Finite Fields and Their Applications 33 (2015) 90–102

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On classification of toric surface codes of low dimension

Xue Luo [a], Stephen S.-T. Yau [b,*], Mingyi Zhang [b], Huaiqing Zuo [c]

[a] *School of Mathematics and System Sciences, Beihang University, Beijing, 100191, PR China*
[b] *Department of Mathematical Sciences, Tsinghua University, Beijing, 100084, PR China*
[c] *Mathematical Sciences Center, Tsinghua University, Beijing, 100084, PR China*

A R T I C L E I N F O

Article history:
Received 6 March 2014
Received in revised form 17 September 2014
Accepted 14 November 2014
Available online xxxx
Communicated by Xiang-dong Hou

Dedicated to Professor Ronald Graham on the occasion of his 80th birthday

MSC:
14G50
94B27

Keywords:
Toric code
Monomially equivalent
Lattice equivalence
Minimum distance

A B S T R A C T

This work is a natural continuation of our previous work [14]. In this paper, we give a complete classification of toric surface codes of dimension equal to 6, except a special pair, $C_{P_6^{(4)}}$ and $C_{P_6^{(5)}}$ over $\mathbb{F}_8$. Also, we give an example, $C_{P_6^{(5)}}$ and $C_{P_6^{(6)}}$ over $\mathbb{F}_7$, to illustrate that two monomially equivalent toric codes can be constructed from two lattice non-equivalent polygons.

* Corresponding author.
E-mail addresses: xluo@buaa.edu.cn (X. Luo), yau@uic.edu (S.S.-T. Yau), zmysljk@gmail.com (M. Zhang), hqzuo@math.tsinghua.edu.cn (H. Zuo).

http://dx.doi.org/10.1016/j.ffa.2014.11.007

1. Introduction

Toric codes, which were introduced by J. Hansen [5], are constructed on toric varieties. These toric codes have attracted quite a bit of attention in the last decade, because they are, in some sense, a natural extension of Reed–Solomon codes, which have been studied recently in [4–6,8,9,7], etc.

Compared to the other codes, the toric codes have their own advantage for study. The properties of these codes are closely tied to the geometry of the toric surface X_P associated with the normal fan $\triangle_P$ of the polygon P. Thanks to this advantage, D. Ruano [11] estimated the minimum distance using intersection theory and mixed volumes, extending the methods of J. Hansen for plane polygons. J. Little and H. Schenck [8] obtained upper and lower bounds on the minimum distance of a toric code constructed from a polygon $P \subset \mathbb{R}^2$ by examining Minkowski sum decompositions of subpolygons of P. The most interesting things are that J. Little and R. Schwarz [9] used a more elementary approach to determine the minimum distance of toric codes from simplices and rectangular polytopes. They also proved a general result that if there is a unimodular integer affine transformation taking one polytope P_1 to another polytope P_2, i.e. P_1 and P_2 are lattice equivalent (Definition 2.4), then the corresponding toric codes are monomially equivalent (hence have the same parameters). However, the reverse implication is not true. An explicit example will be given in our paper to illustrate this statement. Based on this useful tool, they classified the toric surface codes with a small dimension. However, one case of toric codes of dimension 5 was missing in their classification of toric surface codes. In [14], the second and the last author of this paper supplemented the missing case and completed the proof of classification of toric codes with dimension less than or equal to 5. There are other families of higher dimensional toric codes for which the minimum distance is computed explicitly, see [13].

In this paper, we give an (almost) complete classification of toric surface codes of dimension equal to 6. Also some interesting phenomena have been discovered in the process of our proofs. On the one hand, we give an explicit example that two monomially equivalent toric codes can be constructed from two lattice non-equivalent polygons, see Proposition 3.4. On the other hand, the number of the codewords in C_P over $\mathbb{F}_q$ with some particular weight can be varied by the choice of q, see [10, Tables 3.2–3.5]. The methods in this paper shed a light on classification of toric surface codes of higher dimension and it may give better champion codes than those in [2].

The main results in this paper are stated below:

Theorem 1.1. *Every toric surface code with $k = 6$, where k is the dimension of the code, is monomially equivalent to one constructed from one of the polygons in Fig. 1.*

Theorem 1.2. *$C_{P_6^{(i)}}$ and $C_{P_6^{(j)}}$ are not monomially equivalent over $\mathbb{F}_q$ for all $q \geq 7$, except that*

