UNIVERSITY OF AARHUS
DEPARTMENT OF MATHEMATICS

ISSN: 1397–4076

TORIC SURFACES AND CODES, TECHNIQUES AND EXAMPLES

By Johan P. Hansen

Preprint Series No.: 1

January 2004

Ny Munkegade, Bldg. 530
DK-8000 Aarhus C, Denmark

http://www.imf.au.dk
institut@imf.au.dk

TORIC SURFACES AND CODES, TECHNIQUES AND EXAMPLES

JOHAN P. HANSEN

Abstract. We treat toric surfaces and their application to construction of error-correcting codes and determination of the parameters of the codes, surveying and expanding the results of [4].

For any integral convex polytope in $\mathbb{R}^2$ there is an explicit construction of a unique error-correcting code of length $(q-1)^2$ over the finite field $\mathbb{F}_q$. The dimension of the code is equal to the number of integral points in the polytope.

The code can be considered as obtained by evaluation of rational functions on a (not uniguely determined) toric surface associated to the given polytope. Intersection theory on the toric surface will in two different ways be applied to bound the minimal distance of the code. In some cases we even obtain the precise minimal distance of the code.

The techniques are illustrated by several examples

1. Toric codes

Let $M \simeq \mathbb{Z}^2$ be a free $\mathbb{Z}$-module of rank 2 over the integers $\mathbb{Z}$. Let $\Box$ 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 $m = \lambda_1 m_1 + \lambda_2 m_2 \in M \cap \Box$, we let $\mathbf{e}(m)(P_{ij}) = (\xi^i)^{\lambda_1}(\xi^j)^{\lambda_2}$.

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

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

In [4] we obtain the following results with precise determination of the parameters of two families of toric codes.

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

Theorem 1.3. *Let d, e, r be positive integers and let $\Box$ be the polytope in $M_{\mathbb{R}}$ with vertices $(0,0),(d,0),(d,e+rd),(0,e)$, see figure 2. Assume that $d < q-1$, that $e < q-1$ and that $e+rd < q-1$. The toric code $C_\Box$ has length equal to $(q-1)^2$, dimension*

Document version: January 2, 2004.

1991 *Mathematics Subject Classification.* 14M25, 94Bxx.

Key words and phrases. Toric Surfaces, Error-correcting Codes. Intersection Theory.

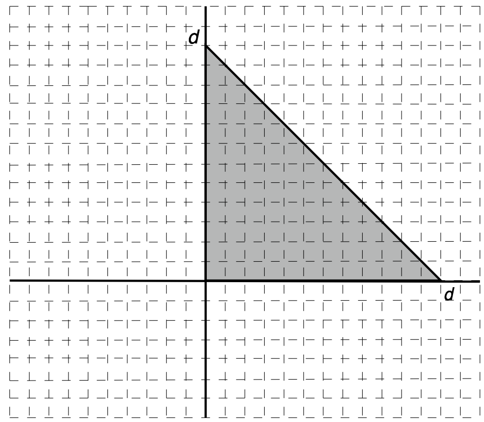

FIGURE 1. The convex polytope of Theorem 1.2 with vertices $(0,0),(d,0),(0,d)$.

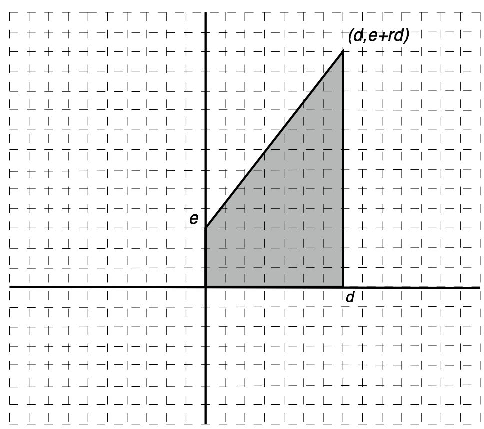

FIGURE 2. The convex polytope of Theorem 1.3 with vertices $(0,0),(d,0),(d,e+rd),(0,e)$.

equal to $\#(M\cap\square)=(d+1)(e+1)+r\frac{d(d+1)}{2}$ *(the number of lattice points in* $\square$*) and the minimal distance is equal to* $\mathrm{Min}\{(q-1-d)(q-1-e),(q-1)(q-1-e-rd)\}$.

