AAECC (2009) 20:175–185
DOI 10.1007/s00200-009-0096-2

Notes on classification of toric surface codes of dimension 5

Stephen S.-T. Yau · Huaiqing Zuo

Received: 4 August 2008 / Revised: 2 March 2009 / Published online: 31 March 2009

Abstract This is an addendum to the beautiful paper by Little and Schwarz (Appl Algebra Eng Commun Comput 18:349–367, 2007) in which one case of toric surface codes of dimension 5 was missing in their classification result of toric surface codes of dimension less than 6. Our main purpose is to fill the gap of this paper. We find that our new code $C_{P_5^{(7)}}$ enjoys more symmetry, and it has more codewords of minimum distance in general. However, over some special fields $\mathbb{F}_{2^m}$, $C_{P_5^{(5)}}$ and $C_{P_5^{(7)}}$ have the same number of the codewords of minimum distance.

1 Introduction

In [3,4], Hansen introduces the evaluation codes defined over some toric surfaces. He uses the proper combinational techniques of toric surfaces to estimate the parameters of these codes toric surface codes. Actually toric codes are in a sense a natural

H. Zuo was supported by NSFC and PSSCS of Shanghai.

S. S.-T. Yau
Institute of Mathematics, East China Normal University,
Shanghai, People's Republic of China

S. S.-T. Yau (✉)
Department of MSCS, M/C 249, Room 322, University of Illinois at Chicago,
851 S. Morgan St., Chicago, IL 60607-7045, USA
e-mail: yau@uic.edu

H. Zuo
Department of Mathematics, East China Normal University,
No. 500, Dong-chuan Road, 200062 Shanghai, People's Republic of China
e-mail: hqzuo@hotmail.com

extension of Reed-Solomon codes. In this paper we focus only on toric surface codes. We will follow the terminology and notation for toric codes from [7].

The properties of these codes are closely tied to the geometry of the toric surface X_P associated with the normal fan Δ_P of the polygon P. For example, Ruano [8] estimated the minimum distance using intersection theory and mixed volumes, extending the methods of Hansen for plane polygons. In [6] Little and Schenck obtained upper and lower bounds on the minimum distance of a toric code constructed from a polygons of P. The most interesting things was that Little and Schwarz [7] provided a good approach that applies quite well to many high dimensional toric codes. Their methods are based on a sort of multivariate generalization of vandermonde determinants that has also been used in the study of multivariate polynomial interpolation. They used these vandermonde determinants to determine the minimum distance of toric codes from simplices and rectanglur polytopes, and proved a general result showing that if there is a unimodular integer affine transformation taking one polytopes P_1 to a second P_2, then the corresponding toric codes are monomially equivalent (hence have the same parameters). The most important thing is that they also used those tools to classify the toric surface codes with small dimension. However, the classification results in [7] is not complete. One case of toric code of dimension 5 was missing in their classification of toric surface codes. In this paper, our main purpose is to supply the missing case and finish the proof of classification of toric codes of dimension less than 6. Between $C_{P_5^{(5)}}$ and $C_{P_5^{(7)}}$, we also find a interesting fact. Since our new code $C_{P_5^{(7)}}$ enjoys more symmetry, it has more codewords of minimum distance in general. However, over some special field $\mathbb{F}_{2^m}$, these two codewords have the same number of the codewords of minimum distance. The main results in this paper are the following theorems.

Theorem 1.1 *Every toric surface code with $3 \leq k \leq 5$, where k is the dimension of the code, is monomially equivalent to one constructed from the one of the polygons in Figs. 1, 2, 3 or 4.*

Remark In [7], there is only 12 pictures, however we have 13 pictures here. Figure 4 was missing in [7].

Theorem 1.2 *Let $q > 5$. No two of the toric codes $C_p(\mathbb{F}_q)$ constructed from the polygons in Theorem 1.1 are monomially equivalent.*

