REMARKS ON GENERALIZED TORIC CODES

JOHN LITTLE

Abstract. This note presents some new information on how the minimum distance of the generalized toric code corresponding to a fixed set of integer lattice points $S \subset \mathbb{R}^2$ varies with the base field. The main results show that in some cases, over sufficiently large fields, the minimum distance of the code corresponding to a set S will be the same as that of the code corresponding to the convex hull $\mathrm{conv}(S)$. In an example, we will also discuss a $[49, 12, 28]$ generalized toric code over $\mathbb{F}_8$, better than any previously known code according to M. Grassl's online tables, as of September 2011.

1. Introduction

We consider linear block codes over finite fields $\mathbb{F}_q$, that is, vector subspaces $C \subset \mathbb{F}_q^n$. Following standard notation in coding theory, n will always denote the block length, and k will always denote the dimension of C as a vector space over $\mathbb{F}_q$. An $[n, k, d]$ code is a linear code with block length n, dimension k and minimum distance d. The book [9] is a good general reference for other coding theory concepts.

Toric codes are a class of m-dimensional cyclic codes introduced by J. Hansen in [7], [8]. Hansen's description uses the geometry of toric varieties corresponding to polytopes, but toric codes may also be understood within the general context of evaluation codes.

Definition 1.1. Let P be a rational polytope (the convex hull of a finite set of integer lattice points), contained in $[0, q-2]^m \subset \mathbb{R}^m$. Let $\mathbb{F}_q$ be a finite field with primitive element α. For $f \in \mathbb{Z}^m$ with $0 \leq f_i \leq q-2$ for all i, let $p_f = (\alpha^{f_1}, \ldots, \alpha^{f_m})$ in $(\mathbb{F}_q^{\times})^m$. For any $e = (e_1, \ldots, e_m) \in P \cap \mathbb{Z}^m$, let x^e be the corresponding monomial and write

$$(p_f)^e = (\alpha^{f_1})^{e_1} \cdots (\alpha^{f_m})^{e_m} = \alpha^{\langle f, e \rangle}.$$

The toric code over the field $\mathbb{F}_q$ associated to P, denoted by $C_P(\mathbb{F}_q)$, is the linear code of block length $n = (q-1)^m$ with generator matrix

$$G = ((p_f)^e).$$

The rows are indexed by the $e \in P \cap \mathbb{Z}^m$, and the columns are indexed by the $p_f \in (\mathbb{F}_q^{\times})^m$. In other words, letting $L = \mathrm{Span}\{x^e : e \in P \cap \mathbb{Z}^m\}$, we define the evaluation mapping

$$\begin{aligned} \mathrm{ev} : L &\to \mathbb{F}_q^{(q-1)^m} \\ g &\mapsto (g(p_f) : p_f \in (\mathbb{F}_q^{\times})^m) \end{aligned}$$

Then $C_P(\mathbb{F}_q) = \mathrm{ev}(L)$.

Date: September 12, 2011.
2000 *Mathematics Subject Classification.* Primary 94B27; Secondary 52B20, 14M25.
Key words and phrases. coding theory, toric code, Minkowski length.

If P is the interval $[0, \ell-1] \subset \mathbb{R}$, then $C_P(\mathbb{F}_q)$ is the Reed-Solomon code $RS(\ell, q)$. So toric codes are, in a sense, generalizations of Reed-Solomon codes.

In considering code equivalences, the description of dual codes of toric codes, minimum distance bounds, etc. (see the articles cited below), one is naturally led to consider "generalized" toric codes, defined by the same construction, but using an arbitrary set S of integer lattice points in $[0, q-2]^m \subset \mathbb{R}^m$ instead of the set of all lattice points in a convex polytope. We will use the parallel notation $C_S(\mathbb{F}_q)$ for these codes. If $P = \mathrm{conv}(S)$, then the code $C_S(\mathbb{F}_q)$ is a subcode of $C_P(\mathbb{F}_q)$. In algebraic geometry terms, the $C_S(\mathbb{F}_q)$ can be defined using an incomplete linear system $V \subset |\mathcal{O}_{X_P}(D_P)|$, where X_P is the toric variety determined by P and D_P is the corresponding divisor class on X_P.