Using various intersection techniques on suitable chosen toric surfaces, we obtain the following new results.

Theorem 1.4. *Let* d *be a positive integers and let* $\square$ *be the polytope in* $M_{\mathbb{R}}$ *with vertices* $(0,0),(d,0),(0,2d)$*, see figure 3. Assume that* $2d<q-1$*. The toric code* $C_{\square}$ *has length equal to* $(q-1)^2$ *, dimension equal to* $\#(M\cap\square)=d^2+2d+1$ *(the number of lattice points in* $\square$*) and the minimal distance is greater or equal to* $(q-1)^2-2d(q-1)=(q-1)(q-1-2d)$.

Theorem 1.5. *Let* d,e,f *be positive integers such that* $f>e$ *and* $f-e$ *is even. Let* $\square$ *be the polytope in* $M_{\mathbb{R}}$ *with vertices* $(0,0),(d,f-d),(\frac{f-e}{2},\frac{f+e}{2}),(0,e)$ *see figure*

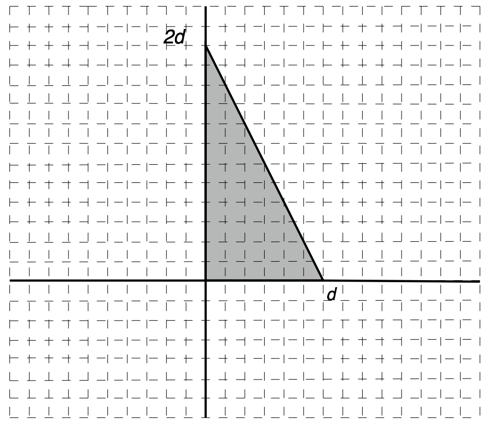

FIGURE 3. The convex polytope of Theorem 1.4 with vertices $(0,0),(d,0),(0,2d)$.

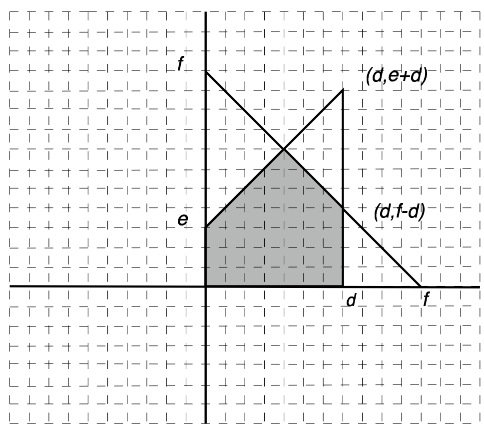

FIGURE 4. The convex polytope of Theorem 1.5 with vertices $(0,0),(d,f-d),(\frac{f-e}{2},\frac{f+e}{2}),(0,e)$

4. Assume that $d < q-1$, that $e < q-1$ and that $\frac{f+e}{2} < q-1$. The toric code $C_\square$ has length equal to $(q-1)^2$, dimension equal to

$$\#(M \cap \square) = -1/2\, d^2 - 1/4\, e^2 + 1/2\, ef - 1/4\, f^2 + fd + 1/2\, f + 1/2\, d + 1/2\, e + 1$$

(the number of lattice points in $\square$) and the minimal distance is greater than or equal to $\left(q-1-\left(\frac{f+e}{2}\right)\right)(q-1-d)$.

In [3] and [4] we presented general methods to obtain the dimension and a lower bound for the minimal distance of a toric code. D. Joyner has in [6] presented extensive MAGMA calculations on toric codes.

2. Toric varieties

For the general theory of toric varieties we refer to [1] and [7]. Here we recollect some of the theory of relevance for the present purpose.

Let k be an algebraically closed field and let $T = (k^*)^n$ be the n-dimensional torus. A toric variety is a compactification X of T with an action $T \times X \to X$ of T on X that extends the natural action of T on itself.

