On the Structure of Generalized Toric Codes

Diego Ruano*

Abstract

Toric codes are obtained by evaluating rational functions of a nonsingular toric variety at the algebraic torus. One can extend toric codes to the so called generalized toric codes. This extension consists on evaluating elements of an arbitrary polynomial algebra at the algebraic torus instead of a linear combination of monomials whose exponents are rational points of a convex polytope. We study their multicyclic and metric structure, and we use them to express their dual and to estimate their minimum distance.

1 Introduction

J.P. Hansen introduced toric codes in [4]; these codes are algebraic-geometry codes at a toric variety over a finite field [2]. Algebraic-geometry codes are obtained by evaluating rational functions on a normal variety [12]. For a toric variety and a Cartier divisor D, toric codes are obtained by evaluating rational functions of $\mathcal{L}(D)$ at the points of the algebraic torus $T = (\mathbb{F}_q^*)^r$, where $\mathbb{F}_q$ is the finite field with q elements. Toric codes have been studied in [3, 4, 5, 6, 7, 8, 11]. In [6] there are some examples of toric codes with very good parameters.

We extend the definition of toric codes to the so called generalized toric codes. Generalized toric codes are obtained by evaluating polynomials at T as for toric codes but considering arbitrary polynomial algebras instead of $\mathcal{L}(D)$. We emphasize that toric codes are generalized toric codes. [3] claimed that toric codes are multicyclic and it was proved there for a toric code defined using a toric surface. We prove that generalized toric codes are multicyclic, and therefore toric codes coming from a convex polytope of arbitrary dimension. The aim of this paper is to study the multicyclic and metric structure of generalized toric codes. We compute the dual of a generalized toric code, which is a generalized toric code (the dual of a toric code is not a toric code in general). One cannot estimate its minimum distance using intersection theory [5, 11] but we provide here a method to estimate the minimum distance similar to the one in [8] studying its structure.

In the next section we have compiled some basics facts about toric codes and we also introduce the generalized toric codes. In section 3 we study the multicyclic structure of generalized toric codes. Finally in section 4 we study their metric structure which makes it possible to compute the dual of a generalized

*Partially supported by MEC MTM2004-00958 and FPU-AP2002-0087 and by Junta de CyL VA068/04, Spain. Address: Department of Algebra, Geometry and Topology, Faculty of Sciences, University of Valladolid, E-47005 Valladolid, Spain. E-mail: ruano@agt.uva.es

toric code. Furthermore we show that there are no self-dual generalized toric codes.

2 Toric Codes and Generalized Toric Codes

Let M be a lattice isomorphic to $\mathbb{Z}^r$ for some $r \in \mathbb{Z}$ and $M_{\mathbb{R}} = M \otimes \mathbb{R}$. A convex polytope is the same datum as a toric variety and Cartier divisor. Let P be an r-dimensional convex polytope in $M_{\mathbb{R}}$ and let us consider X_P and D_P the toric variety and the Cartier divisor defined by P. We may assume that X_P is non singular, in other case we refine the fan. Let $\mathcal{L}(D_P) = \mathrm{H}^0(X_P, \mathcal{O}(D_P))$ be the $\mathbb{F}_q$-vector space of rational functions f over X_P such that $\operatorname{div}(f) + D_P \succeq 0$.

The **toric code $\mathcal{C}_P^t$ associated to** P is the image of the $\mathbb{F}_q$-linear evaluation map

$$\begin{array}{rcl} \mathrm{ev} : \mathcal{L}(D_P) & \rightarrow & \mathbb{F}_q^n \\ f & \mapsto & (f(t))_{t \in T} \end{array}$$

where $T = (\mathbb{F}_q^*)^r$. Since we evaluate at $\#T$ points, $\mathcal{C}_P^t$ has length $n = (q-1)^r$. For a toric variety X_P one has that $\mathcal{L}(D_P)$ is the $\mathbb{F}_q$-vector space generated by the monomials with exponents in $P \cap M$

$$\mathcal{L}(D_P) = \langle \{ Y^u = Y_1^{u_1} \cdots Y_r^{u_r} \mid u \in P \cap M \} \rangle \subset \mathbb{F}_q[Y_1, \ldots, Y_r]$$