The survey [13] covers most of the work on these codes contained in [11], [12], [14], [15], [17], and [1]. Not all toric codes or generalized toric codes are as good as Reed-Solomon codes from the coding theory perspective, but the class of generalized toric codes does contain some very good codes. See §2 below for a new example.

From now on we will concentrate on the case $m = 2$. The principal new results of this note are some observations about the way the minimum distance of the generalized toric code $C_S(\mathbb{F}_q)$ depends on q and how it relates to the minimum distance of $C_P(\mathbb{F}_q)$ if $P = \mathrm{conv}(S)$ and q is large enough. These rely on the connection between the minimum distance of toric codes and Minkowski sum decompositions of subpolytopes $Q \subset P$ first noticed by Little and Schenck in [12] and later developed and refined by Soprunov and Soprunova in [17]. The other ingredient is some statements about the distribution of polynomials in $\mathbb{F}_q[u]$ with given factorization patterns from [2].

The main result will say that in many situations, and for large enough q, the "missing" lattice points in $(P \cap \mathbb{Z}^n) \setminus S$ do not always help, in the sense that $d(C_{S'}(\mathbb{F}_q))$ can equal $d(C_S(\mathbb{F}_q))$ for many $S' \supsetneq S$. In particular, there are even situations where $S' = P \cap \mathbb{Z}^n$ gives a code with the same minimum distance over all $\mathbb{F}_q$ with sufficiently large characteristic. Read one way, for a fixed polytope P, our results say that the generalized toric codes for $S \subset P$ tend to give interesting results only over small fields. On the other hand, these results also can help to identify situations when a proper supercode of a generalized toric code has the same minimum distance. Hence they can be used to find improved examples with the same d but a higher code rate k/n.

To conclude, we will also make some remarks about the toric and generalized toric codes from the "exceptional triangle" T_0 studied in [17] and the set S obtained by deleting the interior lattice point. In this case, when certain coefficients are nonzero, the polynomials that are evaluated to produce the codewords define elliptic curves. Some facts about numbers of points on elliptic curves over finite fields provide some interesting results in this case and provide some extra detail concerning the Minkowski decompositions in [17]. In this case, we will see that the pattern of how $C_S(\mathbb{F}_q)$ depends on q is considerably more intricate.

2. A new best known code

One of the reasons for the interest in the toric code construction is that a number of isolated examples of very good codes have been produced this way. For instance, using certain heuristic search methods, students at the MSRI-UP 2009 REU program found

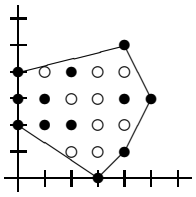

FIGURE 1. The set S and the polygon P in Example 2.1.

- an $m = 3$ generalized toric code over $\mathbb{F}_5$ with parameters $[64, 8, 42]$, and
- an $m = 2$ generalized toric code over $\mathbb{F}_8$ with parameters $[49, 8, 34]$.

(Both are reported in [4] and, as of September 2011, are still the best known codes for these n, k over these fields.)

Here is a new, similar, example.

Example 2.1. Consider the generalized toric code over $\mathbb{F}_8$ corresponding to the set

$$S = \{(3,0), (4,1), (0,2), (1,2), (2,2), (0,3), (1,3), (4,3), (5,3), (0,4), (2,4), (4,5)\},$$

marked with solid circles in Figure 1. The polygon P is the convex hull of S, and contains nine lattice points other than the points of S, shown as empty circles.

