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
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 uniquely 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.
Theorem 1.2. Let $d$ be a positive integer and let $\square$ be the polytope in $\mathbb{M}_\mathbb{R}$ with vertices $(0,0), (d,0), (0,d)$. 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 equal to $\min\{(q - 1 - d)(q - 1 - e), (q - 1)(q - 1 - e - rd)\}$.

Theorem 1.3. Let $d, e$ be positive integers such that $f > e$ and $f - e$ is even. Let $\square$ be the polytope in $\mathbb{M}_\mathbb{R}$ with vertices $(0,0), (d,e), (d,e + rd), (0,e)$. 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 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 integer and let $\square$ be the polytope in $\mathbb{M}_\mathbb{R}$ 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 $\mathbb{M}_\mathbb{R}$ with vertices $(0,0), (d,f - d), \left(\frac{4d}{f-e}, \frac{4d}{f-e}\right), (0,e)$, 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 $C_{\Box}$ has length equal to $(q - 1)^2$, dimension equal to

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

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

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 \( M \cong \mathbb{Z}^n \), where the \( n \)-tuple \( m = (m_1, \ldots, m_n) \in \mathbb{Z}^n \) corresponds to the character
\[
e(m)(t_1, \ldots, t_n) = t_1^{m_1} \cdots t_n^{m_n}.
\]
Also \( N \cong \mathbb{Z}^n \), 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 \( < e(m), \lambda(u) > = m_1u_1 + \cdots + m_nu_n \). 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 :
\[
\sqrt{h} = \{ m \in M | < m, n > \geq h(n) \ \forall n \in N \}.
\]

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 \( \Delta \) 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 \( \Delta \) 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
\[
h_{\square}(n) = < l_{\sigma}, n > \ \forall n \in \sigma.
\]

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 \( \{n_1, \ldots, n_s\} \) 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 $\#\Box$ in a convex polytope. In the 2-dimensional case Pick’s formula gives that

$$\#\Box = \text{vol}_2(\Box) + \frac{\text{Perimeter}(\Box)}{2} + 1.$$  

In calculating the perimeter one should take into account that the length of an edge of $\Box$ is one more that the number of 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

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

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

$$\#\Box = \left[ g(e + d) - d^2 - \frac{(e - t + 2d)^2}{4} \right] + \frac{f + d + e}{2} + 1$$

$$= -1/2 d^2 - 1/4 e^2 + 1/2 e f - 1/4 f^2 + f d + 1/2 f + 1/2 d + 1/2 e + 1$$

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 let $\Box$ be the polytope in $\mathbb{R}^2$ 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 $\sigma_1$ 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 corresponding support function is:

$$h_{\square}(n_1, n_2) = \begin{cases} \begin{pmatrix} 0 \\ 0 \\ d \\ 0 \\ 2d \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \\ n_1 \\ n_2 \\ n_2 \end{pmatrix} & \text{if } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_1, \\
\begin{pmatrix} 1 \\ 0 \\ 0 \\ 2d \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \\ n_2 \\ n_2 \end{pmatrix} & \text{if } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_2 \cup \sigma_3, \\
\begin{pmatrix} 0 \\ 2d \\ 0 \\ 2d \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \\ n_2 \\ n_2 \end{pmatrix} & \text{if } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_4. \end{cases}$$

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 $\mathbb{R}^2$ with vertices $(0,0)$, $(d,f-d)$, $(f-e,f+e)$, $(0,e)$ 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 $\sigma_1$ 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 $n(\rho_4)$, $\sigma_4$ the cone generated by $n(\rho_4)$ and $n(\rho_5)$, $\sigma_5$ the cone generated by $n(\rho_5)$ and $n(\rho_6)$ and $\sigma_6$ the cone
generated by $n(\rho_h)$ and $n(\rho_1)$. The corresponding support function is:
\[
h_{□}(n_1, n_2) = \begin{cases} 
0 & \text{if } n_1 \in \sigma_1, \\
0 & \text{if } n_1 \in \sigma_2, \\
d \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{if } n_1 \in \sigma_3, \\
f - d \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{if } n_1 \in \sigma_4 \cup \sigma_5, \\
t - d \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{if } n_1 \in \sigma_6., \\
0 & \text{if } n_1 \in \sigma_6.
\end{cases}
\]