The dimension of the code and the kernel of ev are computed in [11]. Let $u \in P \cap M$ and $u = c_u + b_u$ where $c_u \in H = \{0, \ldots, q-2\} \times \cdots \times \{0, \ldots, q-2\}$ and $b_u \in ((q-1)\mathbb{Z})^r$. We will also denote $\overline{u} = c_u$. Let $\overline{P} = \{\overline{u} \mid u \in P \cap M\}$. The dimension of the code $\mathcal{C}_P^t$ is $k = \#\overline{P}$.

The minimum distance of a toric code $\mathcal{C}_P^t$ is estimated using intersection theory [4, 11]. Also, it can be estimated using a multivariate generalization of Vandermonde determinants on the generator matrix [8].

Let $U \subset H = \{0, \ldots, q-2\} \times \cdots \times \{0, \ldots, q-2\}$, $T = (\mathbb{F}_q^*)^r$ and $\mathbb{F}_q[U]$ the $\mathbb{F}_q$-vector space

$$\mathbb{F}_q[U] = \langle Y^u = Y_1^{u_1} \cdots Y_r^{u_r} \mid u = (u_1, \ldots, u_r) \in U \rangle \subset \mathbb{F}_q[Y_1, \ldots, Y_r]$$

The **Generalized toric code** $\mathcal{C}_U$ is the image of the $\mathbb{F}_q$-linear map

$$\begin{array}{rcl} \mathrm{ev} : \mathbb{F}_q[U] & \rightarrow & \mathbb{F}_q^n \\ f & \mapsto & (f(t))_{t \in T} \end{array}$$

where $n = \#T = (q-1)^r$. Some of the results for toric codes are also valid for generalized toric codes. Namely, the following result ensures that the map ev is injective and therefore the dimension of $\mathcal{C}_U$ is $k = \#U$.

Lemma 1. *Let $U \subset H$ and set*

$$f = \sum_{u \in U} \lambda_u Y^u, \quad \lambda_u \in \mathbb{F}_q$$

Then $(f(t))_{t \in T} = (0)_{t \in T}$ if and only if $\lambda_u = 0, \ \forall \ u \in H$.

The proof of the previous result if the same as the one of [11, lemma 3.2] for toric codes, and consequently we do not reproduce it. This is because the proof for toric codes shows that a nonzero polynomial which is a linear combination of monomials of H does not vanish completely on T.

We have defined the generalized toric codes for $U \subset H$ as the evaluation of $\mathbb{F}_q[U]$ at T. As we claimed in the previous section, this family of codes include the ones obtained evaluating polynomials of an arbitrary subalgebra of $\mathbb{F}_q[Y_1, \ldots, Y_r]$ at T. The following result shows this fact.

Proposition 2. *Let $V \subset \mathbb{Z}^r$, $\mathbb{F}_q[V] = \langle Y^v \mid v \in V \rangle$ and $\mathcal{C}_V$ the linear code defined by the image of the evaluation map* ev *at T*

$$\begin{array}{rcl} \mathrm{ev} : \mathbb{F}_q[V] & \to & \mathbb{F}_q^n \\ f & \mapsto & (f(t))_{t \in T} \end{array}$$

Let $v \in \mathbb{Z}^r$, where we write $v = c_v + b_v$ with $c_v \in H$ and $b_v \in ((q-1)\mathbb{Z})^r$. We also denote it by $\overline{v} = c_v$. Then $\mathcal{C}_U = \mathcal{C}_V$, where $U = \overline{V} \subset H$.

Proof. Let $f = \sum_{v \in V} \lambda_v Y^v \in \mathbb{F}_q[V]$ and $t \in T$. One has that

$$f(t) = \sum_{v \in V} \lambda_v t^{c_v + b_v} = \sum_{v \in V} \lambda_v t^{c_v}$$

And the result holds. □

Let P be a convex polytope in $M_{\mathbb{R}}$, by the previous proposition it follows that $\mathcal{C}_P^t = \mathcal{C}_U$ with $U = \overline{P}$. Therefore all the results for generalized toric codes are valid in particular for toric codes.