There are reducible sections of the line bundle $\mathcal{O}_{X_P}(D_P)$ of the form

$$f(x,y) \equiv y^3x^4(x-\alpha_1)(x-\alpha_2)(x-\alpha_3) \bmod \langle x^7-1, y^7-1\rangle$$

with the α_i distinct and $\alpha_1+\alpha_2+\alpha_3 = 0$. Since these have exactly 21 zeroes at the points in $(\mathbb{F}_8^\times)^2$, we see $d(C_S(\mathbb{F}_8)) \le 28$. Using David Joyner's Magma procedures for toric codes ([11]), it can be checked that this is a $[49, 12, 28]$ code over $\mathbb{F}_8$. In other words, polynomials in two variables that are linear combinations of the 12 monomials corresponding to the points in S can have at most 21 zeroes at the points in $(\mathbb{F}_8^\times)^2$. This improves the $[49, 12, 27]$ code previously known according to [4]. $\diamondsuit$

3. Factorization patterns for polynomials in one variable

In this section, we will adapt some known facts about the distribution of polynomials in $\mathbb{F}_q[u]$ with given factorization patterns. The original source for these statements is [2]; the survey [5] also contains a summary and discussion of the results we need.

Let $q = p^h$ and consider any linear family $\mathcal{F}$ of polynomials of the form

$$f(u) = u^\ell + t_1u^{k_1} + \cdots + t_{m-1}u^{k_{m-1}} + t_m \tag{3.1}$$

in $\mathbb{F}_q[u]$, where

(1) $p > \ell$,
(2) the exponents $\ell > k_1 > \cdots > k_{m-1} > k_m = 0$ are fixed,
(3) the coefficients t_i, $1 \le i \le m$ run over the finite field $\mathbb{F}_q$, and
(4) the $\ell, k_1, \ldots, k_{m-1}$ are *not* all multiples of some fixed integer $j > 1$.

Some natural questions in this context are:

- What can be said about the number of elements of the family $\mathcal{F}$ that are irreducible in $\mathbb{F}_q[u]$?

- More generally, what can be said about the number of elements of the family $\mathcal{F}$ that factor in $\mathbb{F}_q[u]$ into a given number of factors of given degrees?

To describe the situation for the second question, we will say that a polynomial $f(u)$ of degree ℓ has factorization pattern

$$\lambda = 1^{a_1} 2^{a_2} \cdots \ell^{a_\ell},$$

where $\sum_{i=1}^{\ell} a_i \cdot i = \ell$, if in $\mathbb{F}_q[u]$, $f(u)$ factors as a product of a_i irreducible factors of degree i (not necessarily distinct) for each $i = 1, \dots, \ell$. Let

$$T(\lambda) = \frac{1}{a_1! \cdots a_\ell! 1^{a_1} \cdots \ell^{a_\ell}}$$

be the proportion of elements of the symmetric group S_n with cycle decomposition of shape λ. Then S. Cohen proved the following statement.

Theorem 3.1 ([2, Theorem 3])**.** *Let $\mathcal{F}$ satisfy the conditions above, and let $\mathcal{F}_\lambda$ be the subset of $\mathcal{F}$ consisting of polynomials with factorization pattern λ in $\mathbb{F}_q[u]$. Then for all q sufficiently large,*

$$|\mathcal{F}_\lambda| = T(\lambda) q^m + O\left(q^{m-\frac{1}{2}}\right) \tag{3.2}$$

where the implied constant depends only on ℓ.