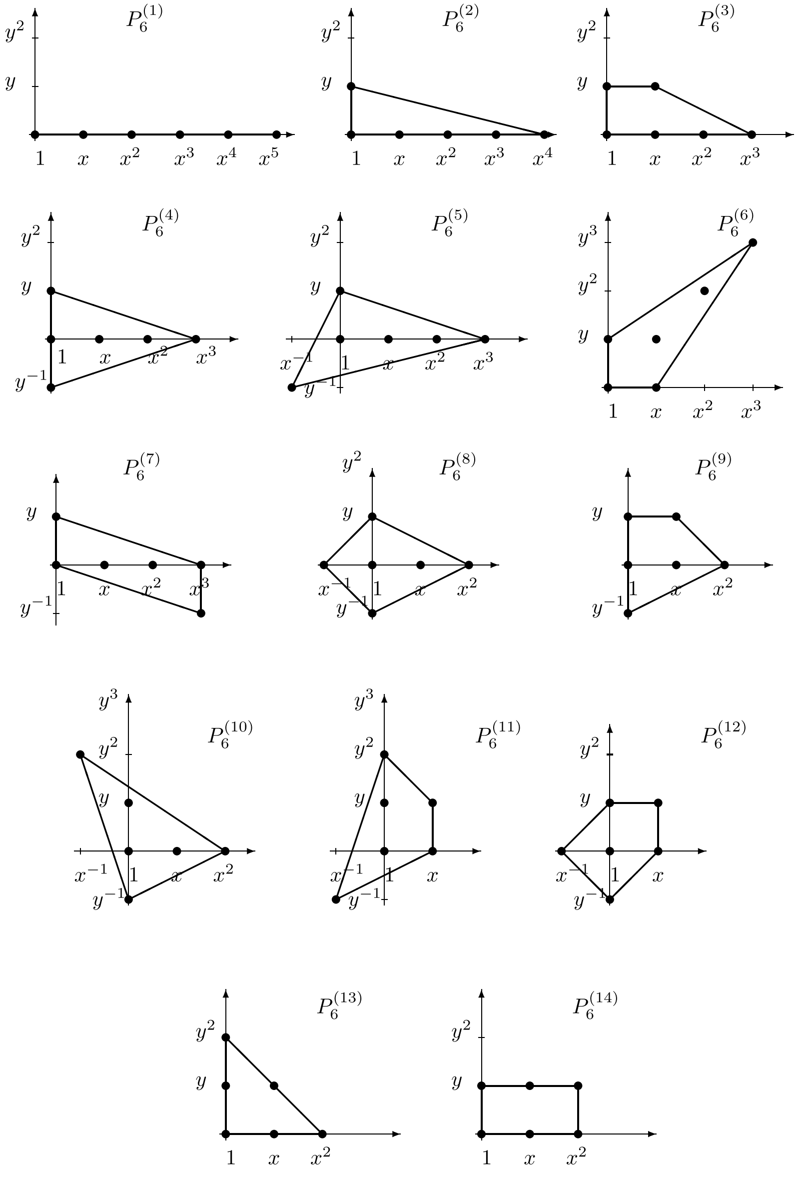

Fig. 1. Polygons yielding toric codes with $k = 6$.

(1) *$C_{P_6^{(5)}}$ and $C_{P_6^{(6)}}$ over $\mathbb{F}_7$ are monomially equivalent;*
(2) *the monomial equivalence of $C_{P_6^{(4)}}$ and $C_{P_6^{(5)}}$ over $\mathbb{F}_8$ remains open.*

The above theorems and the main results in [9,14] yield an (almost) complete classification of the toric codes of dimension ≤ 6 up to monomial equivalence. Based on the fact that the enumerator polynomial of $C_{P_6^{(4)}}$ and $C_{P_6^{(5)}}$ over $\mathbb{F}_8$ is exactly the same (see [10, Table A.1]), we conjecture the following:

Conjecture 1.1. *$C_{P_6^{(4)}}$ and $C_{P_6^{(5)}}$ over $\mathbb{F}_8$ are monomially equivalent.*

This paper is organized as follows. In Section 2, some preliminaries have been introduced. Section 3 is devoted to the sketch of the proofs. All the data computed by GAP (code from [7]) to support the proofs are collected in the tables in [10]. Due to the page limitation, the detailed proofs can be found there.

2. Preliminaries

In this section, we shall recall some basic definitions and results to be used later in this paper. We shall follow the terminology and notations for toric codes in [9].

2.1. Toric surface codes

Given a finite field $\mathbb{F}_q$ where q is a power of prime number. Let P be any convex lattice polygon contained in $\square_{q-1} = [0, q-2]^2$. We associate P with an $\mathbb{F}_q$-vector space of polynomials spanned by the bivariate power monomials:

$$\mathcal{L}(P) = \operatorname{Span}_{\mathbb{F}_q}\{x^{m_1}y^{m_2} \mid (m_1, m_2) \in P\}.$$

The toric surface code C_P [12] is a linear code with codewords the strings of values of $f \in \mathcal{L}(P)$ at all points of the algebraic torus $(\mathbb{F}_q^*)^2$:

$$C_P = \left\{\left(f(t), t \in \left(\mathbb{F}_q^*\right)^2\right) \mid f \in \mathcal{L}(P)\right\}.$$

2.2. Minkowski sum and minimum distance of toric codes

For some special polygons P, one can compute the minimum distance of the toric surface code C_P, say the rectangles and triangles.

