A Study on Toric Surfaces, Techniques and Code

Dr. Ashwani Kumar

Asst. Prof., Dronacharya P.G College of Education Rait, Kangra H.P.

Abstract: **We treat toric surfaces and their application to construction of error-correcting codes and determination of the parameters of the codes, surface veying and expanding the results. For any integral convex polytope in R2 there is an explicit construction of a unique error-correcting code of length (q − 1)2 over the finitefield Fq . 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 toric surface associated to the given polytope. Intersection theory on the toric surface will in two ways is applied to bind 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.**

Key words: **Toric, Surfaces, polytope and Code.**

I. TORIC CODES:

Let $M \approx Z^2$ be a free Z-module of rank 2 over the integers Z. Let Δ be an integral convex polytope in $M_R = M \otimes_Z R$, i.e. a compact convex polyhedron such that the vertices belong to M.

$e(m)(P_{ij}) = (\xi_i)^{\lambda 1} (\xi_j)^{\lambda 2}$.

Let MZ2 be a free Z-module of rank 2 over the integers Z. Let be a n integral convex polytope in $M_R = M \otimes_Z R$, i.e. a compact convex polyhedron such that the vertices belong to M .

Definition 1.1.

The toric code C Δ associated to Δ is linear length of code n = $(q - 1)^2$ generated by the vectors

{(e (m) (Pij)) i=0,...,q−1;j=0,...,q−1 | m ∈ M ∩Δ}……………(1)

Theorem 1.2. Let d be a positive integer and let be the polytope in M_R with vertices (0, 0), (d, 0), (0, d), see figure 1. Assume that d < q − 1. The toric code CΔ has length equal to $(q-1)^2$, dimension equal to #(M ∩ Δ) = (d+1)(d+2) (the number of lattice points in Δ) and the minimal distance is equal to (q − 1)2 − d(q − 1).

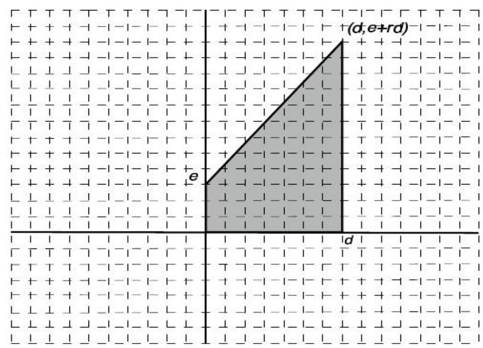
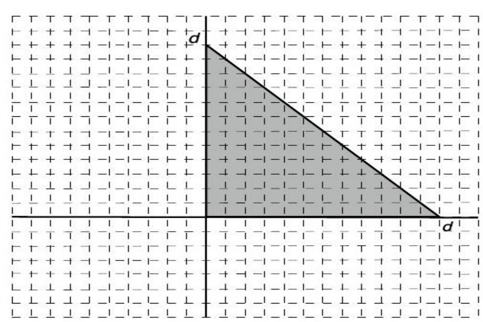


Figure 1. The convex polytope of Theorem 1.2 with vertices (0, 0), (d, 0), (0, d).

Theorem 1.3. Let d, e, r be positive integers and let Δ be the polytope in MR 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 CΔ has length equal to $(q-1)^2$, dimension equal to



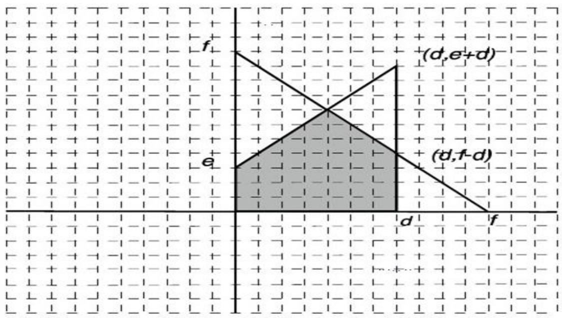


Figure 2. The convex polytope of Theorem 1.3 with vertices (0, 0), (d, 0), (d, e + rd), (0, e).

$\#(M \cap \Delta) = (d+1)(e+1) + r\frac{d(d+1)}{2}$ (the number of lattice points in Δ) and the minimal distance is equal to 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 Δ be the polytope in MR with vertices (0, 0), (d, 0), (0, 2d), see figure 3. Assume that 2d < q − 1. The toric code CΔ has length equal to $(q-1)^2$, dimension equal to #(M \ Δ) = d2 + 2d + 1 (the number of lattice points in Δ) and the minimal distance is greater or equal to

(q − 1)2 − 2d(q − 1) = (q − 1)(q − 1 − 2d).

