Toric Varieties Hirzebruch Surfaces and error-correcting Codes

Johan P. Hansen,
matjph@imf.au.dk
The Mathematical Institute, University of Aarhus, Denmark

IV International Algebraic Conference in Ukraine
Lviv, august 2003

Johan P. Hansen, *Toric Varieties Hirzebruch Surfaces and Error-Correcting Codes*, Applicable Algebra in Engineering, Communication and Computing, Springer-Verlag, Volume 13, Number 4/December 2002, Pages: 289 - 300

Resumé

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.

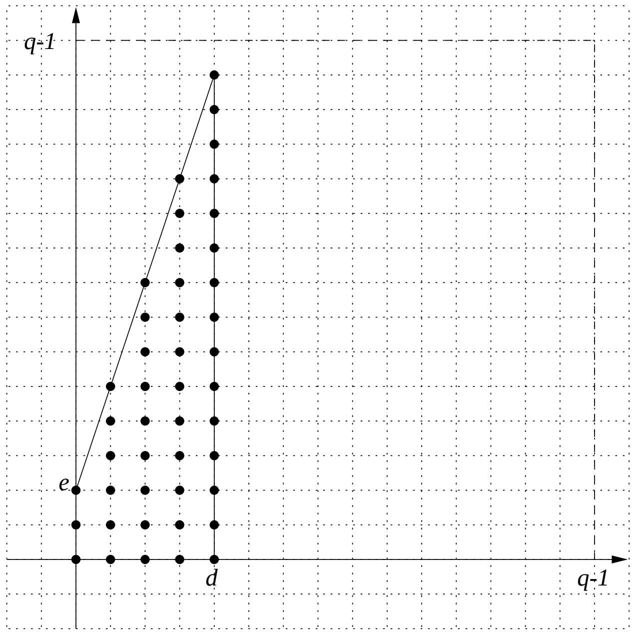
The dimension of the code is equal to the number of integral points in the given polytope and the minimum distance is determined using the cohomology and intersection theory of the underlying surfaces. In detail we treat Hirzebruch surfaces.

Construction of Toric codes

Let $M \simeq \mathbb{Z}^2$ be a $\mathbb{Z}$-module af rank 2 over the integers $\mathbb{Z}$.

Let $\square$ be a integral convex polytope in $M_{\mathbb{R}} = M \otimes_{\mathbb{Z}} \mathbb{R}$.

Example. Polytope with vertices $(0,0), (d,0), (d, e+rd), (0,e)$.



Toric Codes

$\xi \in \mathbb{F}_q$ a primitive element.

$P_{ij} = (\xi^i, \xi^j) \in \mathbb{F}_q{}^* \times \mathbb{F}_q{}^*, \quad i = 0, \dots, q-1; j = 0, \dots, q-1.$

m_1, m_2 a $\mathbb{Z}$-basis for M.

For $m = \lambda_1 m_1 + \lambda_2 m_2 \in M \cap \square$:

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

The toric code $C_\square$ is the linear code of length $n = (q-1)^2$ generated by:

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

The functions in the $\mathbb{F}_q$-vectorspace $L = \mathrm{Span}\{\mathbf{e}(m) | m \in M \cap \square\}$ are evaluated in the points P_{ij} on the torus $\mathbb{F}_q{}^* \times \mathbb{F}_q{}^*$:

$$\begin{aligned} \phi : L = \mathrm{Span}\{\mathbf{e}(m) | m \in M \cap \square\} &\longrightarrow \mathbb{F}^{(q-1)^2} \\ f &\mapsto (f(P_{ij})_{i=0,\dots,q-1; j=0,\dots,q-1}) \end{aligned}$$

