UNIVERSITY OF AARHUS
DEPARTMENT OF MATHEMATICS

ISSN: 1397–4076

# HIRZEBRUCH SURFACES AND ERROR-CORRECTING CODES

By Johan P. Hansen

Preprint Series No.: 6

August 2000

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

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

# HIRZEBRUCH SURFACES AND ERROR-CORRECTING CODES

JOHAN P. HANSEN

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 estimated using the cohomology and intersection theory of the underlying surfaces. In detail we will treat Hirzebruch surfaces.

## Contents

1. Toric codes 1
1.1. Codes from Hirzebruch toric surfaces 2
2. The method of toric varieties 3
2.1. Hirzebruch toric surfaces and their cohomology 4
2.2. Intersection theory on Hirzebruch toric surfaces 7
2.3. Determination of parameters 8
References 11

## 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 $\mathbf{e}(m)(P_{ij}) = (\xi^i)^{\lambda_1}(\xi^j)^{\lambda_2}$.

---

Document version: October 19, 1999.

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

*Key words and phrases.* Toric Varieties, Error-correcting Codes, Hirzebruch Surfaces.

**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

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

In [JPH] we presented a general method to obtain the dimension and a lower bound for the minimal distance of a toric code. In particular we obtained the following three results, where the second code is a subcode of the Reed Muller code on $\mathbb{P}^2$.

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

**Theorem 1.3.** *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 minimal distance greater or equal to $(q-1)^2 - d(q-1)$.*

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

1.1. **Codes from Hirzebruch toric surfaces.** The polytopes we are interested in are the polytopes with vertices $(0,0),(d,0),(d,e+rd)$ and $(0,e)$ as shown in figure 2. We obtain the the following theorem.

**Theorem 1.5.** *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 equal to $\#(M\cap\Box) = (d+1)(e+1) + r\frac{d(d+1)}{2}$ (the number of lattice points in $\Box$) and minimal distance greater or equal to $(q-1-d)(q-1-e)$.*

One should note that Theorem 1.4 is a special case when $r = 0$ and that the estimate for the minimal distance is independent of $r$. The estimate for the minimal distance is the best possible, in the case when $q = 5, d = e = 1, r = 2$ the true minimal distance is the same as the estimate.