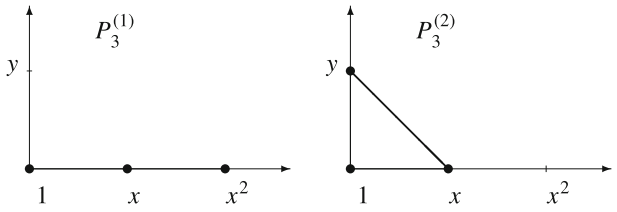


Fig. 1 Polygons yielding toric codes with $k = 3$

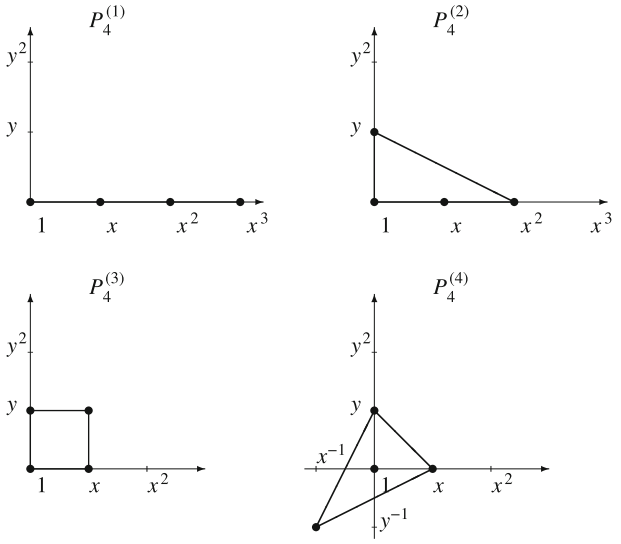


Fig. 2 Polygons yielding toric codes with $k = 4$

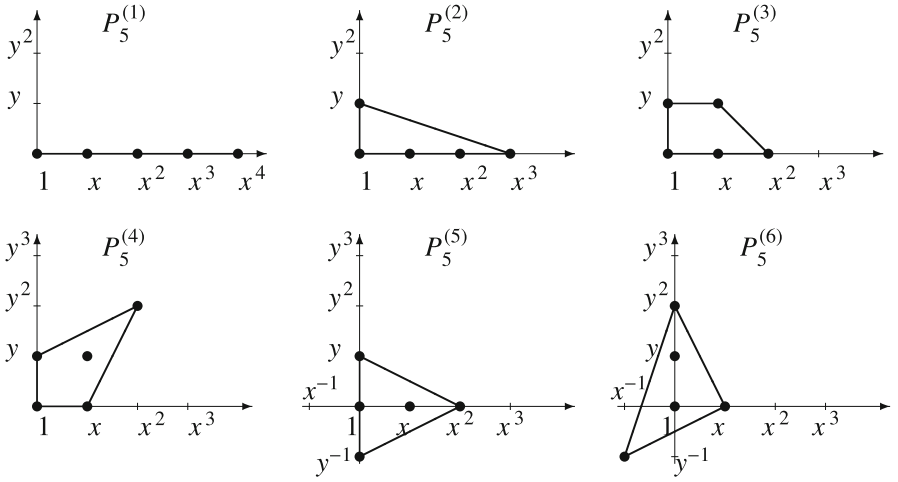
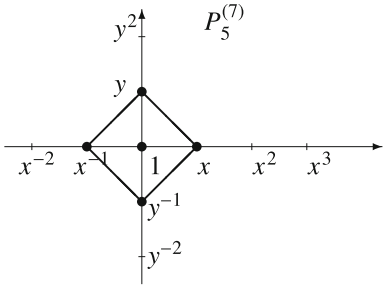


Fig. 3 Polygons yielding toric codes with $k = 5$

Fig. 4 A polygon yielding toric codes with $k = 5$



2 Preliminaries

In this section, we shall recall some basic definitions and results which are needed in this paper.

2.1 Minkowski sum and minimum distance of toric codes

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:

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

For a polygon P, let $I(P)$ denote the number of lattice points in the interior of P.

Theorem 2.2 [6] *Let $\mathbb{F}_q$ be a finite field and let $P \subset \mathbb{R}^2$ be an integral convex polygon strictly contained in $\square_{q-1}$. Assume that $q \geq (4I(P) + 3)^2$ (the lower bound on q will rarely be sharp), let ℓ bet the largest positive integer such that there is some $P' \subseteq P$ such that P' is decomposed as a Minkowski sum $P' = P_1 + P_2 + \cdots + P_\ell$ with nontrival P_i (i.e. P_i is not a point). Then*

$$d(C_P(\mathbb{F}_q)) \geq \sum_{i=1}^{\ell} d(C_{P_i}(\mathbb{F}_q)) - (\ell - 1)(q - 1)^2.$$

Let $P_{k,\ell}$ be the rectangular $P_{k,\ell} = \text{conv}\{(0, 0), (k, 0), (0, \ell), (k, \ell)\}$ be the convex hull of the vectors $(0, 0), (k, 0), (0, \ell), (k, \ell)$. We have the following theorem about $C_{P_{k,\ell}}$.