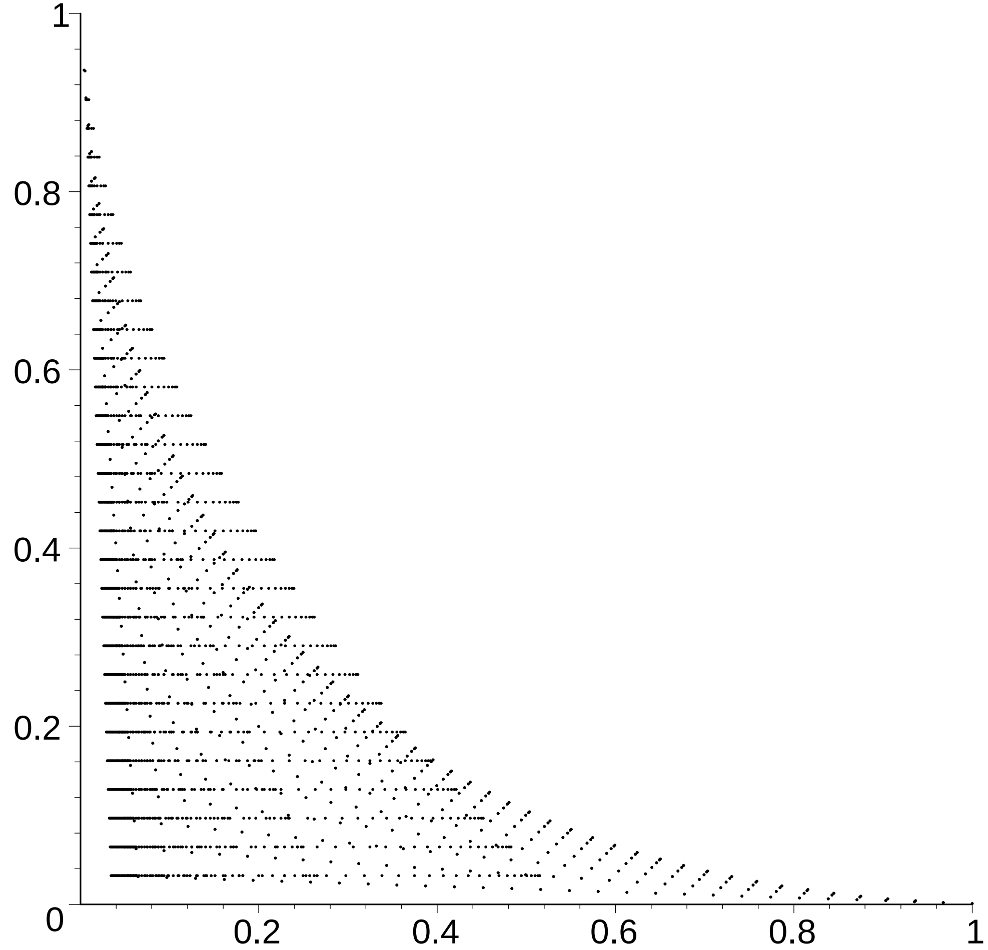
Theorem

Let $\Box$ be the polytope in $M_{\mathbb{R}}$ with vertices $(0,0),(d,0),(d,e+rd),(0,e)$ as above. Assume $d < q-1$, $e < q-1$ and $e+rd < q-1$.

The toric code $C_\Box$ has

- length $(q-1)^2$
- dimension $\#(M \cap \Box) = (d+1)(e+1) + r\frac{d(d+1)}{2}$ (the number of lattice points in $\Box$)
- minimal distance (the minimal number of nonzero entries in a codeword different from zero) $\mathrm{Min}\{(q-1-d)(q-1-e),(q-1)(q-1-e-rd)\}$.

Rate and relative minimal distance ($q = 32$)



$$x = \frac{\text{dimension}}{\text{length}}, y = \frac{\text{minimaldistance}}{\text{length}}, (q = 32)$$

Toric varieties - support functions

Let M be the lattice $M \simeq \mathbb{Z}^2$.