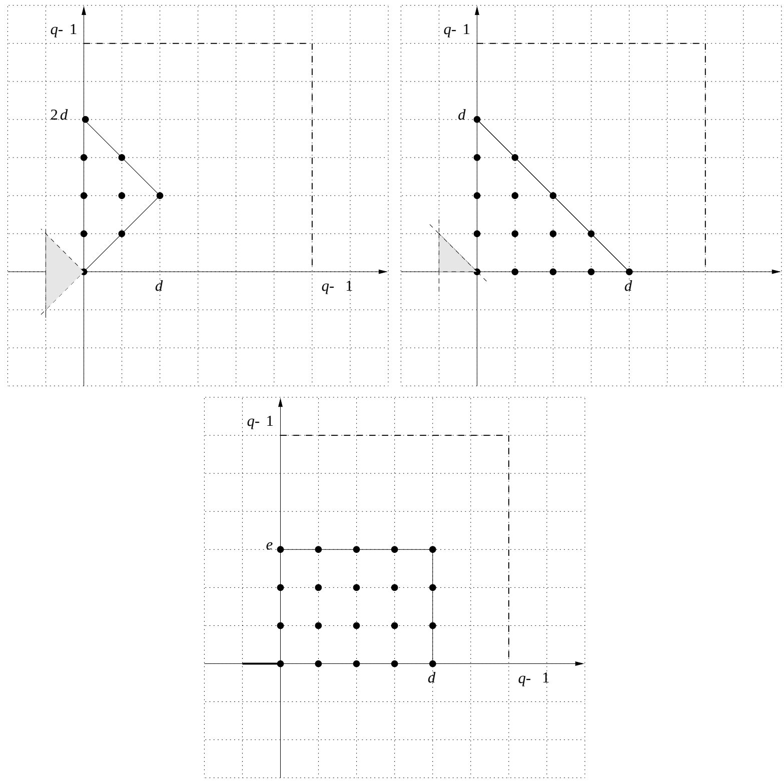


FIGURE 1. The polytope of Theorem 1.2 is the left triangle with vertices $(0,0),(d,d),(0,2d)$, the polytope of Theorem 1.3 is the right triangle with vertices $(0,0),(d,0),(0,d)$ and the polytope of Theorem 1.4 is the square with vertices $(0,0),(d,0),(d,e),(0,e)$.

In figure 5 and 6, 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 a lower bound for the relative minumal distance $\frac{\text{minimaldistance}}{\text{length}}$.

## 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 [F] and [O]. 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

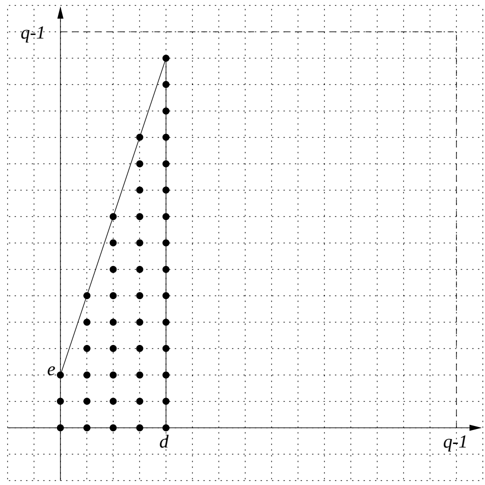


FIGURE 2. The polytope of Theorem 1.5 is the polytope with vertices $(0,0),(d,0),(d,e+rd),(0,e)$.

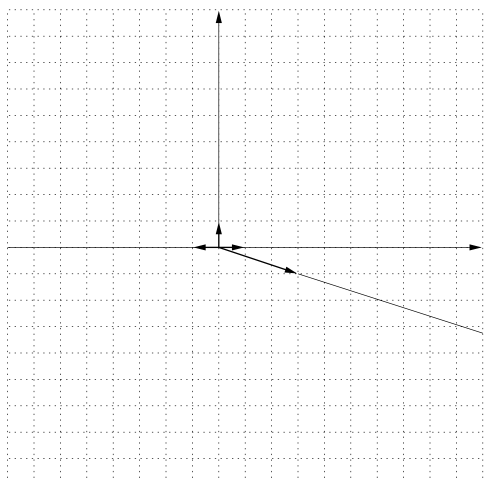

FIGURE 3. The normal fan of the polytope of Theorem 1.5 (see figure 2)

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. **Hirzebruch toric surfaces and their cohomology.** Let $M$ be an integer lattice $M \simeq \mathbb{Z}^2$. Let $N = \mathrm{Hom}_{\mathbb{Z}}(M,\mathbb{Z})$ be the dual lattice with canonical $\mathbb{Z}$ - bilinear pairing $<\ ,\ >: M \times N \to \mathbb{Z}$ 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 $<\ ,\ >: M_{\mathbb{R}} \times N_{\mathbb{R}} \to \mathbb{R}$.

Given a 2-dimensional integral convex polytope $\Box$ in $M_{\mathbb{R}}$. The support function $h_\Box : N_{\mathbb{R}} \to \mathbb{R}$ is defined as $h_\Box(n) := \inf\{< m, n > | m \in \Box\}$ and $\Box$ can be reconstructed:

$$\Box_h = \{m \in M| < m, n > \geq h(n) \quad \forall n \in N\}. \tag{2}$$

The support function $h_\Box$ 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 $h_\Box$ is linear on each cone. A fan is a collection $\Delta$ of strongly convex polyhedral cones in $N_{\mathbb{R}}$ such that every face of $\sigma \in \Delta$ is contained in $\Delta$ and $\sigma \cap \sigma' \in \Delta$ for all $\sigma, \sigma' \in \Delta$.