Theorem 2.3 [7] *Let $k, \ell < q - 1$, so that $P_{k,\ell} \subset \square_{q-1} \subset \mathbb{R}^2$. Then the minimum distance of the toric surface code $C_{P_{k,\ell}}$ is*

$$d(C_{P_{k,\ell}}) = (q - 1)^2 - (k + l)(q - 1) + \kappa\ell = ((q - 1) - k)((q - 1) - \ell).$$

Remark There are a similar results to high dimensional toric codes associated to rectangular polytope $[0, k_1], \ldots, [0, k_m] \subset \square_{q-1} \subset \mathbb{R}^m$.

2.2 Some theorems about classification of toric codes

Definition 2.4 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 equivalence 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.

Definition 2.5 We will say that two integral convex polytopes P_1 and P_2 in $\mathbb{R}^m$ are **lattice equivalent** if there exists an invertible integer affine transformation T as above such that $T(P_1) = P_2$.

In [7], the authors proved the following three results.

Theorem 2.6 *If two polytopes P_1 and P_2 are lattice equivalent, then the toric codes C_{P_1} and C_{P_2} are monomially equivalent.*

Proposition 2.7 *Every toric surface code C_p with $k = 2$ is monomially equivalent to the toric code C_{P_2} for $P_2 = conv\{(0, 0), (1, 0)\}$.*

Theorem 2.8 *Let $q > 5$, no two of the toric codes $C_P(\mathbb{F}_q)$ constructed from the polytopes in Figs. 1, 2, 3 are monomially equivalent.*

2.3 Two general theorems

Theorem 2.9 [1] *If Y is a absolutely irreducible but possibly singular curves, g is the* arithmetic genus *of Y, $Y(\mathbb{F}_q)$ is the $\mathbb{F}_q-$rational points of curve, then*

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

These two bounds are called the Hasse–Weil bounds.

Theorem 2.10 [2] *Let $F(X, Y) = 0$ define an irreducible curve $\mathcal{X}$ over an algebraically closed field. Then the genus g of the nonsingular model of $\mathcal{X}$ satisfies*

$$g \leq 1 + area\,\Gamma(F) - \frac{1}{2}\{number\ of\ integral\ points\ on\ \partial\Gamma(F)\}.$$

This last expression is equal to the number of integral points in the interior of $\Gamma(F)$.

3 Proof of the theorem

Proof of Theorem 1.1 Basing on Proposition 2.7, the next step is to find a "nice" lattice polygon in each possible lattice equivalence class with $\#(P) = 3, 4, 5$. One way is to add additional points to P_2. Using Pick's Theorem:"$A(P) = \#(P)+\frac{1}{2}\partial(P)-1$"(where $\partial(P)$ is the number of Lattice points in the boundary of P) and the fact that

affine transformation preserves the collinear points and concurrent lines, one sees that polygons are exactly 13 pictures in Figs. 1, 2, 3 or 4 up to lattice equivalence.

In order to classify the toric surface codes of dimension less than 6. The final step is to show that no two of the toric surface codes constructed from these polygons can be monomially equivalent.