Let $N = \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Z})$ be the dual lattice with $\mathbb{Z}$ - bilinear parring

$$< \quad , \quad >: M \times N \to \mathbb{Z}.$$

Let $\Box$ be a 2-dimensional integral convex polytope in $M_{\mathbb{R}} = M \otimes_{\mathbb{Z}} \mathbb{R}$. Then there is a support function

$$h_{\Box} : N_{\mathbb{R}} = N \otimes_{\mathbb{Z}} \mathbb{R} \to \mathbb{R}$$

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

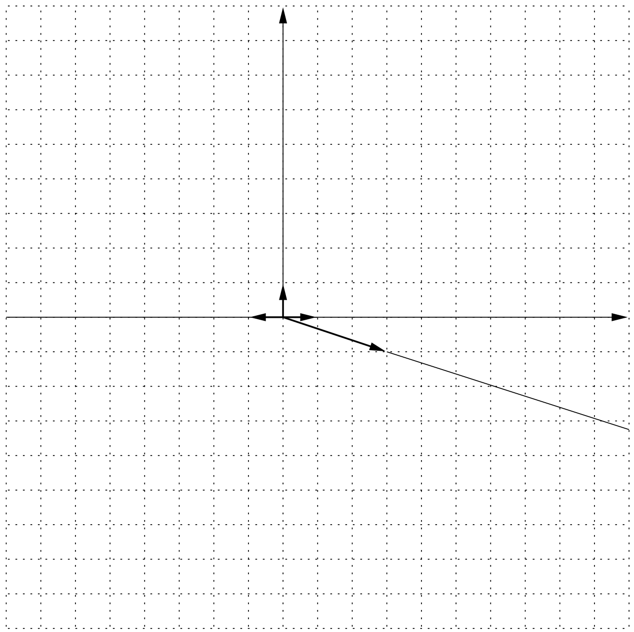
such that $\Box$ can be reconstructed as:

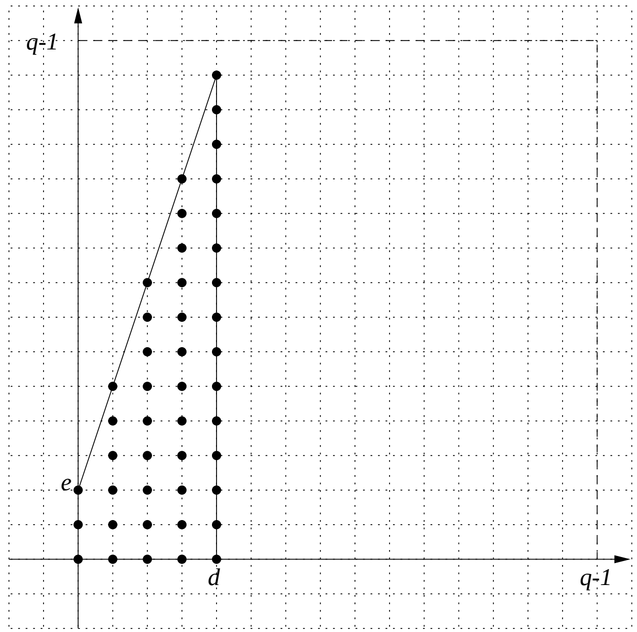
$$\Box_h = \{m \in M | \ < m, n > \geq \ h(n) \quad \forall n \in N\}.$$

The support function is piecewise linear: $N_{\mathbb{R}}$ is the union of finitely many polyhedral cones in $N_{\mathbb{R}}$ and $h_{\Box}$ is linear on each cone.

Hirzebruch surfaces - the toric surfaces asociated to the polyhedra in our example

N as union of polyhedral cones in our example





Generators for the 1-dimensional cones are:

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

.

Toric variety - definition

$T_N := \mathrm{Hom}_{\mathbb{Z}}(M, \overline{\mathbb{F}}_q^{\,*}) \backsimeq \overline{\mathbb{F}}_q^{\,*} \times \overline{\mathbb{F}}_q^{\,*}$ is a 2-dimensional algebraic torus.

$\mathbf{e}(m) : T \to \overline{\mathbb{F}}_q^{\,*}$, $m \in M$ defined as $\mathbf{e}(m)(t) = t(m)$ for $t \in T_N$ is a multiplicative character.