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

$$h_\Box(n) = < l_\sigma, n > \quad \forall n \in \sigma. \tag{3}$$

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 figure 1 are shown in figure 4.

Consider the polytope of Theorem 1.5, see figure 2 . The refined normal fan is show in figure 3. We have that $n(\rho_1) = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ , $n(\rho_2) = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $n(\rho_3) = \begin{pmatrix} -1 \\ 0 \end{pmatrix}$ and $n(\rho_4) = \begin{pmatrix} r \\ -1 \end{pmatrix}$. Let $\sigma_1$ be the cone generated by $n(\rho_1)$ and $n(\rho_2)$, $\sigma_2$ be the cone generated by $n(\rho_2)$ and $n(\rho_3)$ , $\sigma_3$ the cone generated by $n(\rho_3)$ and $n(\rho_4)$ and $\sigma_4$ the cone generated by $n(\rho_4)$ and $n(\rho_1)$. The support function is:

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

The 2-dimensional *algebraic torus* $T_N \simeq \overline{\mathbb{F}}_q^{\,*} \times \overline{\mathbb{F}}_q^{\,*}$ is defined by $T_N := \mathrm{Hom}_{\mathbb{Z}}(M, \overline{\mathbb{F}}_q^{\,*})$. The multiplicative character $\mathbf{e}(m)$, $m \in M$ is the homomorphism $\mathbf{e}(m) : T \to \overline{\mathbb{F}}_q^{\,*}$ defined by $\mathbf{e}(m)(t) = t(m)$ for

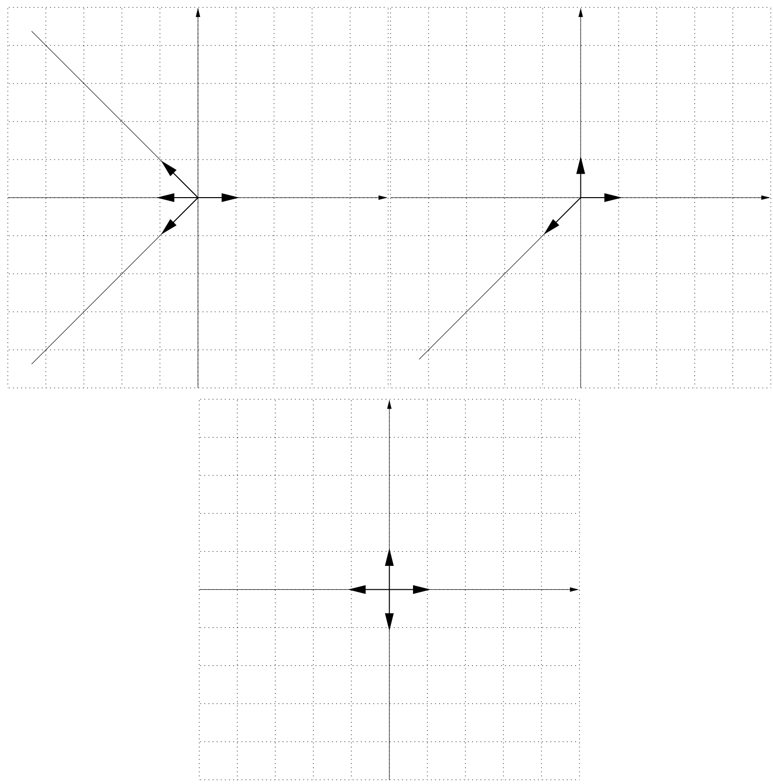

FIGURE 4. The normal fans af the polytopes in figure 1

$t \in T_N$. 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 $T_N \backsimeq \overline{\mathbb{F}}_q^{\,*} \times \overline{\mathbb{F}}_q^{\,*}$ 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 $\Delta$ of $\square$ is irreducible, non-singular and complete

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

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

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

If $\sigma, \tau \in \Delta$ and $\tau$ is a face of $\sigma$, then $U_\tau$ is an open subset of $U_\sigma$. Obviously $S_0 = M$ and $U_0 = T_N$ 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 $U_\sigma$ is $T_N$-stable. The orbits of this action is in one-to-one correspondance with $\Delta$. 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 $X_\square$. Define $V(\sigma)$ to be the closue of $\mathrm{orb}(\sigma)$ in $X_\square$.