Let $P_{k,l}^{\square} = \operatorname{conv}\{(0,0),(k,0),(0,l),(k,l)\}$ be the convex hull of the vectors $(0,0)$, $(k,0)$, $(0,l)$, (k,l). Let $\square_{q-1} = [0, q-2]^2 \subset \mathbb{Z}^2$. The minimum distance of $C_{P_{k,l}^{\square}}$ is given in the following theorem.

Theorem 2.3. *(See [9].) Let $k, l < q-1$, so that $P_{k,l}^{\square} \subset \square_{q-1} \subset \mathbb{R}^2$. Then the minimum distance of the toric surface code $C_{P_{k,l}^{\square}}$ is*

$$d(C_{P_{k,l}^{\square}}) = (q-1)^2 - (k+l)(q-1) + kl = \bigl((q-1)-k\bigr)\bigl((q-1)-l\bigr).$$

Let $P_{k,l}^{\triangle} = \operatorname{conv}\{(0,0),(k,0),(0,l)\}$ be the convex hull of the vectors $(0,0)$, $(k,0)$, $(0,l)$. Similarly, the minimum distance of $C_{P_{k,l}^{\triangle}}$ is given below:

Theorem 2.4. *(See [9].) If $P_{k,l}^{\triangle} \subset \square_{q-1} \subset \mathbb{R}^2$, and $m = \max\{k, l\}$, then*

$$d(C_{P_{k,l}^{\triangle}}) = (q-1)^2 - m(q-1).$$

Remark 2.1. These two theorems above can be generalized to higher dimensional case, see [9].

In the paper [12], the authors give a good bound for the minimum distance of C_P in terms of certain geometric invariant $L(P)$, the so-called full Minkowski length of P.

Definition 2.1. Let P and Q be two subsets of $\mathbb{R}^n$. The Minkowski sum is obtained by taking the pointwise sum of P and Q:

$$P + Q = \{x + y \mid x \in P, y \in Q\}.$$

Let P be a lattice polytope in $\mathbb{R}^n$. Consider a Minkowski decomposition

$$P = P_1 + \cdots + P_l$$

into lattice polytopes P_i of positive dimension. Let $l(P)$ be the largest number of summands in such decompositions of P, and called the Minkowski length of P.

Definition 2.2. *(See [12].)* The full Minkowski length of P is the maximum of the Minkowski lengths of all subpolytopes Q in P,

$$L(P) := \max\bigl\{l(Q) \bigm| Q \subset P\bigr\}.$$

We shall use the results in [12] to give a bound of the minimum distance of C_P:

Theorem 2.5. *(See [12].) Let $P \subset \square_{q-1}$ be a lattice polygon with area A and full Minkowski length L. For $q \geq \max(23, (c + \sqrt{c^2 + 5/2})^2)$, where $c = A/2 - L + 9/4$, the minimum distance of the toric surface code C_P satisfies*

$$d(C_P) \geq (q-1)^2 - L(q-1) - 2\sqrt{q} + 1.$$

With the condition that no factorization $f = f_1 \cdots f_{L(P)}$ for all $f \in \mathcal{L}(P)$ contains an exceptional triangle (a triangle with exactly 1 interior and 3 boundary lattice points), we have a better bound for the minimum distance of C_P:

Proposition 2.1. *(See [12].) Let $P \subset \square_{q-1}$ be a lattice polygon with area A and full Minkowski length L. Under the above condition on P, for $q \geq \max(37, (c + \sqrt{c^2 + 2})^2)$, where $c = A/2 - L + 11/4$, the minimum distance of the toric surface code C_P satisfies*

$$d(C_P) \geq (q-1)^2 - L(q-1).$$

2.3. Some theorems about classification of toric codes

In this paper, we shall classify the toric codes with dimension equal to 6, according to the monomial equivalence. Thus, we state the precise definition below.

Definition 2.3. Let C_1 and C_2 be two codes of block length n and dimension k over $\mathbb{F}_q$. Let G_1 be a generator matrix for C_1. Then C_1 and C_2 are said to be monomially equivalent if there is an invertible $n \times n$ diagonal matrix Δ and an $n \times n$ permutation matrix Π such that

$$G_2 = G_1 \Delta \Pi$$

is a generator matrix for C_2.

It is easy to see that monomial equivalence is actually an equivalent relation on codes since a product $\Pi\Delta$ equals $\Delta'\Pi$ for another invertible diagonal matrix Δ'. It is also a direct consequence of the definition that monomially equivalent codes C_1 and C_2 have the same dimension and the same minimum distance (indeed, the same full weight enumerator).