3 Multicyclic Structure of Generalized Toric Codes

Multicyclic codes are those whose words are invariant under certain cyclic permutations; they can also be understood as ideals in a certain polynomial algebra. [3] proves that a toric code defined using a plane convex polytope ($r = 2$) is multicyclic by representing the words of the code by matrices. The proof is hard to extend for arbitrary dimension because one should consider r-dimensional arrays, although the result was claimed there for any r. We represent the words of the code by polynomials in order to prove that a generalized toric code of arbitrary dimension is multicyclic.

Let $\mathcal{C} \subset \mathbb{F}_q^n$ be a linear code. We call $\mathcal{C}$ a **cyclic code** if $c = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ implies that $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in \mathcal{C}$.

Let $\mathbb{F}_q[X]_{\leq n-1}$ be the $\mathbb{F}_q$-vector space of polynomials of degree lower than n and A the quotient ring $\mathbb{F}_q[X]/(X^n - 1)$. Since $\mathbb{F}_q^n$, $\mathbb{F}_q[X]_{\leq n-1}$ and A are vector spaces over the same field with the same finite dimension n they are isomorphic. Then we consider the isomorphisms

$$\mathbb{F}_q^n \simeq \mathbb{F}_q[X]_{\leq n-1} \simeq \mathbb{F}_q[X]/(X^n - 1)$$

and for abbreviation one identifies $(c_0, c_1, \ldots, c_{n-1})$, the polynomial $c_0 + c_1 X + \cdots + c_{n-1} X^{n-1}$ and the class $c_0 + c_1 X + \cdots + c_{n-1} X^{n-1} + (X^n - 1)$. In practice one uses the most convenient notation when no confusion can arise. A code in the polynomial algebra A is cyclic if and only if it is an ideal in A.

Cyclic codes have been deeply studied and used for real applications [9]. A natural extension of cyclic codes are the so called multicyclic codes. A code $\mathcal{C} \subset A = \mathbb{F}_q[X_1, \dots, X_r]/(X_1^{N_1} - 1, \dots, X_r^{N_r} - 1)$ is **multicyclic or r-D cyclic** if it is an ideal in A, with $N_1, \dots, N_r \in \mathbb{N}$. Let $\mathbb{F}_q[X_1, \dots, X_r]_{\leq (N_1-1, \dots, N_r-1)}$ be the $\mathbb{F}_q$-vector space of polynomials in the variables $X_1, \dots, X_r$ of degree lower than N_i in each variable X_i for all i. In particular, a cyclic code is a 1-cyclic code. In the same way as for the cyclic case one can consider the following isomorphisms of vector spaces

$$\mathbb{F}_q^n \simeq \mathbb{F}_q[X_1, \dots, X_r]_{\leq (N_1-1, \dots, N_r-1)} \simeq A \tag{1}$$

where $n = N_1 \cdots N_r$ and we can identify its elements.

Let $\mathcal{C}_U$ be the generalized toric with $U \subset H$. Set α a primitive element of $\mathbb{F}_q$, i.e. $\mathbb{F}_q^* = \{\alpha^0, \alpha^1, \dots, \alpha^{q-2}\}$ and therefore $T = \{\alpha^i = (\alpha^{i_1}, \dots, \alpha^{i_r}) \mid i \in H\}$. Then $\mathcal{C}_U$ is the vector subspace of $\mathbb{F}_q^n$ generated by $\{(Y^u(\alpha^i))_{i \in H} \mid u \in U\}$, where $Y^u(\alpha^i) = \alpha^{\langle u,i \rangle} = \alpha^{u_1 i_1 + \cdots + u_n i_n}$. In order to study the multicyclic structure we shall use the previous isomorphism, and we denote the code $\mathcal{C}_U$ in A as $\mathcal{C}_U^A$. Namely, we represent (with multi-index notation for X^i)

$$(\alpha^{\langle u,i \rangle})_{i \in H} \in \mathcal{C}_U \quad \text{by} \quad \sum_{i \in H} \alpha^{\langle u,i \rangle} X^i \in \mathcal{C}_U^A$$