The toric surface $X_\square$ associated to $\square$ is

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

U_σ are the $\overline{\mathbb{F}}_q$-valued points on the affine scheme $\mathrm{Spec}(\overline{\mathbb{F}}_q[S_\sigma])$, that is

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

where S_σ is the additive subsemigroup of M

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

$X_\square$ is irreducible, (smooth) and complete.

T_N acts on $X_\Box$. On $u \in U_\sigma$ the element $t \in T_N$ acts in the following way:

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

For $\sigma \in \Delta$

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

ia a T_N orbit $X_\Box$. $V(\sigma)$ is defined to be the closure of $\text{orb}(\sigma)$ in $X_\Box$.

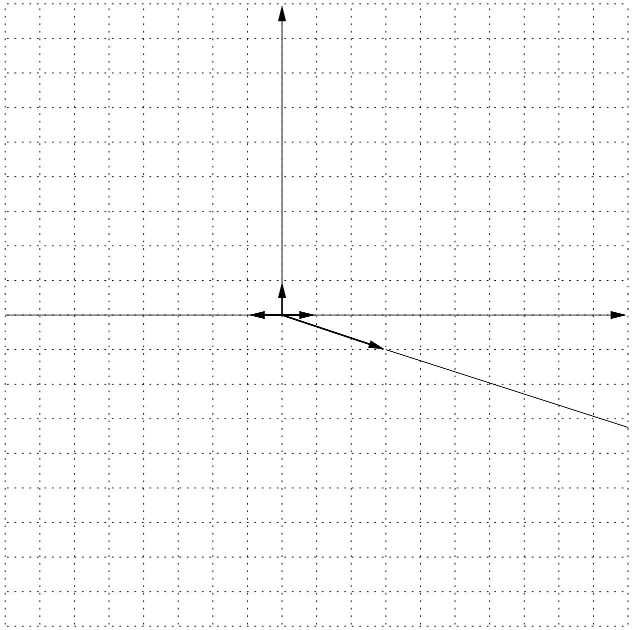
A Δ-linear support function h gives rise to a Cartier divisor D_h:

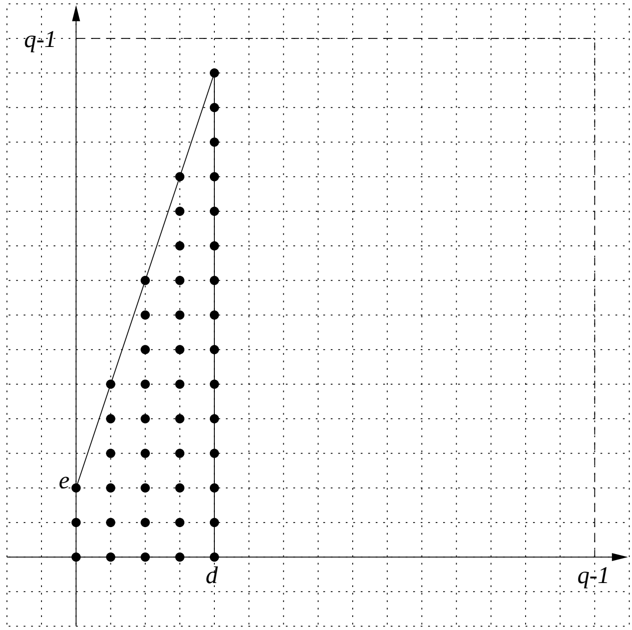
$$D_h := -\sum_{\rho \in \Delta(1)} h(n(\rho))\, V(\rho)$$

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

where $\Delta(1)$ are the 1-dimensional cones in Δ and $n(\rho)$ is a generator for the 1-dimensional cone ρ.

Lemma 1. *The vector space* $\mathrm{H}^0(X, O_X(D_h))$ *af globale sections of* $O_X(D_h)$ *has dimension* $\#(M \cap \Box_h)$ *and* $\{\mathbf{e}(m) | m \in M \cap \Box_h\}$ *is a basis.*





Generators for the 1-dimensional cones are:

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

.