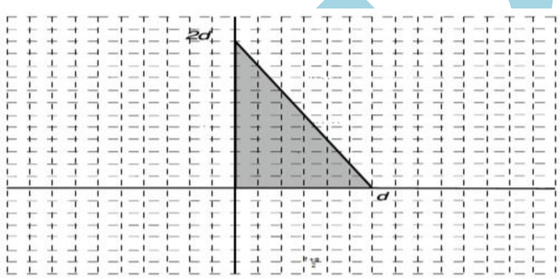


Figure 3. The convex polytope of Theorem 1.4 with vertices (0, 0), (d, 0), (0, 2d).

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

Figure 4.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 Δ has length equal to (q − 1)2, dimension equal to $\#(M \cap \Delta) = -1/2\, d2 - 1/4\, e^2 + 1/2\, e f - 1/4\, f^2 + fd + 1/2\, f + 1/2\, d + 1/2\, e + 1$ (the number of lattice points in Δ) and the minimal distance is greater than or equal to

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

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.

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

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 algebraicaly let T = (k ∗) be the n-dimensional torus. A toric variety is a compactification X of T with an action T × X → X of T on X that extends the natural action of T on itself.

The character group is
M = {χ: T → k ∗ |χ is a group homomorphism} and the group of 1-parameter subgroups is

N = {λ: k ∗ → T |λ is a group homomorphism}.
We remark, that M sponds to the character Z^n, where the n-tuple $m = (m_1, \ldots, m_n) \in Z^n$
corre- $e(m)(t_1, \ldots, t_n) = t^{m}{}_1, \cdots, t^{m}{}_n$ .n1

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

$$\lambda(u)(t) = (t^{u}{}_1, \ldots, t^{u}{}_n).$$

n1

For χ ∈ M and λ ∈ N there is an integer < χ, λ >, such that the composition χ ◦ λ: k ∗ → k ∗ is of the form

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

This gives a perfect pairing < −, − > M × N → Z and in the notation above, we have that
$< e(m), \lambda(u) > = m_1 u_1 + \cdots + m_n u_n$. Let $M_R = M \otimes_Z R$ and $N_R = N \otimes_Z R$ with canonical R - bilinear pairing < −, − >: $M_R \times N_R \to R$.

2.1. Convex polytopes and support functions. Fans, normal fans and refined normal fans. Given a n-dimensional integral convex polytope in M_R . The support function of the polytope is the function.

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 half line. Lattice and we obtain the refined normal fan. In the 2-dimensional case there is a method using continued fractions to obtain the refinement,

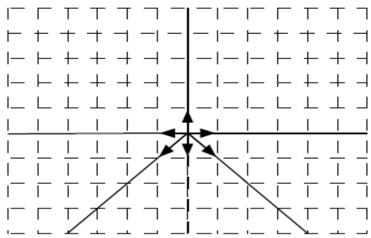


Figure 5.

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.

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 point's # in a convex polytope. In the 2-dimensional case Pick's formula gives that

$$\#\,\Delta = \mathrm{Vol}_2.(\Delta) + \frac{\mathrm{Perimeter}(\Delta)}{2} + 1$$

In calculating the perimeter one should take into account that the length of an edge of is one more that the number af lattice points lying strictly between the endpoints of the edge.

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

$$\#\,\Delta = \frac{2d.d}{2} + \frac{d+2d+d}{2} + 1 = 1 + 2d + d^2$$

$$\#\,\Delta = [g\ (e + d) - d^2/2 - (e - f + 2d)2 + \frac{(f+e+2d)^2}{2} + 1$$

$$\#(M \cap \Delta) = -1/2\, d2 - 1/4\, e^2 + 1/2\, e\, f - 1/4\, f^2 + fd + 1/2\, f + 1/2\, d + 1/2\, e + 1$$

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 letbe the polytope in MR 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

$$n(\rho)=\binom{1}{0},\ n(\rho2)=\binom{0}{1}\quad n(\rho3)=\binom{-1}{0},\ n(\rho4)=\binom{-2}{-1}$$

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 half-line.