Proof of Theorem 1.2 According Theorem 2.8, we only need to prove that $C_{P_5^{(7)}}$ is not monomially equivalent to $C_{P_3^{(i)}}$ for $i = 1, 2$, $C_{P_4^{(i)}}$ for $1 \leq i \leq 4$, and $C_{P_5^{(i)}}$ for $1 \leq i \leq 6$. If the dimensions are different, the toric codes are certainly not monomially equivalent. Hence we only need to consider $C_{P_5^{(7)}}$ is not monomially equivalent to $C_{P_5^{(i)}}$ for $1 \leq i \leq 6$. In [7], the authors showed that $d(C_{P_5{}^{(1)}}) = (q-1)^2 - 4(q-1), d(C_{P_5{}^{(2)}}) = (q-1)^2 - 3(q-1), d(C_{P_5{}^{(i)}}) = (q-1)^2 - 2(q-1)$, for $3 \leq i \leq 6$. We claim that $d(C_{P_5{}^{(7)}}) = (q-1)^2 - 2(q-1)$. Observe that $d(C_{P_5{}^{(7)}})$ has a subpolygon $P' = \text{conv}\{(-1, 0), (1, 0)\}$. Let $P_1 = \text{conv}\{(-1, 0), (0, 0)\}$, $P_2 = \text{conv}\{(0, 0), (1, 0)\}$. Since $P' = P_1 + P_2$, by Theorem 2.2 we have $d(C_{P_5{}^{(7)}}) \geq d(C_{P_1}) + d(C_{P_2}) - (q-1)^2$ for $q \geq 49$. In view of Theorem 2.3 (with $\ell = 0$) $d(C_{p_i}) = (q-1)^2 - (q-1)$, i = 1,2. So $d(C_{P_5{}^{(7)}}) \geq (q-1)^2 - 2(q-1)$ for $q \geq 49$. On the other hand, we have codewords $\text{ev}(b(x-a_1)(x^{-1}-a_2))$ where $b, a_1, a_2 \in (\mathbb{F}_q^*)^2$ and $a_1 \neq a_2^{-1}$. Since the weight of these codewords are all $(q-1)^2 - 2(q-1)$, so $d(C_{P_5{}^{(7)}}) \leq (q-1)^2 - 2(q-1)$. Therefore for $q \geq 49, d(C_{P_5{}^{(7)}}) = (q-1)^2 - 2(q-1)$. For $5 < q < 49$, we verify directly that $d(C_{P_5{}^{(7)}}) = (q-1)^2 - 2(q-1)$, using the Magma code (or programs) from [5]. The results are given in Table 1.

Table 1 $d(C_{P_5{}^{(7)}}(\mathbb{F}_q))$

q	$d(C_{P_5{}^{(7)}}(\mathbb{F}_q))$	$(q-1)^2 - 2(q-1)$
7	24	24
8	35	35
9	48	48
11	80	80
13	120	120
16	195	195
17	224	224
19	288	288
23	440	440
25	528	528
29	728	728
31	840	840
37	1,224	1,224
41	1,520	1,520
43	1,680	1,680
47	2,024	2,024

Next step is to show that the $C_{P_5^{(7)}}$ with $d = (q-1)^2 - 2(q-1)$ are not monomially equivalent to $C_{P_5^{(i)}}$ for $3 \leq i \leq 6$ with $d = (q-1)^2 - 2(q-1)$. There are two cases to be considered.

Case 1 $C_{P_5^{(7)}}$ is not monomially equivalent to $C_{P_5^{(i)}}$, for $i = 3, 4, 6$.

We need to look at a finer invariant than before. More precisely, $C_{P_5(7)}$ can be distinguished from the $C_{P_5(3)}$,$C_{P_5(4)}$ and $C_{P_5(6)}$ by the number of words of minimum weight. In $C_{P_5(7)}$, there are two different sets of three collinear lattice points while in the $C_{P_5(i)}$ for $i = 3, 4, 6$ there is only one. This means that there will be more codewords of the minimum weight in $C_{P_5(7)}$ than those in $C_{P_5(i)}$ for $i = 3, 4, 6$. $C_{P_5(7)}$ has at least $2\binom{q-1}{2}(q-1)$ such codewords because there are two distinct families of reducible functions: $b(x - a_1)(x^{-1} - a_2)$ with $b, a_i \in \mathbb{F}_q^*$ and $a_1 \neq a_2^{-1}$, and $b(y - a_1)(y^{-1} - a_2)$ with $b, a_i \in \mathbb{F}_q^*$ and $a_1 \neq a_2^{-1}$. Since each of these two families of functions has (a_1, b_i) and (a_2^{-1}, b_i), $b_i \in \mathbb{F}_q^*$ or (b_i, a_1) and (b_i, a_2^{-1}), $b_i \in \mathbb{F}_q^*$ zeroes, so they give minimal weight . On the other hand, in [7], the authors showed that $C_{P_5(i)}$ for $i = 3, 4, 6$ have only $\binom{q-1}{2}(q-1)$ such codewords for sufficient large q. For q small, the number of such codewords maybe more than $\binom{q-1}{2}(q-1)$, but it is strictly less than $2\binom{q-1}{2}(q-1)$ (see Table 2). Therefore $C_{P_5^{(7)}}$ is not monomially equivalent to $C_{P_5^{(i)}}$, for $i = 3, 4, 6$.