The *character group* is

$$M = \{\chi : T \to k^* | \chi \text{ is a group homomorphism}\}$$

and the group of 1-*parameter subgroups* is

$$N = \{\lambda : k^* \to T | \lambda \text{ is a group homomorphism}\}.$$

We remark, that $M \simeq \mathbb{Z}^n$, where the n-tuple $m = (m_1, \ldots, m_n) \in \mathbb{Z}^n$ corresponds to the character

$$\mathbf{e}(m)\,(t_1, \ldots, t_n) = t_1^{m_1} \cdot \cdots \cdot t_n^{m_n}.$$

Also $N \simeq \mathbb{Z}^n$, where the n-tuple $u = (u_1, \ldots, u_n) \in \mathbb{Z}^n$ corresponds to the 1-parameter subgroup

$$\lambda(u)(t) = (t_1^{u_1}, \ldots, t_n^{u_n}).$$

For $\chi \in M$ and $\lambda \in N$ there is an integer $< \chi, \lambda >$, such that the composition $\chi \circ \lambda : k^* \to k^*$ is of the form

$$\chi \circ \lambda\,(t) = t^{<\chi,\lambda>}.$$

This gives a perfect pairing $< -, - > M \times N \to \mathbb{Z}$ and in the notation above, we have that $< \mathbf{e}(m), \lambda(u) >= m_1 u_1 + \cdots + m_n u_n$. 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 $< -, - >: M_{\mathbb{R}} \times N_{\mathbb{R}} \to \mathbb{R}$.

2.1. **Convex polytopes and support functions. Fans, normal fans and refined normal fans.** Given a n-dimensional integral convex polytope $\square$ in $M_{\mathbb{R}}$. The support function of the polytope is the function

$$h_\square : N_{\mathbb{R}} \to \mathbb{R}$$

$$h_\square(n) := \inf\{< m, n > | \, m \in \square\}.$$

The convex polytope $\square$ can be reconstructed from the support function :

$$\square_h = \{m \in M | \, < m, n > \geq h(n) \quad \forall n \in N\}.$$

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 of the convex polytope $\square$ is the coarsest fan such that the support function $h_\square$ is linear on each $\sigma \in \Delta$, i.e. for all $\sigma \in \Delta$ there exists $l_\sigma \in M$ such that

$$h_\square(n) =< l_\sigma, n > \quad \forall n \in \sigma.$$

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 for every $\sigma \in \Delta$ there exists a $\mathbb{Z}$-basis $\{n_1, \ldots, n_r\}$ of N and $s \leq r$ such that $\sigma = \mathbb{R}_{\geq 0} n_1 + \cdots + \mathbb{R}_{\geq 0} n_s$. In the 2-dimensional case it means that two successive pairs of $n(\rho)$'s generate the

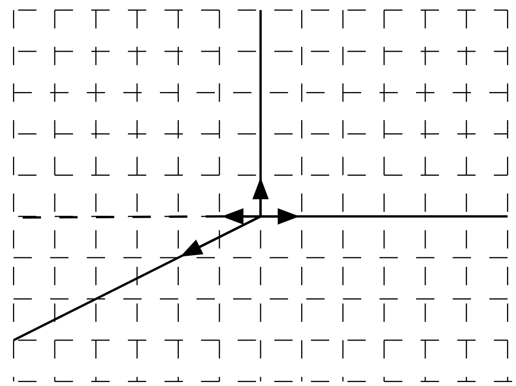

FIGURE 5. The normal fan and the refined normal fan with primitive generators of the 1-dimensional cones of the polytope in figure 3. The added 1-dimensional cone in the refined fan is shown as a dotted halfline.

lattice and we obtain *the refined normal fan.* In the 2-dimensional case there is a method using continued fractions to obtain the refinement, see [7, Sec. 1.6].

2.1.1. *Pick's formula for the number of lattice points in a convex polytope.* It will be important to calculate the number of lattice points $\#\square$ in a convex polytope. In the 2-dimensional case *Pick's formula* gives that

$$\#\square = vol_2(\square) + \frac{\text{Perimeter}(\square)}{2} + 1.$$

In calculating the perimeter one should take into account that the length of an edge of $\square$ is one more that the number af lattice points lying strictly between the endpoints of the edge. See [1, p.113] and [7, p.101].