A $\Delta$-linear support function $h$ gives rise to the Cartier divisor $D_h$. Let $\Delta(1)$ be the 1-dimensional cones in $\Delta$ 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 [O] Lemma 2.3 we have the lemma.

**Lemma 2.1.** *Let $h$ be a $\Delta$-linear support function with associated Cartier divisor $D_h$ and convex polytope $\square_h$ defined in (2). 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 $X_\square$ such that $\mathrm{div}(f) + D_h \geq 0$ has dimension $\#(M \cap \square_h)$ and has $\{\mathbf{e}(m) | m \in M \cap \square_h\}$ as a basis.*

In case of the polytope in Theorem 1.5, see figure 2, we have

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

and

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

2.2. **Intersection theory on Hirzebruch toric surfaces.** For a $\Delta$-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 is number is obtained in [O], Lemma 2.11. The cone $\rho$ 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 $l_\rho$ on $\rho$, 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 $\rho$. There exist 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

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

The divisor classes are represented by the 1-dimensional cones and the their table of intersections in case of the Hirzebruch surface obtained from the fan in figure3 is the following:

| $(V(\rho_i); V(\rho_j))$ | $V(\rho_1)$ | $V(\rho_2)$ | $V(\rho_3)$ | $V(\rho_4)$ |
|---|---|---|---|---|
| $V(\rho_1)$ | $-r$ | 1 | 0 | 1 |
| $V(\rho_2)$ | 1 | 0 | 1 | 0 |
| $V(\rho_3)$ | 0 | 1 | r | 1 |
| $V(\rho_4)$ | 1 | 0 | 1 | 0 |