Case 2 $C_{P_5^{(7)}}$ is not monomially equivalent to $C_{P_5^{(5)}}$.

In this case, since both $C_{P_5(7)}$ and $C_{P_5(5)}$ have two different sets of three collinear lattice points, so we should use the more symmetry geometry properties of polygon $P_5^{(7)}$ which means $C_{P_5(7)}$ has more codewords of minimum weight theoretically.

For $C_{P_5(5)}$, there are two different sets of three collinear lattice points. This means that $C_{P_5(5)}$ has at least $2\binom{q-1}{2}(q-1)$ codewords of minimum weight $(q-1)^2-2(q-1)$, because there are two different families of reducible polynomials: $b(x - a_1)(x - a_2)$ with $b, a_1, a_2 \in \mathbb{F}_q^*$ and $a_1 \neq a_2$ and $b(y - a_1)(y^{-1} - a_2)$ with $b, a_1, a_2 \in \mathbb{F}_q^*$ and $a_1 \neq a_2^{-1}$. In fact, for any $q > 5$ we claim that there are exactly $2\binom{q-1}{2}(q-1)$ such codewords. Firstly we prove that for sufficiently large q, there are exactly $2\binom{q-1}{2}(q-1)$ such codewords. We claim that codewords of minimum weight $(q-1)^2 - 2(q-1)$ come only from evaluations $\mathrm{ev}(b(x - a_1)(x - a_2))$ and $\mathrm{ev}(b(y - a_1)(y^{-1} - a_2))$. To see this we need to show that any other such codewords could come only from evaluating a linear combination $a + bx + cx^2 + dy + ey^{-1}$ of $\{1, x, x^2, y, y^{-1}\}$, in which x^2, y, y^{-1} all appear with nonzero coefficients. If $c = 0$, since $P_5^{(5)}$ with the vertex x^2 deleted is lattice equivalent to $P_4{}^{(2)}$, so we may consider $\mathrm{ev}(a + bx + dy + ey^{-1})$ as a codeword of $C_{P_4{}^{(2)}}$. From [7] we know that all the minimum codewords of $C_{P_4{}^{(2)}}$ are the $\mathrm{ev}(b(x - a_1)(x - a_2))$ with $b, a_1, a_2 \in \mathbb{F}_q^*$ and $a_1 \neq a_2$ which are in a previous covered case. Thus $c \neq 0$. Similarly we can show that $d \neq 0$ and $e \neq 0$. Since $c, d, e \neq 0$, so $a+bx+cx^2+dy+ey^{-1}$ defines a curve $ay+bxy+cx^2y+dy^2+e = 0$ and this curve is absolutely irreducible, of arithmetic genus $P_a \leq 1$ (because of the one interior lattice points in this case, see Theorem 2.10). If $P_a = 1$, by Theorem