In the case of the polytope of Theorem 1.4, shown in figure 3, we get

$$\#\square = \frac{2d \cdot d}{2} + \frac{d + 2d + d}{2} + 1 = d^2 + 2d + 1.$$

In the case of the polytope of Theorem 1.5, shown in figure 4, we get

$$\begin{aligned}\#\square = & \quad \left[g(e+d) - \tfrac{d^2}{2} - \tfrac{(e-f+2d)^2}{4}\right] + \tfrac{f+d+e}{2} + 1 \\ = & \quad -1/2\, d^2 - 1/4\, e^2 + 1/2\, ef - 1/4\, f^2 + fd + 1/2\, f + 1/2\, d + 1/2\; e + 1\end{aligned}$$

2.1.2. *Support functions and fans associated to the polytope of Theorem 1.4 shown in figure 3.* Let d, e be a positive integers and let $\square$ be the polytope in $M_{\mathbb{R}}$ with vertices $(0,0), (d,0), (0,2d)$, see figure 3. Assume that $2d < q - 1$. In figure 5 the normal fan and the refined normal fan of the polytope are shown together with the primitive generators of the 1-dimensional cones in the refined normal fan

$$n(\rho_1) = \begin{pmatrix}1\\0\end{pmatrix}, n(\rho_2) = \begin{pmatrix}0\\1\end{pmatrix}, n(\rho_3) = \begin{pmatrix}-1\\0\end{pmatrix}, n(\rho_4) = \begin{pmatrix}-2\\-1\end{pmatrix}.$$

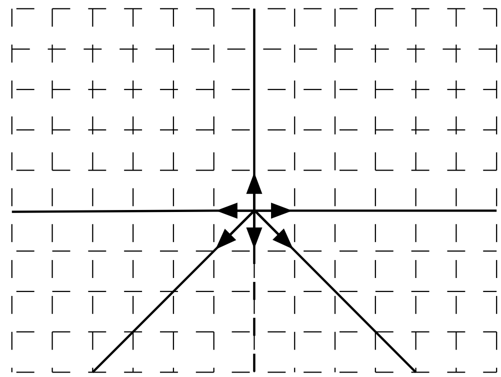

FIGURE 6. The normal fan and the refined normal fan with primitive generators of the 1-dimensional cones of the polytope in figure 4. The added 1-dimensional cone in the refined fan is shown as a dotted halfline.

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 corresponding support function is:

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

2.1.3. *Support functions and fans associated to the polytope of Theorem 1.5 shown in figure 4.* Let d, e, f be positive integers such that $f > e$ and $f - e$ is even. Let $\square$ be the polytope in $M_{\mathbb{R}}$ with vertices $(0,0), (d, f-d), (\frac{f-e}{2}, \frac{f+e}{2}), (0, e)$ see figure 4. Assume that $d < q-1$, that $e < q-1$ and that $\frac{f+e}{2} < q-1$.

In figure 6 the normal fan and the refined normal fan of the polytope are shown together with the primitive generators of the 1-dimensional cones in the refined normal fan

$$n(\rho_1) = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, n(\rho_2) = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, n(\rho_3) = \begin{pmatrix} -1 \\ 0 \end{pmatrix}$$

$$n(\rho_4) = \begin{pmatrix} -1 \\ -1 \end{pmatrix}, n(\rho_5) = \begin{pmatrix} 0 \\ -1 \end{pmatrix}, n(\rho_6) = \begin{pmatrix} 1 \\ -1 \end{pmatrix},$$

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 $n(\rho_4)$, σ_4 the cone generated by $n(\rho_4)$ and $n(\rho_5)$, σ_5 the cone generated by $n(\rho_5)$ and $n(\rho_6)$ and σ_6 the cone generated by $n(\rho_6)$ and $n(\rho_1)$. The corresponding support function is:

$$h_{\Box}\begin{pmatrix} n_1 \\ n_2 \end{pmatrix} = \begin{cases} \begin{pmatrix} 0 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{if } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_1, \\ \begin{pmatrix} d \\ 0 \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{if } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_2, \\ \begin{pmatrix} d \\ f-d \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{if } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_3 \\ \begin{pmatrix} \frac{f-e}{2} \\ \frac{f+e}{2} \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{if } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_4 \cup \sigma_5 \\ \begin{pmatrix} 0 \\ e \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{if } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_6. \end{cases}$$

2.2. **Toric varieties defined by fans associated to polytopes.** The *toric variety* $X_{\Box}$ associated to the refined normal fan Δ of $\Box$ is

$$X_{\Box} = \cup_{\sigma\in\Delta} U_\sigma$$

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

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

where S_σ is the additive subsemigroup of M

$$S_\sigma = \{m \in M | < m, y > \geq 0 \forall y \in \sigma\}.$$

The *toric variety* $X_{\Box}$ 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 $S_0 = M$ and $U_0 = T_N$ such that the algebraic torus T_N is an open subset of $X_{\Box}$.