Let $U \subset H$ and $A = \mathbb{F}_q[X_1, \dots, X_r]/(X_1^{q-1} - 1, \dots, X_r^{q-1} - 1)$. The code $\mathcal{C}_U^A \subset A$ which is identified with $\mathcal{C}_U \subset \mathbb{F}_q^n$ under the isomorphism (1) is

$$\mathcal{C}_U^A = \{\sum_{u \in U} \lambda_u \sum_{i \in H} \alpha^{\langle u,i \rangle} X^i \mid \lambda_u \in \mathbb{F}_q\} \subset A$$

Proposition 3. *Let $U \subset H = (\{0, \dots, q-2\})^r$, $\mathcal{C}_U^A$ is an r-D cyclic code with $N_1 = q-1$, $\dots$, $N_r = q-1$.*

Proof. Let $u \in U$, $\sum_{i \in H} \alpha^{\langle u,i \rangle} X^i \in \mathcal{C}_U^A$.

$X^a \sum_{i \in H} \alpha^{\langle u,i \rangle} X^i = \sum_{i \in H} \alpha^{u_1(i_1 - a_1) + \cdots + u_r(i_r - a_r)} X^i = \alpha^{-\langle u,a \rangle} \sum_{i \in H} \alpha^{\langle u,i \rangle} X^i$. And the result holds due to the linearity of $\mathcal{C}_U^A$. □

In addition to the product of polynomials in $\mathbb{F}_q[H]$ which we denote by $\cdot$, $Y^u \cdot Y^v = Y^{\overline{u+v}}$, we consider the multiplicative structure of A in $\mathbb{F}_q[H]$. The product of A is given in the basis $\{X^i\}_{i \in H}$ by $X^i * X^j = X^{i+j}$. The following result pulls back the structure of A in $\mathbb{F}_q[H]$ which will be used in theorem 5.

Proposition 4. *Let us denote* $\mathrm{ev}^{-1}(X^i)$ *by* X^i *in* $\mathbb{F}_q[H]$*, then*

$$X^i * Y^u = \alpha^{-\langle u,i \rangle} Y^u$$

$$Y^u * Y^v = \begin{cases} 0 & \text{if } u \neq v \\ (-1)^r Y^u & \text{if } u = v \end{cases}$$

Proof. By the following isomorphisms considered above

$$\begin{array}{ccccc} \mathbb{F}_q[H] & \longleftrightarrow & \mathbb{F}_q^n & \longleftrightarrow & A \\ Y^u & \mapsto & (\alpha^{\langle u,i \rangle})_{i \in H} & \mapsto & \sum_{i \in H} \alpha^{\langle u,i \rangle} X^i \end{array} \tag{2}$$

one has that

$X^i * Y^u = X^i * \sum_{j \in H} \alpha^{\langle u,j \rangle} X^j = \alpha^{-\langle u,i \rangle} Y^u$, by proposition 3.

$$Y^u * Y^v = \sum_{i\in H} \alpha^{\langle u,i\rangle} X^i * Y^v = \sum_{i\in H} \alpha^{\langle u-v,i\rangle} Y^v =$$

$$= \left\{ \begin{array}{ll} \sum_{i\in H} \alpha^{\langle u-v,i\rangle} Y^v = \frac{q(q-1)}{2}(\sup(u-v)) = 0 & \text{if } u \neq v \\ \sum_{i\in H} Y^u = (-1)^r Y^u & \text{if } u = v \end{array} \right.$$

where $\sup(u-v)$ is the number of nonzero coordinates of $u-v$. □

The following result proves that any linear code over $\mathbb{F}_q$ which is r-D cyclic with $N_1 = q-1, \ldots, N_r = q-1$, is a generalized toric code. That is, the ideals of $A = \mathbb{F}_q[X_1, \ldots, X_r]/(X_1^{q-1} - 1, \ldots, X_r^{q-1} - 1)$ are generalized toric codes. Therefore the generalized toric codes and the r-D cyclic codes with $N_1 = q-1$, …, $N_r = q-1$ are the same family of codes.