Table 2 Weight enumerators

Over $\mathbb{F}_7$

$P_5^{(3)}: 1+90x^{24}+648x^{25}+\cdots$

$P_5^{(4)}: 1+90x^{24}+216x^{25}+\cdots$

$P_5^{(5)}: 1+180x^{24}+324x^{26}+\cdots$

$P_5^{(6)}: 1+90x^{24}+432x^{26}+\cdots$

$P_5^{(7)}: 1+288x^{24}+108x^{26}+\cdots$

Over $\mathbb{F}_8$

$P_5^{(3)}: 1+147x^{35}+1029x^{36}+\cdots$

$P_5^{(4)}: 1+147x^{35}+343x^{36}+\cdots$

$P_5^{(5)}: 1+294x^{35}+343x^{37}+\cdots$

$P_5^{(6)}: 1+147x^{35}+1029x^{37}+\cdots$

$P_5^{(7)}: 1+294x^{35}+343x^{36}+\cdots$

Over $\mathbb{F}_9$

$P_5^{(3)}: 1+224x^{48}+1536x^{49}+\cdots$

$P_5^{(4)}: 1+224x^{48}+512x^{49}+\cdots$

$P_5^{(5)}: 1+448x^{48}+512x^{51}+\cdots$

$P_5^{(6)}: 1+224x^{48}+512x^{50}+\cdots$

$P_5^{(7)}: 1+704x^{48}+256x^{50}+\cdots$

Over $\mathbb{F}_{11}$

$P_5^{(3)}: 1+450x^{80}+3000x^{81}+\cdots$

$P_5^{(4)}: 1+450x^{80}+1000x^{81}+\cdots$

$P_5^{(5)}: 1+900x^{80}+1500x^{84}+\cdots$

$P_5^{(6)}: 1+650x^{80}+1000x^{82}+\cdots$

$P_5^{(7)}: 1+1400x^{80}+500x^{82}+\cdots$

Over $\mathbb{F}_{13}$

$P_5^{(3)}: 1+792x^{120}+5184x^{121}+\cdots$

$P_5^{(4)}: 1+792x^{120}+1728x^{121}+\cdots$

$P_5^{(5)}: 1+1584x^{120}+7776x^{126}+\cdots$

$P_5^{(6)}: 1+792x^{120}+1728x^{125}+\cdots$

$P_5^{(7)}: 1+2448x^{120}+864x^{122}+\cdots$

Over $\mathbb{F}_{16}$

$P_5^{(3)}: 1+1575x^{195}+10125x^{196}+\cdots$

$P_5^{(4)}: 1+1575x^{195}+3375x^{196}+\cdots$

$P_5^{(5)}: 1+3150x^{195}+13500x^{203}+\cdots$

$P_5^{(6)}: 1+2250x^{195}+13500x^{203}+\cdots$

$P_5^{(7)}: 1+3150x^{195}+3375x^{196}+\cdots$

Over $\mathbb{F}_{17}$

$P_5^{(3)}: 1+1920x^{224}+12288x^{225}+\cdots$

$P_5^{(4)}: 1+1920x^{224}+4096x^{225}+\cdots$

$P_5^{(5)}: 1+3840x^{224}+5120x^{232}+\cdots$

Table 2 continued

$P_5{}^{(6)}: 1+1920x^{224}+4096x^{230}+\cdots$
$P_5{}^{(7)}: 1+5888x^{224}+2048x^{226}+\cdots$
Over $\mathbb{F}_{19}$
$P_5{}^{(3)}: 1+2754x^{288}+17496x^{289}+\cdots$
$P_5{}^{(4)}: 1+2754x^{288}+5832x^{289}+\cdots$
$P_5{}^{(5)}: 1+5508x^{288}+32076x^{298}+\cdots$
$P_5{}^{(6)}: 1+2754x^{288}+5832x^{294}+\cdots$
$P_5{}^{(7)}: 1+8424x^{288}+2916x^{290}+\cdots$
Over $\mathbb{F}_{23}$
$P_5{}^{(3)}: 1+5082x^{440}+31944x^{441}+\cdots$
$P_5{}^{(4)}: 1+5082x^{440}+10648x^{441}+\cdots$
$P_5{}^{(5)}: 1+5508^{195}+32076x^{298}+\cdots$
$P_5{}^{(6)}: 1+5082x^{440}+154396x^{450}+\cdots$
$P_5{}^{(7)}: 1+15488x^{440}+5324x^{442}+\cdots$

2.9 there are at most $1+q+2\sqrt{q}$ rational points in such curve. a simple argument shows that $1+q+2\sqrt{q} < 2q-2$ for all $q \geq 11$. This means that the weight of corresponding codewords is at least $(q-1)^2-(1+q+2\sqrt{q}) > (q-1)^2-2(q-1)$. Similarly, if $P_a = 0$, then there are $1+q$ rational points in such curve. Note that for $q > 5$, $1+q < 2q-2$, so the weight of corresponding codewords is at least $(q-1)^2-(1+q) > (q-1)^2-2(q-1)$. Hence there are exactly $2\binom{q-1}{2}(q-1)$ codewords of minimum weight $(q-1)^2-2(q-1)$, for $q \geq 11$. Secondly for smaller values of q, we verify directly from the weight enumerators of $C_{P_5{}^{(5)}}(\mathbb{F}_q)$, to see that the number of codewords of minimum weight also satisfies $2\binom{q-1}{2}(q-1)$ (see Table 2).