T_N *acts algebraically* on $X_{\Box}$. 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

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

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

2.3. **Support functions and Cartier divisors on toric varieties.** 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

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

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

Lemma 2.1. *Let h be a Δ-linear support function with associated Cartier divisor D_h and convex polytope $\Box_h$ defined in (2.1). The vector space* $\mathrm{H}^0(X, O_X(D_h))$ *of global sections of $O_X(D_h)$, i.e. rational functions f on $X_{\Box}$ such that* $\mathrm{div}(f) + D_h \geq 0$ *has dimension $\#(M \cap \Box_h)$ and has $\{\mathbf{e}(m) | m \in M \cap \Box_h\}$ as a basis.*

The lemma and the results of 2.1.1 gives that the Cartier divisor associated to the polytope of Theorem 1.4 is

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

and

$$\dim \mathrm{H}^0(X, O_X(D_h)) = d^2 + 2d + 1,$$

whereas the Cartier divisor associated to the polytope of Theorem 1.5 is

$$D_h := -\sum_{\rho\in\Delta(1)} h(n(\rho))\,V(\rho) = d\,V(\rho_3) + f\,V(\rho_4) + \left(\frac{f+e}{2}\right)V(\rho_5) + e\,V(\rho_6)$$

and

$$\dim \mathrm{H}^0(X, O_X(D_h)) =$$
$$-1/2\,d^2 - 1/4\,e^2 + 1/2\,ef - 1/4\,f^2 + fd + 1/2\,f + 1/2\,d + 1/2\,e + 1.$$

2.4. **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 $\mathcal{L} = O_X(D)$, 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

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

Lemma 2.2. *For any $l_\rho \in M$, such that h coincides with l_ρ on ρ, let $\overline{h} = h - l_\rho$. Then*

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

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 2.3. *Let D_h be a Cartier divisor and let $\Box_h$ be the polytope associated to h , see (2.1). Then*

$$(D_h; D_h) = 2\,\mathrm{vol}_2(\Box_h),$$

where vol_2 *is the normalized Lesbesgue-measure.*

In the situation of Theorem 1.4 there are four 1-dimensional cones (2.1.2) and the intersection table becomes

	$V(\rho_1)$	$V(\rho_2)$	$V(\rho_3)$	$V(\rho_4)$
$V(\rho_1)$	2	1	0	1
$V(\rho_2)$	1	0	1	0
$V(\rho_3)$	0	1	-2	1
$V(\rho_4)$	1	0	1	0

In the situation of Theorem 1.5 there are six 1-dimensional cones (2.1.3) and the intersection table becomes

	$V(\rho_1)$	$V(\rho_2)$	$V(\rho_3)$	$V(\rho_4)$	$V(\rho_5)$	$V(\rho_6)$
$V(\rho_1)$	-1	1	0	0	0	1
$V(\rho_2)$	1	0	1	0	0	0
$V(\rho_3)$	0	1	-1	1	0	0
$V(\rho_4)$	0	0	1	-1	1	0
$V(\rho_5)$	0	0	0	1	-1	1
$V(\rho_6)$	1	0	0	0	1	-1

2.5. **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 $\mathrm{H}^0(X, O_X(D_h))$

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

Let $\mathrm{H}^0(X, O_X(D_h))^{\mathrm{Frob}}$ denote the rational functions in $\mathrm{H}^0(X, O_X(D_h))$ 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 $C_\square$:

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

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 (1.1).