An affine transformation of $\mathbb{R}^m$ is a mapping of the form $T(x) = Mx + \lambda$, where λ is a fixed vector and M is an $m \times m$ matrix. The affine mappings T, where $M \in GL(m, \mathbb{Z})$ (so $Det(M) = \pm 1$) and λ have integer entries, are precisely the bijective affine mappings from the integer lattice $\mathbb{Z}^m$ to itself.

Generally speaking, it's impractical to determine two given toric codes to be monomially equivalent directly from the definition. A more practical criteria comes from the nice connection between the monomial equivalence class of the toric codes C_P and the lattice equivalence class of the polygon P in [9].

Theorem 2.6. *If two polytopes P and $\tilde{P}$ are lattice equivalent, then the toric codes C_P and $C_{\tilde{P}}$ are monomially equivalent.*

The definition of the lattice equivalence of two polygons is the following:

Definition 2.4. We say that two integral convex polytopes P and $\tilde{P}$ in $\mathbb{Z}^m$ are lattice equivalent if there exists an invertible integer affine transformation T as above such that $T(P) = \tilde{P}$.

For the sake of completeness, we list some simple facts about lattice equivalence of two polytopes P and $\tilde{P}$ in $\mathbb{Z}^2$.

Proposition 2.2.

(i) *If P can be transformed to $\tilde{P}$ by translation, rotation and reflection with respect to x-axis or y-axis, then P and $\tilde{P}$ are lattice equivalent;*

(ii) *If P and $\tilde{P}$ are lattice equivalent, then they have the same number of sets of n collinear points and the same number of sets of n concurrent segments;*
(iii) *If P and $\tilde{P}$ are lattice equivalent, then they are both n-side polygons;*
(iv) *If P and $\tilde{P}$ are lattice equivalent, then they have the same number of interior integer lattices.*

These properties are directly followed from Definition 2.4.

Besides the properties of lattice equivalence, Pick's formula is also a useful tool in the proof of Theorem 1.1.

Theorem 2.7 *(Pick's formula). Assume P is a convex rational polytope in the plane, then*

$$\sharp(P) = A(P) + \frac{1}{2} \cdot \partial(P) + 1,$$

where $\sharp(P)$ represents the number of lattice points in P, $A(P)$ is the area of P and $\partial(P)$ is the perimeter of P, with the length of an edge between two lattice points defined as one more than the number of lattice points lying strictly between them.

Remark 2.2. Generally speaking, $\partial(P)$ is the number of lattice points on the boundary of P. The only exception in plane is line segment, which should follow the precise definition of length of the edge above.

2.4. Some theorems to eliminate the upper bound of q

Let us introduce the so-called Hasse–Weil bounds, which will be used in the proof of Theorem 1.2 frequently to help specifying the exact number of the codewords with some particular weight, for q large.

Theorem 2.8. *(See [1].) If Y is an absolutely irreducible but possibly singular curve, g is the* arithmetic genus *of Y, $Y(\mathbb{F}_q)$ is the set of $\mathbb{F}_q$-rational points of curve, then*

$$1 + q - 2g\sqrt{q} \le \left|Y(\mathbb{F}_q)\right| \le 1 + q + 2g\sqrt{q}.$$

These two bounds are called the Hasse–Weil bounds.

Let $f \in \mathcal{L}(P)$ and P_f denote its Newton polygon, which is the convex hull of the lattice points in $(\mathbb{F}_q^*)^2$. Denote

$$f = \sum_{m=(m_1,m_2)\in P_f} \lambda_m x^{m_1} y^{m_2}, \quad \lambda_m \in \mathbb{F}_q^*.$$

Let X be a smooth toric surface over $\overline{\mathbb{F}}_q$ defined by a fan $\Sigma_X \subset \mathbb{R}^2$ which is a refinement of the normal fan of P_f. Let C_f be the closure in X of the affine curve given by $f = 0$. If f is absolutely irreducible, then C_f is irreducible. By Theorem 2.8,

$$\left|C_f(\mathbb{F}_q)\right| \le q + 1 + 2g\sqrt{q},$$

where g is the arithmetic genus of C_f.

Let $Z(f)$ be the number of zeros of f in the torus $(\mathbb{F}_q^*)^2$. It is well known that the arithmetic genus g of C_f equals to the number of interior lattice points in P_f (see [8] for the curves).

Proposition 2.3. *Let f be absolutely irreducible with Newton polygon P_f. Then*

$$Z(f) \le q + 1 + 2I(P_f)\sqrt{q},$$

where $I(P_f)$ is the number of interior lattice points.