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:

$$h\binom{n1}{n2} = \begin{cases} \binom{0}{0} & \binom{n1}{n2} \\ \binom{0}{d} & \binom{n1}{n2} \quad if \quad .\binom{n1}{n2} \in \sigma2 \cup \sigma3 \\ \binom{0}{2d} & \binom{n1}{n2} \end{cases}$$

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 Δ be the polytope in MR with vertices (0, 0), (d, f − d), $(\frac{f-e}{2}, \frac{f+e}{2})$, (0, e) see figure4. 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

$$n(\rho)=\binom{1}{0},\ n(\rho2)=\binom{0}{1}\quad n(\rho3)=\binom{-1}{0},\ n(\rho4)=\binom{-1}{-1}, n(\rho5)=\binom{0}{-1},\ n(\rho6)=\binom{-1}{-1}$$

Let σ1 be the cone by generated by $n(\rho_1)$ and $n(\rho_2)$, σ_2 be the cone generated $n(\rho_2)$ 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

$$h\binom{n1}{n2} = \begin{cases} \binom{d}{f-d} & .\binom{n1}{n2} \\ \begin{pmatrix} \frac{f-c}{2} \\ \frac{f+e}{2} \end{pmatrix} & .\binom{n1}{n2} \quad if \quad .\binom{n1}{n2} \in \sigma4, \sigma5, \sigma6 \\ \binom{0}{e} & . \binom{n1}{n2} \end{cases}$$

2.2. Toric varieties defined by fans associated to polytopes. The toric variety X associated to the refined normal fan Δ of is

$$X = \cup_{\sigma \in \Delta} U\sigma$$

where Uσ is the Fq - valued points of the affine scheme Spec(Fq [Sσ]), i.e

$$U_\sigma = \{u : S_\sigma \to Fq\ |u(0) = 1,$$

$u(m + m) = u(m)u(m)\ \forall m, m \in S_\sigma b$, where S_σ is the additive sub semi group of M

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

The toric variety X is irreducible, non-singular and complete,. If σ, τ ∈ Δ and τ is a face of σ, then U^{τ} is an open subset of Uσ . Obviously S^0 = M and $U^0 = T^N$ such that the algebraic torus T^N is an open subset of X.

T_N acts algebraically on X. On u ∈ U_σ the action of t ∈ T^N is obtained as

$(t_u)(m)$:= t(m)u(m) , m ∈ S_σ such that $t_u \in U_\sigma$ and U_σ is T^N -stable. The orbits of this action are in one-to-one correspondence with Δ. For each σ ∈ Δ let orb(σ) := {u : M ∩ σ → F_q |u is a group homomorphism}. Then orb(σ) is a T^N orbit in X . Define V (σ) to be the closure of orb (σ) in X

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 Δ (1) be the 1- dimensional cones in Δ then

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

$$Dm = \mathrm{div}\,(e(-m))\quad m \in M$$

Lemma 2.1. Let h be a Δ-linear support function with associated Cartier divisor Dh and convex polytope h defined in (2.1). The vector space H0 (X, O_X (Dh)) of global sections of O_X (Dh), i.e. rational functions f on X such that div(f) + Dh ≥ 0 has dimension #(M ∩ h) and has {e(m)|m ∈ M ∩ h } as a basis.

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

$$\dim H^0 (X, O_X (Dh)) = d/2 + 2d + 1 ,$$

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

$$= d\, V(\rho_3) + f\, V(\rho_4) + \frac{f+e}{2} + (\rho_5) + e\, V(\rho_6)$$

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

2.4. Intersection theory and the number of rational zeroes of a rational function. For a fixed line bundle L on X, given an effective divisor D such that L = O_X (D), the fundamental question to answer is: How many points from a fixed set P of rational points are in the support of D. This question is treated in general using intersection theory. 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 ρ ∈ Δ (1) we will determine the intersection number (Dh ; V (ρ)) between the Cartier divisor Dh and V (ρ)) = P_1 .The cone ρ is the common face of two 2-dimensional cones σ , σ ∈ Δ(2). Choose primitive elements n , n ∈ N such that

N' + n" ∈ Rρ

σ + Rρ = R≥0 n + Rρ
σ + Rρ = R≥0 n + Rρ

Lemma 2.2. For any lρ ∈ M , such that h coincides with lρ on ρ, let h = h − lρ .Then

(Dh ; V (ρ)) = −(h(n) + h(n).

n + n + an (ρ) = 0,

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

(V (ρ); V (ρ)) = a.