Theorem 5. *Let $J \subset \mathbb{F}_q[X_1, \ldots, X_r]/(X_1^{q-1} - 1, \ldots, X_r^{q-1} - 1)$ an ideal, then there exists $U \subset H$ such that $J = \mathcal{C}_U^A$.*

Proof.

Since A is isomorphic to $\mathbb{F}_q[H]$ by (2) and $\{Y^u \mid u \in H\}$ is a basis of $\mathbb{F}_q[H]$, we have that $\{\text{ev}(Y^u) \mid u \in H\}$ is a basis of A, where $\text{ev}(Y^u) = \sum_{i\in H} \alpha^{\langle u,i\rangle} X^i \in A$.

Let $\sum_{v\in H} \lambda_v \text{ev}(Y^v) \in J$ and let $u \in H$; according to proposition 4 we have that $\text{ev}(Y^u) \sum_{v\in H} \lambda_v \text{ev}(Y^v) = (-1)^r \lambda_u ev(Y^u) \in J$. Therefore $\text{ev}(Y^u) \in J$ if $\lambda_u \neq 0$. We now apply this argument again, for every generator of J and u in H, to obtain U such that $J = (\text{ev}(Y^u) \mid u \in U)$. □

4 Metric Structure of Generalized Toric Codes

In this section we study the metric structure given by the bilinear form which defines the dual of a linear code, $\langle x, y\rangle = \sum_{i=1}^n x_i y_i$ with $x, y \in \mathbb{F}_q^n$. The following result considers the metric structure of a generalized toric code $\mathcal{C}_U \subset \mathbb{F}_q^n$ in $\mathbb{F}_q[H]$ and computes its dual.

Theorem 6. *With the above notations set $u, v \in H$, one has that*

$$\langle \text{ev}(Y^u), \text{ev}(Y^v)\rangle = \left\{ \begin{array}{ll} 0 & \text{if } \overline{u+v} \neq 0 \\ (-1)^r & \text{if } \overline{u+v} = 0 \end{array} \right.$$

Let $u \in H$, $u' = \overline{-u}$ with $\overline{u}$ as in proposition 2 and $U' = \{u' \mid u \in U\}$, $\#U = \#U'$. Let $U \subset H$ and $U^\perp = H \setminus U' = (H \setminus U)'$, then the dual code of $\mathcal{C}_U$ is $\mathcal{C}_U^\perp = \mathcal{C}_{U^\perp}$

Proof. Let $u, v \in H$, then one has that $\langle (\alpha^{\langle u,i\rangle})_{i\in H}, (\alpha^{\langle v,i\rangle})_{i\in H}\rangle = \sum_{i\in H} \alpha^{\langle u+v,i\rangle}$

$$\sum_{i\in H} \alpha^{\langle u+v,i\rangle} = \sum_{i\in H} \alpha^{\langle \overline{u+v},i\rangle} = \left\{ \begin{array}{ll} \frac{q(q-1)}{2}(\sup(\overline{u+v})) = 0 & \text{if } \overline{u+v} \neq 0 \\ \sum_{i\in H} 1 = (-1)^r & \text{if } \overline{u+v} = 0 \end{array} \right.$$

where $\sup(\overline{u+v})$ is the number of nonzero coordinates of $\overline{u+v}$.

Then $\langle \text{ev}(Y^u), \text{ev}(Y^v)\rangle = 0$ for $u \in U$, $v \in U^\perp$ since $\overline{u+v} \neq 0$. On account of the dimension of $\mathbb{F}_q[U]$ and $\mathbb{F}_q[U^\perp]$ and the linearity of the codes the proof is completed. □

The previous result shows that the dual of a toric code $\mathcal{C}_{P_1}$ is a toric code only when there is a convex polytope P_2 such that $\overline{P_1}^\perp = \overline{P_2}$. However the dual of a generalized toric code is a generalized toric code.

Remark 7. The main results of this paper were published without proofs in [10]. Later, a similar result to theorem 6 has been obtained independently in [1].