3. Proof of the theorems

In this section, we shall give the sketch of the proofs of Theorems 1.1 and 1.2. Before that, let us clarify the notations first. Let P_i denote an integral convex polygon in $\mathbb{Z}^2$ with i lattice points, $P_i^{(j)}$ is the jth lattice equivalence class of P_i, V is the additional lattice point, which will be added to $P_i^{(j)}$ and $P_{i,V}^{(j)} := \operatorname{conv}\{P_i^{(j)}, V\}$ denote a new integral convex polygon formed by $P_i^{(j)}$ and V. Our strategy is almost the same as that in [9], by adding all possible choices of V to $P_5^{(j)}$ to get all lattice equivalence classes of P_6 with the help of Pick's formula. For the sake of self-contain, we list all the $P_5^{(j)}$, $j = 1, \cdots, 7$ in Fig. 2.

Proof of Theorem 1.1. Let us add V to $P_5^{(1)} = \operatorname{conv}\{(0,0),(4,0)\}$ to see that $P_6^{(1)}$ and $P_6^{(2)}$ are the only two lattice equivalence classes. If V is on the x-axis to form a line segment, the only choices of V would be $(5,0)$ or $(-1,0)$, otherwise the new convex polygon have more than 6 lattice points. Notice that $P_6^{(1)} = \operatorname{conv}\{P_5^{(1)}, (5,0)\}$ and $\operatorname{conv}\{P_5^{(1)}, (-1,0)\}$ are lattice equivalent by translation (i.e. Proposition 2.2 (i)). If V is not on the x-axis, then we have $\partial(P_{5,V}^{(1)}) = 6$. By using Pick's formula, $6 = \#(P_{5,V}^{(1)}) = A(P_{5,V}^{(1)}) + \frac{1}{2}\partial(P_{5,V}^{(1)}) + 1 = A(P_{5,V}^{(1)}) + 4$, we get $A(P_{5,V}^{(1)}) = 2$. Therefore, the choices of V are the lattice points on $y = \pm 1$. Say, $V = (x_0, 1)$, x_0 is integer. By the definition of lattice equivalence, there is an integer affine transformation $M = \begin{pmatrix} 1 & 0 \\ -x_0 & 1 \end{pmatrix}$, which transforms $\operatorname{conv}\{P_5^{(1)}, (x_0, 1)\}$ to $P_6^{(2)}$. The similar transformation can be found to $\operatorname{conv}\{P_5^{(1)}, (x_0, -1)\}$.

There are only 14 lattice equivalence classes $P_6^{(i)}$, $i = 1, \cdots, 14$, as shown in Fig. 1. Since the arguments are similar, we just list all the possible V's and in which equivalence class $P_{5,V}^{(i)}$ is, for $i = 1, \cdots, 7$, in [10, Table 3.1]. The verification is left to the interested readers. □

In order to show Theorem 1.2, we only need to determine whether two toric surface codes constructed from the polygons in Fig. 1 can be pairwise monomially equivalent. Our strategy is the following:

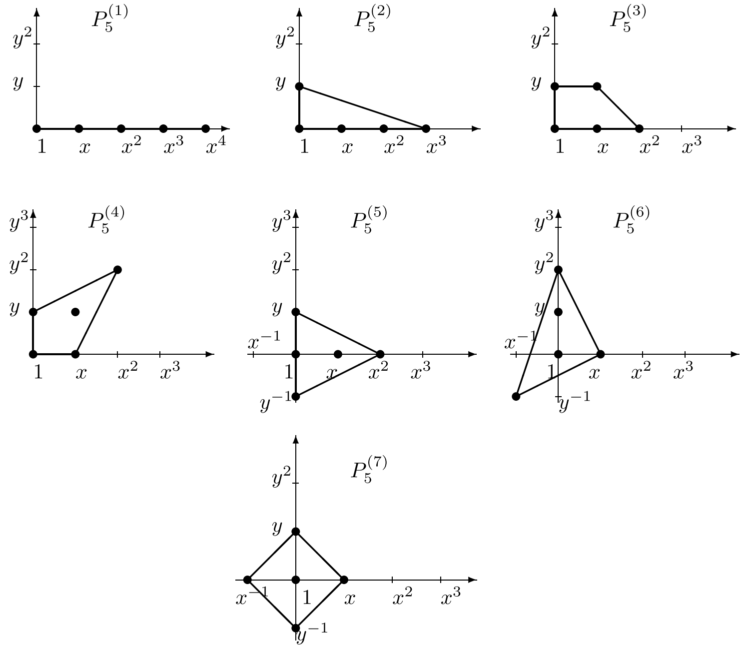

Fig. 2. Polygons yielding toric codes with $k = 5$.