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

**Lemma 2.3.** *Let $D_h$ be a Cartier divisor and let $\square_h$ be the polytope associated to $h$ , see (2). Then*

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

*where* $\mathrm{vol}_2$ *is the normalized Lesbesque-measure.*

*Proof.* see [O]. $\square$

### 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

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

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

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

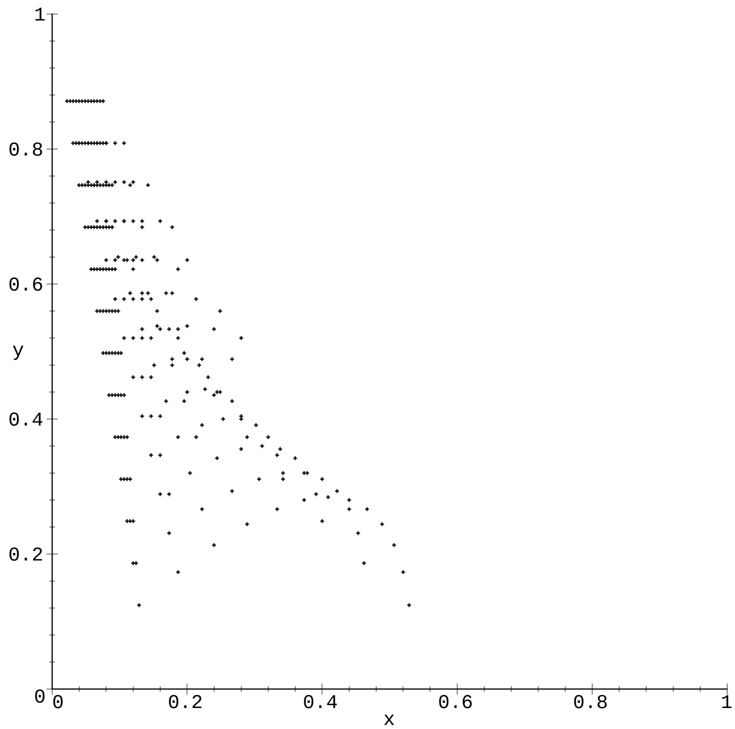


FIGURE 5. For all possible codes obtained by Theorem 1.5 in the case $q = 16$ a point is marked in the usual $xy$-diagram, where $x$ for a given code is the rate of the code, that is the fraction $\frac{\text{dimension}}{\text{length}}$, and $y$ is a lower bound for the relative minumal distance $\frac{\text{minimaldistance}}{\text{length}}$.

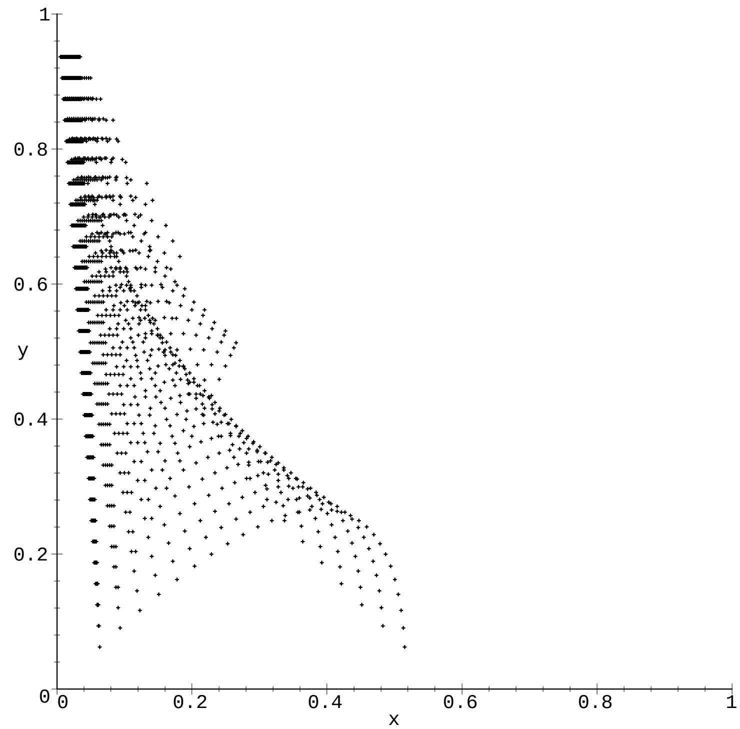


FIGURE 6. For all possible codes obtained by Theorem 1.5 in the case $q = 32$ a point is marked in the usual $xy$-diagram, where $x$ for a given code is the rate of the code, that is the fraction $\frac{\text{dimension}}{\text{length}}$, and $y$ is a lower bound for the relative minumal distance $\frac{\text{minimaldistance}}{\text{length}}$.

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 $X_\Box$ 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

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

In the cases of Theorem 1.5 this 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 [H] at most the intersection number:

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

which is equal to

$$(d\,V(\rho_3) + e\,V(\rho_4) - a(V(\rho_1) + V(\rho_4)); V(\rho_1) + V(\rho_4)) = e + (d-a)r$$

using the intersection table as $\mathrm{div}(\mathbf{e}(m_1)))_0 = V(\rho_1) + V(\rho_4)$.

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

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

This implies that the evaluation map

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

is injective and that the parameters of the toric code are as claimed.

## References


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

[JPH] J. P. Hansen, "Toric Surfaces and Error-correcting codes," *Preprint Series No. 9, 1998, University of Aarhus.*

[H] S. H. Hansen, "Error-correcting codes from higher-dimensional varieties," *Preprint Series No. 4, 1998, University of Aarhus.*

[O] 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