Summarizing, the matrix M of the evaluation map $\mathrm{ev} : \mathbb{F}_q[H] \to \mathbb{F}_q^n$ is

$$M = \begin{pmatrix} \alpha^{\langle u_1,i_1\rangle} & \alpha^{\langle u_1,i_2\rangle} & \dots & \dots & \alpha^{\langle u_1,i_n\rangle} \\ \alpha^{\langle u_2,i_1\rangle} & \alpha^{\langle u_2,i_2\rangle} & \dots & \dots & \alpha^{\langle u_2,i_n\rangle} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha^{\langle u_n,i_1\rangle} & \alpha^{\langle u_n,i_2\rangle} & \dots & \dots & \alpha^{\langle u_n,i_n\rangle} \end{pmatrix}$$

where $\{u_1, \dots, u_n\} = \{i_1, \dots, i_n\} = H$ and if moreover $u_j = i_j$ then M is a symmetric matrix, therefore we assume $u_j = i_j \ \forall j = 1, \dots n$.

We have thus proved that a generator matrix of the code $\mathcal{C}_U$ with $U \subset H$, $k = \#U$, is the $(k \times n)$-matrix $M(U)$ consisting in the k rows $\alpha^{\langle u,i_1\rangle}, \dots, \alpha^{\langle u,i_n\rangle}$ of M with $u \in U$ and a control matrix of $\mathcal{C}_U$ is the $(n-k \times n)$-matrix $M(U^\perp)$ consisting of the $n-k$ rows $\alpha^{\langle u,i_1\rangle}, \dots, \alpha^{\langle u,i_n\rangle}$ of M with $u \in U^\perp$. Or equivalently the transpose of a control matrix is the $(n \times n-k)$-matrix consisting of the $n-k$ columns $\alpha^{\langle u_1,i\rangle}, \dots, \alpha^{\langle u_n,i\rangle}$ of M with $i \in U^\perp$ since we assume $u_j = i_j \ \forall j = 1, \dots n$.

The knowledge of the dual of a generalized toric code provides the following result to compute the minimum distance. This proposition is an analogue of [8, Proposition 2.1] for toric codes whose proof remains valid for generalized toric codes. Using the control matrix one simplifies the computations with respect to the generator matrix.

Proposition 8. *Let $U \subset H$ and set d an integer greater than or equal to 1. Suppose that $\forall \ S \subset H$ with $\#S = d-1$ exists $V \subset U^\perp$ with $\#V = d-1$ such that the square submatrix $M(S,V)$ of M has nonzero determinant then $d(\mathcal{C}_U) \geq d$, where $M(S,V)$ is the submatrix of M corresponding to the rows of S and columns of V, i.e. $M(S,V) = (\alpha^{\langle u_S, i_V\rangle})_{u_S \in S, i_V \in V}$.*

Proof. The minimum distance of a linear code is greater than or equal to d if any $d-1$ columns of a control matrix are linearly independent. A control matrix of $\mathcal{C}_U$ is $M(U^\perp)$. Therefore the minimum distance of $\mathcal{C}_U$ is greater than or equal to d if any $d-1$ columns of $M(U^\perp)$ are linearly independent that is equivalent to the fact that exists a square submatrix of $M(U^\perp)$ with size $d-1$ and nonzero determinant. □

Let $\sigma(u) = u'$, and since $\sigma^2 = \mathrm{Id}$, one has that σ is an involution. Moreover we can order the elements of H in such a way that the matrix of the involution σ has a characteristic form, as follows. By Theorem 6 we have that $\langle \mathrm{ev}(Y^u), \mathrm{ev}(Y^v)\rangle = 0$ if and only if $\overline{u+v} \neq 0$. We consider first the elements $u \in H$ such that $\sigma(u) = u' = u$, then $\overline{u+u} = 0$ and we have $\langle \mathrm{ev}(Y^u), \mathrm{ev}(Y^u)\rangle = (-1)^r$ and $\langle \mathrm{ev}(Y^u), \mathrm{ev}(Y^v)\rangle = 0$ for all $v \in H \setminus \{u\}$. Then, we consider in H the pairs of elements u and $\sigma(u) = u'$, with $u \neq \sigma(u)$, then $\overline{u+u'} = 0$ and we have $\langle \mathrm{ev}(Y^u), \mathrm{ev}(Y^{u'})\rangle = (-1)^r$, $\langle \mathrm{ev}(Y^u), \mathrm{ev}(Y^v)\rangle = 0$ for all $v \in H \setminus \{u'\}$ and $\langle \mathrm{ev}(Y^{u'}), \mathrm{ev}(Y^v)\rangle = 0$ for all $v \in H \setminus \{u\}$. Let $H = \{u_1, \dots, u_n\}$ ordered in the previous way. One has that the matrix I_σ of the involution σ is