(1) For q small, say $q \leq 8$, we use the GAP code (with toric package and guava package) to get their enumerator polynomials directly. If those enumerator polynomials of $C_{P_6^{(i)}}$, $1 \leq i \leq 14$, are different from each other on $\mathbb{F}_q$, for $7 \leq q \leq 8$, then they are not pairwise monomially equivalent. If they are the same in some cases (for example, $C_{P_6^{(5)}}$ and $C_{P_6^{(6)}}$ over $\mathbb{F}_7$, $C_{P_6^{(4)}}$ and $C_{P_6^{(5)}}$ over $\mathbb{F}_8$, see [10, Table A.1]), we need some further investigations.

(2) For q large, say $q \geq 9$, we shall compare the invariants of the codes, including minimum distance, the number of the codewords with some particular weight, etc. Once we could identify one invariant in one case to be different from that in another case, then we conclude that they are pairwise monomially inequivalent. However, the estimate of the number of the codewords with some particular weight depends on how large q is. Therefore, we still need to use GAP (with toric package and guava package) for small q (see [10, Tables A.2 and A.3]).

The first step in our strategy is to tell the monomial equivalence of $C_{P_6^{(i)}}$, $1 \leq i \leq 14$, for $q \leq 8$. It's easy to see from [10, Table A.1] that all the enumerator polynomials of $C_{P_6^{(i)}}$, $1 \leq i \leq 14$, are different, except that of $C_{P_6^{(5)}}$ and $C_{P_6^{(6)}}$ over $\mathbb{F}_7$ and that of $C_{P_6^{(4)}}$ and $C_{P_6^{(5)}}$ over $\mathbb{F}_8$. Here, an interesting phenomena occurs. Two toric codes constructed from two lattice non-equivalent polygons could also be monomially equivalent. $C_{P_6^{(5)}}$ and $C_{P_6^{(6)}}$ over $\mathbb{F}_7$ is the typical example.

Proposition 3.4. *$C_{P_6^{(5)}}$ and $C_{P_6^{(6)}}$ over $\mathbb{F}_7$ are monomially equivalent.*

Proof. We use the Magma program to give the generator matrices of these two toric codes over $\mathbb{F}_7$. For the Magma code, please refer to [7]. □

Unfortunately, the other pair $C_{P_6^{(4)}}$ and $C_{P_6^{(5)}}$ over $\mathbb{F}_8$ can't be determined by the same way as in Proposition 3.4, since the command "IsEquivalent" in Magma can only be used to compare toric codes over $\mathbb{F}_q$ with $q = 4$ or small prime numbers. Moreover, it is infeasible to show the monomial equivalence directly from the definition. So we leave the problem open. Based on the result in Proposition 3.4 and the fact that the enumerator polynomial of $C_{P_6^{(4)}}$ and $C_{P_6^{(5)}}$ over $\mathbb{F}_8$ is exactly the same, we conjecture that this pair, i.e. $C_{P_6^{(4)}}$ and $C_{P_6^{(5)}}$ over $\mathbb{F}_8$, is also monomially equivalent. Further, we ask a more general question for the interested readers: For which q and k are there monomially equivalent toric codes over $\mathbb{F}_q$ from polytopes that are not lattice equivalent?

Next, we shall classify $C_{P_6^{(i)}}$, $1 \le i \le 14$, for $q \ge 9$. The first invariant to be examined is the minimum distance (or the minimum weight), denoted as $d(C_{P_6^{(i)}})$.

Proposition 3.5. *According to $d(C_{P_6^{(i)}})$, $1 \le i \le 14$, for $q \ge 9$, no code in one of the five groups is monomially equivalent to a code in any of the other four groups:*

(i) $C_{P_6^{(1)}}$;
(ii) $C_{P_6^{(2)}}$;
(iii) $C_{P_6^{(14)}}$;
(iv) $C_{P_6^{(i)}}$, *for* $3 \le i \le 8$;
(v) $C_{P_6^{(i)}}$, *for* $9 \le i \le 13$.

Sketch of the proof. Detailed proof is included in [10, Proposition 3.5]. Here we only summarize the minimum distance below:

(i) $d(C_{P_6^{(1)}}) = (q-1)^2 - 5(q-1)$,
(ii) $d(C_{P_6^{(2)}}) = (q-1)^2 - 4(q-1)$,
(iii) $d(C_{P_6^{(14)}}) = (q-1)^2 - (3q-5)$,
(iv) $d(C_{P_6^{(i)}}) = (q-1)^2 - 3(q-1)$ for $3 \le i \le 8$,
(v) $d(C_{P_6^{(i)}}) = (q-1)^2 - 2(q-1)$ for $9 \le i \le 13$. □

Just according to the minimum distance, the monomial equivalence/inequivalence of any two codes both from either group (iv) or (v) in Proposition 3.5 are still unknown. We shall examine two more invariants: the numbers of the codewords with weight $(q-1)^2 - 2(q-1)$ and $(q-1)^2 - (2q-3)$, denote as $n_1(C_{P_6^{(i)}})$ and $n_2(C_{P_6^{(i)}})$, respectively.

