb{F}_q^*$ be pairwise different elements. Then the function

$$x^d(y - b_1) \cdots (y - b_{e+rd}) \in \mathbf{H}^0(X, O_X(D_h))^{\operatorname{Frob}}$$

evaluates to zero in the $(q - 1)(e + rd)$ points

$$(x, b_j), \quad x \in \mathbb{F}_q^*, j = 1, \dots, e + rd$$

and gives a codeword of weight $(q - 1)^2 - (q - 1)(e + rd) = (q - 1)(q - 1 - (e + rd))$. On the other hand, we let $a_1, \dots, a_d \in \mathbb{F}_q^*$ be pairwise different elements and let $b_1, \dots, b_e \in \mathbb{F}_q^*$ be pairwise different elements. Then the function

$$(x - a_1) \cdots (x - a_d)(y - b_1) \cdots (y - b_e) \in H^0(X, O_X(D_h))^{\text{Frob}}$$


evaluates to zero in the $d(q - 1) + (q - 1)e - de$ points

$$(a_i, y), (x, b_j), \quad x, y \in \mathbb{F}_q^*, i = 1, \dots, d, j = 1, \dots, e$$

and gives a codeword of weight $(q - 1 - d)(q - 1 - e)$.

References

1. Fulton, W.: Introduction to Toric Varieties, Annals of Mathematics Studies; No. 131, Princeton University Press, 1993
2. Fulton, W.: Intersection theory, Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, Berlin Heidelberg New York: Springer 1998
3. Hansen, J. P.: Toric Surfaces and Error-correcting codes, In: Coding theory, cryptography and related areas (Guanajuato, 1998), pp. 132–142, Berlin: Springer 2000
4. Hansen, J. P.: Hirzebruch surfaces and Error-correcting Codes, Preprint Series No. 6, 2000, University of Aarhus
5. Hansen, ■, Søren Have, ■: Error-correcting codes from higher-dimensional varieties, Finite Fields Appl. 7, 531–552 (2001)
6. Joyner, ■, David, ■: Toric codes over finite fields, Preprint, Aug. 2002, <http://front.math.ucdavis.edu/math.AG/0208155>
7. Oda, T.: Convex Bodies and Algebraic Geometry, An Introduction to the Theory of Toric Varieties, Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, Band 15, Berlin Heidelberg New York: Springer 1985

	200	0106	Despatch : 27/9/2002	Journal : AAECC
	Journal No.	Article No.	Author Received	No. of Pages : 12
	Disk Received : Yes		Disk Used : Yes	