$$(-1)^r I_\sigma = \begin{pmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & & 0 & 1 & & & \\ & & & 1 & 0 & & & \\ & & & & & \ddots & & \\ & & & & & & 1 & 0 \\ & & & & & & 0 & 1 \end{pmatrix}$$

and therefore $M^t M = (-1)^r I_\sigma$, and since $M^t = M$ one has that

$$M^{-1} = (-1)^r I_\sigma M$$

With these notations, the number of 1's in the main diagonal of the matrix $(-1)^r I_\sigma$ is established by our next proposition. Also, we deduce that there are no self-dual generalized toric codes.

Proposition 9. *Let σ be the involution $\sigma(u) = u'$ in H. The number of elements $u \in H$ such that $\sigma(u) = u$ is 2^r if q is odd and 1 if q is even. Moreover, there are no self-dual generalized toric codes.*

Proof. Let $u = (u_1, \ldots, u_r)$ in H, $\sigma(u) = u$ if and only if $2u_i = 0 \mod (q-1)$, for $i = 1, \ldots, r$.

If q is odd, then $2u_i = 0 \mod (q-1)$ if and only if u_i is equal to 0 or $(q-1)/2$. Therefore there are 2^r elements in H with $\sigma(u) = u$. We turn to the case q even, then $q-1$ is odd and the only element in H such that $2u_i = 0 \mod (q-1)$ for all i is $(0, \ldots, 0)$.

A linear code is self-dual if $\mathcal{C}^\perp = \mathcal{C}$, in particular n must be even and $k = n/2$. If q is even one has an odd length $n = (q-1)^r$ and therefore there are no self-dual toric codes with q even. Let q be odd, since there are $u_1, \ldots, u_{2^r} \in H$ such that $\langle \mathrm{ev}(Y_i^u), \mathrm{ev}(Y_i^u) \rangle \neq 0$ the maximum dimension of a self-orthogonal code ($\mathcal{C}^\perp \subset \mathcal{C}$) is $n/2 - 2^{r-1} < n/2$, and therefore there are no self dual generalized toric codes. □

Example 10. Let $\mathbb{F}_5$ the finite field with 5 elements and $r = 2$. Therefore $H = \{0,1,2,3\} \times \{0,1,2,3\}$. The length of a generalized toric code $\mathcal{C}_U$ with $U \subset H$ is $n = 4^2 = 16$.

We order the elements of H to obtain I_σ in the previous way. Since the base field has 5 elements one has $\sigma(u) = u$ for $2^2 = 4$ elements $u_1 = (0,0)$, $u_2 = (0,2)$, $u_3 = (2,0)$ and $u_4 = (2,2)$. For the other elements of H we have $\sigma(u) \neq u$ and we consider $u_j = u$ and $u_{j+1} = \sigma(u)$, for instance $\sigma(0,1) = (0,3)$ and $\sigma(0,3) = (0,1)$. Therefore we write $u_5 = (0,1)$, $u_6 = (0,3)$, $u_7 = (1,0)$, $u_8 = (3,0)$, $u_9 = (1,1)$, $u_{10} = (3,3)$, $u_{11} = (1,2)$, $u_{12} = (3,2)$, $u_{13} = (1,3)$, $u_{14} = (3,1)$, $u_{15} = (2,1)$, $u_{16} = (2,3)$. Let $i_j = u_j \; \forall j \in \{1, \ldots n\}$ and let $\alpha = 2$. This ordering of H is not unique.