The basic idea to examine the pairwise monomial inequivalence of any two codes $C_{P_6^{(i)}}$ in group (iv) or (v) is:

(1) to find out $n_1(C_{P_6^{(i)}})$ and to sort the codes with the same $n_1(C_{P_6^{(i)}})$ into subgroups to be determined later;

(2) to give the range of $n_2(C_{P_6^{(i)}})$ among the codes with the same $n_1(C_{P_6^{(i)}})$ and to compare them to give the final classification.

Fortunately, in our situation, these two invariants are enough to give a complete classification of monomial equivalence class to $C_{P_6^{(i)}}$ in group (iv) and (v), respectively.

To be more precise, the way to compute $n_1(C_{P_6^{(i)}})$ is to enumerate the families of evaluations that contribute to weight $(q-1)^2 - 2(q-1)$. The completeness of the enumeration above is followed by Theorem 2.8, which requires q being large, say $q \geq 23$ (this lower bound is given by the inequality in Proposition 2.3, see detailed explanation in the sketch of the proof of Proposition 3.6) in most of the cases. Then, we use the GAP code (with toric package and guava package) again to make up the gap $9 \leq q \leq 19$, see [10, Table A.2]. For $q \geq 23$, with the help of $n_1(C_{P_6^{(i)}})$, we can exclude some codes and sort the ones left into several subgroups with the same $n_1(C_{P_6^{(i)}})$. Then, by enumerating the families of evaluations that contribute to weight $(q-1)^2 - (2q-3)$, the range of $n_2(C_{P_6^{(i)}})$ can be obtained to classify the subgroups.

Proposition 3.6. *For $q \geq 9$, no two codes from the same group either* (iv) *or* (v) *in Proposition 3.5 are monomially equivalent.*

Sketch of the proof. The argument is similar to that in the proof of Theorem 6 in [9]. For the readers' convenience, we investigate $n_1(C_{P_6^{(3)}})$ in detail in [10]. The key point in the argument is to find out the distinct families of reducible polynomials which evaluate to give the codewords with weight $(q-1)^2 - 2(q-1)$, where [3, Theorem 4.2] is used. Table 3.2 in [10] lists the key information for $n_1(C_{P_6^{(i)}})$, $3 \leq i \leq 8$, with $q \geq 23$.

Let us explain where the lower bound of q comes from briefly, say in the case $C_{P_6^{(4)}}$. It is also valid for other $C_{P_6^{(i)}}$, $5 \leq i \leq 8$. Actually, for $q \geq 23$, we claim that there are exactly $5\binom{q-1}{2}(q-1)$ such codewords in $C_{P_6^{(4)}}$. Any other such codewords could only come from evaluating a linear combination of $\{1, x, x^2, x^3, y, y^{-1}\}$ in which both $\{x, x^2, x^3\}$ and $\{y, y^{-1}\}$ appears with at least one element having nonzero coefficients (since otherwise we are in a case previously covered). Such polynomial will be absolutely irreducible. The maximal polygon of such polynomials associates to the polynomials with x^3, y, y^{-1} having nonzero coefficients, as $f = a_1 + a_2x + a_3x^2 + a_4x^3 + a_5y + a_6y^{-1}$ where $a_4, a_5, a_6 \neq 0$. By Proposition 2.3, the number of zeros of f in the torus $(\mathbb{F}_q^*)^2$ has a bound:

$$Z(f) \leq q + 1 + 2I(P_f)\sqrt{q} = 1 + q + 4\sqrt{q}.$$

When $q \geq 23$, $Z(f) < 2q - 2$. Thus such polynomial can never have $2q - 2$ zeros when $q \geq 23$. Any other smaller polygons have fewer interior points and then have lower upper bound. So all such polynomials can never have $2q - 2$ zeros when $q \geq 23$.

Due to Table 3.2 in [10] we still have the following three cases to verify:

(1) When $q \geq 23$, any two codes of $C_{P_6^{(3)}}$, $C_{P_6^{(5)}}$ and $C_{P_6^{(6)}}$ are pairwise monomially inequivalent;
(2) Over $\mathbb{F}_q$, where $3 \nmid (q-1)$, $C_{P_6^{(7)}}$ and any one code of $C_{P_6^{(3)}}$, $C_{P_6^{(5)}}$, $C_{P_6^{(6)}}$ are pairwise monomially inequivalent;
(3) Over $\mathbb{F}_q$, where $q = 2^n$, $n \in \mathbb{Z}_+$, $C_{P_6^{(4)}}$ and $C_{P_6^{(8)}}$ are pairwise monomially inequivalent.