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

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

Toric surfaces - Intersection theory

Let D_h be a Cartier divisor and let $\Box_h$ be the corresponding polytope. Then

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

where vol_2 is the normalized Lesbesgue measure.

I our example we get the intersection table

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

Result on Hirzebruch surfaces

Sætning 1. *Let* $\square$ *be the polytope in* $M_{\mathbb{R}}$ *with vertices* $(0,0),(d,0),(d,e+rd),(0,e)$. *Assume* $d < q-1$, $e < q-1$ *and* $e + rd < q-1$. *The toric code* $C_{\square}$ *has*

- *length* $(q-1)^2$
- *dimension* $\#(M \cap \square) = (d+1)(e+1) + r\frac{d(d+1)}{2}$ *(the number of lattice points in* $\square$*)*
- *minimal distance (the minimal number of nonzero entries in a codeword different from zero)* $\mathrm{Min}\{(q-1-d)(q-1-e),(q-1)(q-1-e-rd)\}$.

Bevis. For $t \in T \simeq \overline{\mathbb{F}}_q^{\,*} \times \overline{\mathbb{F}}_q^{\,*}$, the rationale functions i $\mathrm{H}^0(X, O_X(D_h))$ are evaluated

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

Let $\mathrm{H}^0(X, O_X(D_h))^{\mathrm{Frob}}$ be the Frobenius invariante functions in $\mathrm{H}^0(X, O_X(D_h))$ (functions that are $\mathbb{F}_q-$ linear combinations of $(\mathbf{e})(m)$).

Evaluating in all points in $T(\mathbb{F}_q)$ gives the code $C_\Box$:

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

og generators for the code are the images of the basis functions

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

Let $m_1 = (1, 0)$. The $\mathbb{F}_q$-rationale points on $T \simeq \overline{\mathbb{F}}_q^{\,*} \times \overline{\mathbb{F}}_q^{\,*}$ are on the $q-1$ lines on $X_\Box$ given by the equation $\prod_{\eta \in \mathbb{F}_q} (\mathbf{e}(m_1) - \eta) = 0$.

Let $0 \neq f \in \mathrm{H}^0(X, O_X(D_h))$ and assume that f is identically zero on precisely a of these lines. As $\mathbf{e}(m_1) - \eta$ and $\mathbf{e}(m_1)$ have the same pole-divisor, they have equivalent divisors of zeros:

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

Therefore

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

or equivalently

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

This implies that $a \leq d$ according to Lemma 1 on cohomology.

On any of the $q-1-a$ other lines the number of zeros for f is at most the intersection number:

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

This is determined using the intersection table and the observation $(\mathrm{div}(\mathbf{e}(m_1)))_0 = V(\rho_1) + rV(\rho_4)$. We get

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

As $0 \leq a \leq d$, we conclude that the totale number of (rational) zeros for f is at most

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

Therefore

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

and the dimension and the lower bound for the minimal distance as claimed in the theorem is obtained.

Now we will see that we have determined the true minimal distance. Let $b_1, \ldots, b_{e+rd} \in {\mathbb{F}_q}^*$ be pairwise distinct. The function

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

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

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

and gives a codeword of weight
$(q-1)^2 - (q-1)(e+rd) = (q-1)(q-1-(e+rd))$.

Let $a_1, \ldots, a_d \in {\mathbb{F}_q}^*$ be pairwise distinct and let $b_1, \ldots, b_e \in {\mathbb{F}_q}^*$ be pairwise distinct. The function

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

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

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

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

Litteratur

[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, “Hirzebruch surfaces and Error-correcting Codes,” *Preprint Series No. 6, 2000, University of Aarhus.*

*[5] J. P. Hansen, “Toric Varieties Hirzebruch Surfaces and Error-Correcting Codes,”*Applicable Algebra in Engineering, Communication and Computing, Springer-Verlag, Volume 13, Number 4/December 2002, Pages: 289 - 300

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

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

*[8] 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.