The evaluation matrix M of the map $\mathbb{F}_5[H] \to \mathbb{F}_5^n$ in the previous basis is

$$M=\begin{pmatrix}
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&4&4&1&1&4&4&1&1&4&4&4&4\\
1&1&1&1&1&1&4&4&4&4&4&4&4&4&1&1\\
1&1&1&1&4&4&4&4&1&1&4&4&1&1&4&4\\
1&4&1&4&2&3&1&1&2&3&4&4&3&2&2&3\\
1&4&1&4&3&2&1&1&3&2&4&4&2&3&3&2\\
1&1&4&4&1&1&2&3&2&3&2&3&2&3&4&4\\
1&1&4&4&1&1&3&2&3&2&3&2&3&2&4&4\\
1&4&4&1&2&3&2&3&4&4&3&2&1&1&3&2\\
1&4&4&1&3&2&3&2&4&4&2&3&1&1&2&3\\
1&1&4&4&4&4&2&3&3&2&2&3&3&2&1&1\\
1&1&4&4&4&4&3&2&2&3&3&2&2&3&1&1\\
1&4&4&1&3&2&2&3&1&1&3&2&4&4&2&3\\
1&4&4&1&2&3&3&2&1&1&2&3&4&4&3&2\\
1&4&1&4&2&3&4&4&3&2&1&1&2&3&2&3\\
1&4&1&4&3&2&4&4&2&3&1&1&3&2&3&2
\end{pmatrix}$$

And we have that the matrix $M \cdot M^t = I_\sigma$ is

$$I_\sigma=\begin{pmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0
\end{pmatrix}$$

Let $U = \{(0,0),(1,0),(2,0),(0,1),(1,1),(2,1)\}$ and $\mathcal{C}_U$ the code defined by U of length $n = 16$ and dimension $k = 6$. In this case $\mathcal{C}_U$ is also a toric code [8, Theorem 2.5] and [11, example 5.1]. A generator matrix of $\mathcal{C}_U$ is the submatrix of M consisting of the rows 1, 3, 5, 7, 9 and 15 of M. And a control matrix of $\mathcal{C}_U$, equivalently a generator matrix of $\mathcal{C}_U^\perp$, is the submatrix of M consisting of the rows 2, 4, 5, 7, 9, 11, 12, 13, 14 and 15 of M.

Acknowledgments: The author thanks A. Campillo for helpful comments on this paper.

References

[1] M Bras-Amorós and M O'Sullivan. Duality for several families of evaluation codes. *ArXiv:cs.IT/0609159*, 2006.

[2] V I Danilov. The geometry of toric varieties. *Russian Math. Surverys*, 33(2):97–154, 1978.

[3] V Díaz, C Guevara, and M Vath. Codes from n-dimensional polyhedra and n-dimensional cyclic codes. *Proceedings of SIMU summer institute*, 2001.

[4] J P Hansen. Toric surfaces and error-correcting codes. *Coding theory, cryptography and related areas (Guanajuato,1998)*, pages 132–142, 2000.

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

[6] D Joyner. Toric codes over finite fields. *Appl. Algebra Engrg. Comm. Comput.*, 15:63–79, 2004.

[7] J Little and H Schenck. Toric surface codes and Minkowski sums. *SIAM J. Discrete Math.*, 20 (4):999–1014, 2006.

[8] John Little and Ryan Schwarz. On toric codes and multivariate Vandermonde matrices. *Appl. Algebra Engrg. Comm. Comput.*, 18(4):349–367, 2007.

[9] F J Macwilliams and N J A Sloane. *The theory of error-correcting codes*, volume 16 of *North-Holland mathematical library.* North-Holland, 1977.

[10] D Ruano. Generalized toric codes. In F J Castro-Jiménez and J M Ucha-Enríquez, editors, *Book of abstracts of Tenth Meeting on Computational Algebra and its Applications, Universidad de Sevilla, September 2006*, pages 151–154, 2006.

[11] Diego Ruano. On the parameters of r-dimensional toric codes. *Finite Fields Appl.*, 13(4):962–976, 2007.

[12] M A Tsfasman and S G Vlăduţ. *Algebraic Geometry Codes*, volume 58 of *Mathematics and its applications.* Kluwer Dordrecht, 1991.