We now claim that $C_{P_5{}^{(5)}}$ contains no codewords of weight $(q-1)^2-(2q-3)$. Firstly If q is sufficiently large, we show that $C_{P_5{}^{(5)}}$ contains no codewords of weight $(q-1)^2-(2q-3)$. Similarly as above, we shall show that any such codewords could come only from a linear combination $a+bx+cx^2+dy+ey^{-1}$ of $\{1, x, x^2, y, y^{-1}\}$ in which x^2, y, y^{-1} all appear with nonzero coefficients. If $c = 0$, we may consider $\mathrm{ev}(a+bx+dy+ey^{-1})$ as a codeword of $C_{P_4{}^{(2)}}$. We know that $C_{P_4{}^{(2)}}$ does not have codeword of weight $(q-1)^2-(2q-3)$ [7]. Thus $c \neq 0$. Similarly we can show that $d \neq 0$ and $e \neq 0$. Since $c, d, e \neq 0$, so $a+bx+cx^2+dy+ey^{-1}$ defines a curve $ay+bxy+cx^2y+dy^2+e$ and this curve is absolutely irreducible, of arithmetic genus $P_a \leq 1$ as before. If $P_a = 1$, by Theorem 2.9 there are at most $1+q+2\sqrt{q}$ rational points in such curve. a simple argument shows that $1+q+2\sqrt{q} < 2q-3$ for all $q \geq 11$. This means that the weight of corresponding codewords is at least $(q-1)^2-(1+q+2\sqrt{q}) > (q-1)^2-(2q-3)$. Similarly, if $P_a = 0$, then there are $1+q$ rational points in such curve. Note that for $q > 5$, $1+q < 2q-3$, so the weight of corresponding codewords is at least $(q-1)^2-(1+q) > (q-1)^2-(2q-3)$. Hence there are no codewords of weight $(q-1)^2-(2q-3)$ for $q \geq 11$. Secondly for smaller values of q we again verify directly that $C_{P_5{}^{(5)}}(\mathbb{F}_q)$ does not have codewords of weight

$(q-1)^2-(2q-3)$ (see Table 2). Therefore $C_{P_5^{(5)}}(\mathbb{F}_q)$ contains no codewords of weight $(q-1)^2-(2q-3)$ for any $q>5$.

For $C_{P_5^{(7)}}$, we assume α is a primitive element of $\mathbb{F}_q$, then $(\mathbb{F}_q)^* = \langle 1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\rangle$ is a cyclic group. There are two cases to be considered.

Case A $C_{P_5^{(7)}}$ over $\mathbb{F}_q$ where $q \neq 2^m, m>3$.

We claim that in this case $C_{P_5^{(7)}}$ cannot be monomially equivalent to $C_{P_5^{(5)}}$ over $\mathbb{F}_q$ where $q \neq 2^m, m>3$.

Since $C_{P_5^{(5)}}$ has exactly $2\binom{q-1}{2}(q-1)$ codewords of minimum weight, so we only need to show that the number such codewords in $C_{P_5^{(7)}}$ is strictly more $2\binom{q-1}{2}(q-1)$. If we translate $P_5^{(7)}$ by (1,1) to place it in $\square_{q-1}$, then we evaluate polynomials in $\mathrm{Span}\{x, y, xy, x^2y, xy^2\}$ to get the codewords of the corresponding code which is monomially equivalent to $C_{P_5^{(7)}}$. Observe that there are three distinct families of polynomials: $bx(y-a_1)(y-a_2)$ with $b, a_1, a_2 \in \mathbb{F}_q^*$ and $a_1 \neq a_2$, $by(x-a_1)(x-a_2)$ with $b, a_1, a_2 \in \mathbb{F}_q^*$ and $a_1 \neq a_2$, and $b(y-a_1x)(a_2-xy)$ with $b, a_1, a_2 \in \mathbb{F}_q^*$, $a_1 \neq a_2$ and $\frac{a_1}{a_2} \neq \alpha^{2i}$ for $1 \leq i \leq q-2$. It should be pointed out that the third family does not always yield codewords of weight $(q-1)^2-2(q-1)$. It depends on the field $\mathbb{F}_q$. The point is whether the curves $y=a_1x$ and $xy=a_2$ can intersect in the torus T, and that happens if and only if $x^2=\frac{a_2}{a_1}$, or $\frac{a_2}{a_1}$ is a square in $\mathbb{F}_q$. Equivalently, $\frac{a_1}{a_2}=\alpha^{2i}$, for some i, $1 \leq i \leq q-2$.