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 $0 \neq f \in \mathrm{H}^0(X, O_X(D_h))$ 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

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

Therefore

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

or equivalently

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

On any of the other $q-1-a$ lines the number of zeroes of f is according to [5] at most the intersection number:

$$(D_h - a(\mathrm{div}(\mathbf{e}(m_1)))_0; (\mathrm{div}(\mathbf{e}(m_1)))_0). \tag{1}$$

This number can be calculated using Lemma 2.2 and Lemma 2.3.

2.5.1. *Determination of a lower bound for the minimal distance in the situation of Theorem 1.4.* 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 $0 \neq f \in \mathrm{H}^0(X, O_X(D_h))$ and assume that f is zero along precisely a of these lines. As seen above this implies that

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

which implies that $a \leq d$ according to Lemma 2.1.

On any of the other $q-1-a$ lines the number of zeroes of f is according to [5] at most the intersection number:

$$\begin{aligned}(D_h - a(\mathrm{div}(\mathbf{e}(m_1)))_0; (\mathrm{div}(\mathbf{e}(m_1)))_0) &=\\ (d\,V(\rho_3) + 2d\,V(\rho_4) - a\,V(\rho_1); a\,V(\rho_1)) &=\\ 2d - 2d\end{aligned}$$

calculated using the first intersection table of 2.4. The total number of zeros for f is therefore at most

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

This implies that the evaluation map

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

is injective and the dimension and the lower bound for the minimal distances of the toric code is greater than or equal to

$$(q-1)^2 - (q-1)2d = (q-1)(q-1-2d).$$

2.5.2. *Determination of a lower bound for the minimal distance in the situation of Theorem 1.5.* 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 $0 \neq f \in \mathrm{H}^0(X, O_X(D_h))$ and assume that f is zero along precisely a of these lines. As seen above this implies that

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

which implies that $a \leq d$ according to Lemma 2.1.

On any of the other $q-1-a$ lines the number of zeroes of f is according to [5] at most the intersection number:

$$\begin{aligned}(D_h - a(\mathrm{div}(\mathbf{e}(m_1)))_0; (\mathrm{div}(\mathbf{e}(m_1)))_0) &=\\ (d\,V(\rho_3) + f\,V(\rho_4) + \left(\frac{f+e}{2}\right) V(\rho_5) + e\,V(\rho_6) - a(V(\rho_1) + V(\rho_6)) &=\\ \frac{f+e}{2}\end{aligned}$$

calculated using the second intersection table of 2.4. The total number of zeros for f is therefore at most

$$a(q-1) + (q-1-a)\left(\frac{f+e}{2}\right) \leq d(q-1) + (q-1-d)\left(\frac{f+e}{2}\right).$$

This implies that the evaluation map

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

is injective and the dimension and the lower bound for the minimal distances of the toric code is greater than or equal to

$$(q-1)^2 - d(q-1) + (q-1-d)\left(\frac{f+e}{2}\right) = \left(q-1-\left(\frac{f+e}{2}\right)\right)(q-1-d).$$

References

[1] W. Fulton, "Introduction to Toric Varieties," *Annals of Mathematics Studies; no. 131*, Princeton University Press, 1993.

[2] W. Fulton, "Intersection theory" *Ergebnisse der Mathematik und uhrer Grenzgebiete, 3. Folge*, Springer Verlag, 1998.

[3] J. P. Hansen, "Toric Surfaces and Error-correcting codes," in *Coding theory, cryptography and related areas (Guanajuato, 1998)*, 132-142, Springer, Berlin, 2000

[4] J. P. Hansen, "Toric varieties Hirzebruch surfaces and error-correcting codes," *Appl. Algebra Engrg. Comm. Comput.* 13, 2002, 289–300

[5] Hansen, Søren Have, "Error-correcting codes from higher-dimensional varieties," *Finite Fields Appl.*; no 7, 2001, 531–552

[6] Joyner, jDavid, "Toric codes over finite fields," Preprint, Aug. 2002, `http://front.math.ucdavis.edu/math.AG/0208155`

[7] T. Oda, "Convex Bodies and Algebraic Geometry, An Introduction to the Theory of Toric Varieties," *Ergebnisse der Mathematik und uhrer Grenzgebiete, 3. Folge, Band 15*, Springer Verlag, 1985.

E-mail address: `matjph@mi.aau.dk`

DEPARTMENT OF MATHEMATICS, NY MUNKEGADE, 8000 AARHUS C, DENMARK