2.2. Toric varieties defined by fans associated to polytopes. The toric variety $X_{□}$ associated to the refined normal fan $\Delta$ of $□$ is
\[
X_{□} = \bigcup_{\sigma \in \Delta} U_{\sigma}
\]
where $U_{\sigma}$ is the $\mathbb{F}_q$-valued points of the affine scheme $\text{Spec}(\mathbb{F}_q[S_\sigma])$, i.e.
\[
U_{\sigma} = \{ u : S_\sigma \rightarrow \mathbb{F}_q | u(0) = 1, u(m + m') = u(m)u(m') \forall m, m' \in S_\sigma \},
\]
where $S_\sigma$ is the additive subsemigroup of $M$
\[
S_\sigma = \{ m \in M | < m, y > \geq 0 \forall y \in \sigma \}.
\]
The toric variety $X_{□}$ is irreducible, non-singular and complete, see [7, Chapter 1]. 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 $X_{□}$.
\[T_N \text{ acts algebraically on } X_{□}.\]
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 correspondence with $\Delta$. For each $\sigma \in \Delta$ let
\[
\text{orb}(\sigma) := \{ u : M \cap \sigma \rightarrow \mathbb{F}_q^* | u \text{ is a group homomorphism} \}.
\]
Then $\text{orb}(\sigma)$ is a $T_N$ orbit in $X_{□}$. Define $V(\sigma)$ to be the closure of $\text{orb}(\sigma)$ in $X_{□}$.

2.3. Support functions and Cartier divisors on toric varieties. 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
\[
D_m = \text{div}(e(-m)) \quad m \in M.
\]
Following [7, 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 $□_h$ defined in (2.1). The vector space $H^0(X, O_X(D_h))$ of global sections of $O_X(D_h)$, i.e. rational functions $f$ on $X_{□}$ such that $\text{div}(f) + D_h \geq 0$ has dimension $\#(M \cap □_h)$ and has $\{ e(m) | m \in M \cap □_h \}$ 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

\[ \dim H^0(X, O_X(D_h)) = d^2 + 2d + 1, \]

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

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

2.4. Intersection theory and the number of rational zeroes of a rational function. For a fixed linebundle $L$ 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 in [5] using intersection theory, see [2]. Here we will apply the same methods when $X$ is a toric surface.

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 number is obtained in [7, Lemma 2.11]. The cone $\rho$ is the common face of two 2-dimensional cones $\sigma', \sigma'' \in \Delta(2)$. Choose primitive elements $n', n'' \in \mathbb{N}$ such that

\[ n' + n'' \in R \rho \]
\[ \sigma' + R \rho = R \geq 0 n' + R \rho \]
\[ \sigma'' + R \rho = R \geq 0 n'' + R \rho \]

**Lemma 2.2.** For any $l_\rho \in M$, such that $h$ coincides with $l_\rho$ on $\rho$, 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 $\rho$. 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 $\square_h$ be the polytope associated to $h$, see (2.1). Then

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

where $\text{vol}_2$ 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

\[
\begin{array}{c|cccc}
V(\rho_1) & V(\rho_2) & V(\rho_3) & V(\rho_4) \\
\hline
2 & 1 & 0 & 1 \\
1 & 0 & 1 & 0 \\
0 & 1 & -2 & 1 \\
1 & 0 & 1 & 0 \\
\end{array}
\]

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

\[
\begin{array}{c|ccccc}
V(\rho_1) & V(\rho_2) & V(\rho_3) & V(\rho_4) & V(\rho_5) & V(\rho_6) \\
\hline
-1 & 1 & 0 & 0 & 0 & 1 \\
1 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & -1 & 1 & 0 & 0 \\
0 & 0 & 1 & -1 & 1 & 0 \\
0 & 0 & 0 & 1 & -1 & 1 \\
1 & 0 & 0 & 0 & 1 & -1 \\
\end{array}
\]

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

For each \( t \in T \simeq \mathbb{F}_q^* \times \mathbb{F}_q^* \), we can evaluate the rational functions in \( H^0(X, O_X(D_h)) \)
\[
H^0(X, O_X(D_h)) \rightarrow \mathbb{F}_q^*
\]
\[
f \mapsto f(t).
\]

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 \( (e)(m) \) of Definition 1.1.