More generally the self-intersection number of a Cartier divisor Dh is obtained.

Lemma 2.3. Let Dh be a Cartier divisor and let h be the polytope associated to h .The (Dh ; Dh) = 2 vol.2 (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 (ρ1)	V (ρ2)	V (ρ3)	V (ρ4)
V (ρ1)	2	1	0	1
V (ρ2)	1	0	1	0
V (ρ3)	0	1	-2	1
V (ρ4)	1	0	1	0

Table 2.1 In the situation of Theorem 1.5 there are six 1-dimensional cones (2.1.3) and the Intersection table becomes

	V (ρ1)	V (ρ2)	V (ρ3)	V (ρ4)	V (ρ5)	V (ρ6)
V (ρ1)	-1	1	0	0	0	1
V (ρ2)	1	0	1	0	0	0
V (ρ3)	0	1	-1	1	0	0
V (ρ4)	0	0	1	-1	1	0
V (ρ5)	0	0	0	1	-1	1
V (ρ6)	1	0	0	0	1	-1

Table 2.2.

Determination of parameters. We start by exhibiting the toric codes as evaluation codes.

$$H (X, O_X (Dh))f \xrightarrow{**} C \subset (Fq *)\#T (Fq) \to (f (t))t \in T (Fq)$$

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

e(m) → (e(m)(t))t ∈T (Fq) as in (1.1). Fq × Fq belong to the q – 1

Let m1 = (1, 0). The Fq -rational points of T lines on X given by

$\eta \in Fq\ (e(m1) - \eta) = 0$.

Let $0 = f \in H^0(X, O_X(D_h))$ and assume that f is zero along precisely a of these lines. As e (m) − η and e(m1) have the same divisors of poles, they have equivalent divisors of zeroes, so

$div(e(m1)) - div(f) + Dh - a(div(e(m1)))0 \geq 0$
$div(f) + Dh - a(div(e(m1)))_0 \geq 0$
$f \in H^0(X, O_X(Dh - a(div(e(m1)))_0))$.

On any of the other q − 1 − a lines the number of zeroes of f is according to at most the intersection number:
$(Dh - a(div(e(m_1))_0 ; (div(e(m^1))_0)$.

Theorem 1.4. Let m1 = (1, 0). The Fq -rational points of T Fq × Fq belong to the q − 1 lines on X given by $\eta \in Fq\ (e(m1) - \eta) = 0$. Let $0 = f \in H_0(X, O_X(D_h))$ and assume that f is zero along precisely a of these lines. As seen above this implies that

$$f \in H^0(X, O_X(Dh - a(div(e(m_1))0)),$$

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 at most the intersection number:
$(Dh - a(div(e(m_1)))_0 ; (div(e(m_1))_0) =$
$(d\ V(\rho 3) + 2d\ V(\rho 4) - a\ V(\rho 1); a\ V(\rho 1)) = 2d - 2d$
calculated using the first intersection table of 2.4. The total number of zeros for f is therefore most
$a(q - 1) + (q - 1 - a)(2d - 2a) \leq (q - 1)2d$.
This implies that the evaluation map
$H^0(X, O_X(Dh))Frob \rightarrow C \subset (Fq*)\#T(Fq)$
$f \rightarrow (f(t))t \in T(Fq)$
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 Fq × Fq belong to Theorem 1.5. Let m1 = (1, 0). The Fq -rational points of T the q − 1 lines on X given by $\eta \in Fq\ (e(m1) - \eta) = 0$. Let $0 = f \in H^0(X, O_X(Dh))$ and assume that f is zero along precisely a of these lines. As seen above this implies that

$$f \in H^0(X, O_X(Dh - a(div(e(m1)))_0),$$

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 the intersection number:
$(Dh - a(div(e(m_1)))_0 ; (div(e(m1)))_0) =(d\ V(\rho_3) + f\ V(\rho_4) + \frac{f+e}{2} \rightarrow C \subset (Fq*)\#T(Fq)$.

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 Mathematic und uhrer Grenzgebiete, 3.

[3] Folge, Springer Verlag, 1998.

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

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

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

[7] Joyner,jDavid,"Toric codesover finitefields,"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 Mathematic und uhrer Grenzgebiete, 3. Folge, Band 15 , Springer Verlag, 1985.