It is worth to mention that we could make sure $n_2(C_{P_6^{(4)}}) = 0$ when $q = 2^n$ and $n \geq 5$; and we could settle down the value of $n_2(C_{P_6^{(i)}})$ for $i = 6, 7, 8$ and $q \geq 25$. Thus, it is sufficient to check that no two enumerator polynomials of each codes over $\mathbb{F}_q$, $q \leq 23$, in [10, Table A.2] are exactly the same, which guarantees the codes are pairwise inequivalent in each case above. The way to find out $n_2(C_{P_6^{(i)}})$, $3 \leq i \leq 8$, is similar to that of $n_1(C_{P_6^{(3)}})$ before. So we just list the key information in [10, Table 3.3] say the distinct families of reducible polynomials which evaluate to give the codewords with weight $(q-1)^2 - (2q-3)$, of each codes as before. The verifications are left to the interested readers. We have reached our conclusion for group (iv) in Proposition 3.5.

Similarly, we could give a complete classification of monomial equivalence class of $C_{P_6^{(i)}}$ in group (v). They are classified by $n_1(C_{P_6^{(i)}})$ in [10, Table 3.4]. Three cases are left to be determined by $n_2(C_{P_6^{(i)}})$:

(1) $C_{P_6^{(9)}}$ and $C_{P_6^{(11)}}$ are monomially inequivalent;
(2) $C_{P_6^{(10)}}$ and $C_{P_6^{(13)}}$ are monomially inequivalent;
(3) Over $\mathbb{F}_q$, where $q = 2^m$, $m \in \mathbb{Z}_+$, $C_{P_6^{(12)}}$ and any one of $C_{P_6^{(9)}}$, $C_{P_6^{(11)}}$ are monomially inequivalent.

The conclusion follows immediately from [10, Table 3.5]. □

Acknowledgments

The Magma program and GAP program is provided by John Little, to whom we are extremely thankful, especially for his patience and helpful discussions. X. Luo acknowledges the support of Scientic Research Foundation for the Returned Overseas Chinese Scholars, State Education Ministry and the Fundamental Research Funds for the Central Universities (Grant No. YWF-14-RSC-026). S.S.-T. Yau thanks the start-up fund from Tsinghua University. And H. Zuo gratefully acknowledges the support of National Natural Science Foundation of China (Grant No. 11401335) and the start-up fund from Tsinghua University.

References

[1] Y. Aubry, M. Perret, A Weil theorem for singular curves, in: R. Pellikaan, M. Perret, S.G. Vladut (Eds.), Arithmetic, and Coding Theory, de Gruyter, Berlin, 1996, pp. 1–7.

[2] G. Brown, A.M. Kasprzyk, Seven new champion linear codes, LMS J. Comput. Math. 16 (2013) 109–117.
[3] P. Beelen, R. Pellikaan, The Newton polygon of plane curves with many rational points, Des. Codes Cryptogr. 21 (2000) 41–67.
[4] P. Diaz, C. Guevara, M. Vath, Codes from n-dimensional polyhedra and n-dimensional cyclic codes, in: Proceedings of SIMU Summer Institute, 2001.
[5] J.P. Hansen, Toric surfaces and error-correcting codes, in: Coding Theory, Cryptography and Related Areas, Guanajuato, 1998, Springer, Berlin, 2000, pp. 132–142.
[6] J.P. Hansen, Toric varieties Hirzebruch surfaces and error-correcting codes, Appl. Algebra Eng. Commun. Comput. 13 (2002) 289–300.
[7] D. Joyner, Toric codes over finite fields, Appl. Algebra Eng. Commun. Comput. 15 (2004) 63–79.
[8] J. Little, H. Schenck, Toric surface codes and Minkowski sums, SIAM J. Discrete Math. 20 (2006) 999–1014.
[9] J. Little, R. Schwarz, On toric codes and multivariate Vandermonde matrices, Appl. Algebra Eng. Commun. Comput. 18 (2007) 349–367.
[10] X. Luo, S.S.-T. Yau, M. Zhang, H. Zuo, On classification of toric surface codes of low dimension, arXiv:1402.0060, 2014.
[11] D. Ruano, On the parameters of r-dimensional toric codes, Finite Fields Appl. 13 (4) (2007) 962–976.
[12] I. Soprunov, J. Soprunova, Toric surface codes and Minkowski length of polygons, SIAM J. Discrete Math. 23 (2009) 384–400.
[13] I. Soprunov, J. Soprunova, Bring toric codes to the next dimension, SIAM J. Discrete Math. 24 (2) (2010) 655–665.
[14] S.S.-T. Yau, H. Zuo, Notes on classification of toric surface codes of dimension 5, Appl. Algebra Eng. Commun. Comput. 20 (2009) 175–185.