Evaluating in all points in \( T(\mathbb{F}_q) \) we obtain the code \( C_{\square} \):
\[
H^0(X, O_X(D_h))^{\text{Frob}} \rightarrow C_{\square} \subset (\mathbb{F}_q^*)^#T(\mathbb{F}_q)
\]
\[
f \mapsto (f(t))_{t \in T(\mathbb{F}_q)}
\]

and the generators of the code is obtained as the image of the basis:
\[
(e(m))_{t \in T(\mathbb{F}_q)}.
\]

as in (1.1).

Let \( m_1 = (1, 0) \). The \( \mathbb{F}_q \)-rational points of \( T \simeq \mathbb{F}_q^* \times \mathbb{F}_q^* \) belong to the \( q - 1 \) lines on \( X_{\square} \) given by \( \prod_{\eta \in \mathbb{F}_q}(e(m_1) - \eta) = 0 \). 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 \( e(m_1) - \eta \) and \( e(m_1) \) have the same divisors of poles, they have equivalent divisors of zeroes, so
\[
(\text{div}(e(m_1) - \eta))_0 \sim (\text{div}(e(m_1)))_0.
\]

Therefore
\[
\text{div}(f) + D_h - a(\text{div}(e(m_1)))_0 \geq 0
\]
or equivalently
\[
f \in H^0(X, O_X(D_h - a(\text{div}(e(m_1)))_0)).
\]

On any of the other \( q - 1 - a \) lines the number of zeroes of \( f \) is according to [5] at most the intersection number:
\[
(D_h - a(\text{div}(e(m_1))))_0; (\text{div}(e(m_1)))_0.
\]

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 $T \simeq \mathbb{F}_q^* \times \mathbb{F}_q^*$ belong to the $q - 1$ lines on $X^\square$ given by $\prod_{\eta \in \mathbb{F}_q} (e(m_1) - \eta) = 0$. 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 seen above this implies that

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

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 [5] at most the intersection number:

$$(D_h - a(\text{div}(e(m_1))))_0; (\text{div}(e(m_1)))_0 =$$

$$(d V(\rho_3) + 2d V(\rho_4) - a V(\rho_1); a V(\rho_1)) =$$

$$2d - 2d$$

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

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

This implies that the evaluation map

$$H^0(X, O_X(D_h))^{\text{Frob}} \rightarrow C^\square \subset (\mathbb{F}_q^*)^T(\mathbb{F}_q)$$

$$f \mapsto (f(t))_{t \in T(\mathbb{F}_q)}$$

is injective and the dimension and the lower bound for the minimal distance 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 $T \simeq \mathbb{F}_q^* \times \mathbb{F}_q^*$ belong to the $q - 1$ lines on $X^\square$ given by $\prod_{\eta \in \mathbb{F}_q} (e(m_1) - \eta) = 0$. 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 seen above this implies that

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

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 [5] at most the intersection number:

$$(D_h - a(\text{div}(e(m_1))))_0; (\text{div}(e(m_1)))_0 =$$

$$(d V(\rho_3) + f V(\rho_4) + \left(\frac{f + e}{2}\right) V(\rho_5) + e V(\rho_6) - a(V(\rho_1) + V(\rho_6)) =$$

$$\frac{f + e}{2}$$

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

$$H^0(X, O_X(D_h))^{\text{Frob}} \rightarrow C^\square \subset (\mathbb{F}_q^*)^T(\mathbb{F}_q)$$

$$f \mapsto (f(t))_{t \in T(\mathbb{F}_q)}$$
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


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

Department of Mathematics, Ny Munkegade, 8000 Aarhus C, Denmark