In case $q \neq 2^m$, and we can find a pair $(a_1, a_2) \in (\mathbb{F}_q^*)^2$ such that a_1, a_2 satisfy $a_1 \neq a_2$, $\frac{a_1}{a_2} \neq \alpha^{2i}$ for $1 \leq i \leq q-2$, for instance, $(a_1, a_2) = (\alpha, 1)$ is such a pair. For any such pair, we can get $q-1$ polynomials $b(y-a_1x)(a_2-xy)$ whose evaluation correspond codewords of minimum weight $(q-1)^2-2(q-1)$. Noting that the number of codewords of the first two families is $2\binom{q-1}{2}(q-1)$, thus $C_{P_5^{(7)}}$ has strictly more than $2\binom{q-1}{2}(q-1)$ codewords of minimum weight, while $C_{P_5^{(5)}}$ has only $2\binom{q-1}{2}(q-1)$ such codewords. This means $C_{P_5^{(7)}}$ cannot be monomially equivalent to $C_{P_5^{(5)}}$.

Case B $C_{P_5^{(7)}}$ over $\mathbb{F}_q$ where $q=2^m, m>3$.

We claim that in this case $C_{P_5^{(7)}}$ cannot be monomially equivalent to $C_{P_5^{(5)}}$ over $\mathbb{F}_q$ where $q=2^m, m>3$.

In this case, we cannot find a pair $(a_1, a_2) \in (\mathbb{F}_q^*)^2$ such that a_1, a_2 satisfy $a_1 \neq a_2, \frac{a_1}{a_2} \neq \alpha^{2i}$ for $1 \leq i \leq q-2$. This implies $C_{P_5^{(7)}}$ and $C_{P_5^{(5)}}$ have the same number of codewords of minimum weight. Since $C_{P_5^{(5)}}$ contains no codewords of weight $(q-1)^2-(2q-3)$, so if we can prove that there exists at least one codeword of weight $(q-1)^2-(2q-3)$ in $C_{P_5^{(7)}}$, then $C_{P_5^{(7)}}$ is not monomially equivalent to $C_{P_5^{(5)}}$. The existence of such codewords can be constructed in the following way. Let $(a_1, a_2) = (1, \alpha)$, the zeroes of $(y-x)(\alpha-xy)$ is

$$\{(\alpha^i, \alpha^i), i=0,1,\ldots,2^m-2\,; (\alpha^j, \alpha^{2^m-j}), j=0,1,\ldots,\widehat{2^{m-1}},\ldots,2^m-2\},$$

where $\widehat{2^{m-1}}$ means 2^{m-1} is omitted. Since this set has $(2q-3)$ elements, so $\mathrm{ev}((y-x)(\alpha-xy))$ at $(\mathbb{F}_q^*)^2$ is a codeword of weight $(q-1)^2-(2q-3)$ in $C_{P_5^{(7)}}$.

Remark Table 2 gives the first three nonzero terms in the weight enumerators:

$$W_C(x) = \sum_{i=0}^{(q-1)^2} A_i x^i,$$

where $A_i = |\{w \in C : wt(w) = i\}|$, for the $k = 5$ toric codes with $d = (q-1)^2 - 2(q-1)$. These were all computed using Magma code from [5].

References

1. Aubry, Y., Perret, M.: A Weil theorem for singular curves. In: Pellikaan, R., Perret, M., Vladut, S.G. (eds.) Arithmetic, and Coding Theory, pp. 1–7. de Gruyter, Berlin (1996)
2. Beelen, P., Pellikaan, R.: The Newton polygon of plane curves with many rational points. Des. Codes Cryptogr. **21**, 41–67 (2000)
3. Hansen, J.P.: Toric surfaces and error-correcting codes. In: Coding Theory, Cryptography and Related Areas (Guanajuato, 1998), pp. 132–142. Springer, Berlin (2000)
4. Hansen, J.P.: Toric varities Hirzebruch surfaces and error-correcting codes. Appl. Algebra Eng. Commun. Comput. **13**, 289–300 (2002)
5. Joyner, D.: Toric codes over finite fields. Appl. Algebra Eng. Commun. Comput. **15**, 63–79 (2004)
6. Little, J., Schenck, H.: Toric surface codes and Minkowski sums. SIAM J. Discret. Math. **20**, 999–1014 (2006)
7. Little, J., Schwarz, R.: On toric codes and multivariate vandermonde matrices. Appl. Algebra Eng. Commun. Comput. **18**, 349–367 (2007)
8. Ruano, D.: On the parameters of r-dimensional toric codes (arXiv:math.AG/ 0512285)