For our applications, we want to study factorizations of shape $\lambda = \lambda_0 := 1^\ell$ where, in addition,

$$f(u) = \prod_{i=1}^{\ell} (u - \beta_i)$$

with β_i distinct in $\mathbb{F}_q^\times$. Now the elements of the family $\mathcal{F}$ with repeated roots (possibly in some extension of $\mathbb{F}_q$) correspond to $\mathbb{F}_q$-rational points

$$(t_1, \dots, t_m) \subset \mathcal{D}_\mathcal{F},$$

where $\mathcal{D}_\mathcal{F} = V(\Delta_\mathcal{F})$ and

$$\Delta_\mathcal{F} = \text{resultant}(f(u), f'(u), u)$$

is the discriminant of the family. Note that $\mathcal{D}_\mathcal{F}$ is an $(m-1)$-dimensional affine hypersurface, singular and possible reducible. However, when the characteristic p is large enough, it is known by [3, Theorem 3.1] that when the two conditions after (3.1) hold, $\mathcal{D}_\mathcal{F}$ can have at most one irreducible component other than the hyperplane $V(t_m)$. By the general bound in [6, Proposition 12.1], it follows that

$$|D_\mathcal{F}(\mathbb{F}_q)| \le \delta \pi_{m-1}, \tag{3.3}$$

where $\pi_{m-1} = |\mathbb{P}^{m-1}(\mathbb{F}_q)| = q^{m-1} + q^{m-2} + \cdots + q + 1$, and $\delta = \deg \Delta_\mathcal{F} \le 2\ell - 2$. (The bound (3.3), while sufficient for our purposes, is very weak. Tighter bounds based on a version of the Weil conjectures for singular varieties can also be found in [6].) We have the following result.

Corollary 3.2. *If $p > \ell$ and $q = p^h$ is sufficiently large, there exist elements of the family $\mathcal{F} \subset \mathbb{F}_q[u]$ with factorization pattern $\lambda_0 = 1^\ell$ in which the irreducible factors are distinct, and for which all the roots are nonzero.*

Proof. The first part of this comes from comparing the orders of growth of the various terms in (3.2) and (3.3). The last part of this is clear since if any of the roots is zero, then the coefficient $t_m = 0$, and the locus where that is true has dimension $m - 1$. □

Note that in particular the conclusion of the Corollary holds for all sufficiently large primes p. Hence there will be elements of the family $\mathcal{F} \subset \mathbb{F}_p[u]$ with factorization pattern $\lambda_0 = 1^\ell$ in which the irreducible factors are distinct and for which all the roots are nonzero.

Remark 3.3. If p does not satisfy the condition $p > \ell$, or if the conclusion of the Corollary does not hold for some q, it is still always possible to find a finite extension of $\mathbb{F}_q$ for which the statement of the Corollary holds. Namely, let $f(u)$ be any one element of $\mathcal{F}$ with nonzero discriminant and nonzero constant term. If K is a splitting field for $f(u)$ over $\mathbb{F}_q$, then $f(u)$ splits completely with nonzero roots in $K[u]$.

Example 3.4. Consider the family $\mathcal{F}$ consisting of polynomials of the form

$$u^4 + t_1 u + t_2$$

in $\mathbb{F}_p[u]$ for prime p. Note that $\mathcal{F}$ contains elements of factorization pattern $\lambda_0 = 1^4$ with $t_1 = 0$ whenever $p \equiv 1 \bmod 4$, since then $\mathbb{F}_p^\times$ contains 4th roots of unity. Doing computations in the Maple computer algebra system, we found that for all except 5 of the primes $p < 1000$ and all $p > 19$, there are elements of $\mathcal{F}$ of factorization pattern $\lambda_0 = 1^4$, and with distinct roots. The obvious conjecture is that there are such polynomials for all $p > 19$. However, more precise information about the constants in the asymptotic result (3.2) than is currently available would be necessary for a complete proof. When $p \geq 5$, a constant multiple of the discriminant of this family can be written as

$$\Delta_{\mathcal{F}} = \left(\frac{t_1}{4}\right)^4 - \left(\frac{t_2}{3}\right)^3.$$

The variety $\mathcal{D}_{\mathcal{F}} = V(\Delta_{\mathcal{F}})$ is a singular curve of genus 0 in the (t_1, t_2)-plane. There are exactly $p - 1$ pairs (t_1, t_2) with $t_1 t_2 \neq 0$ that make the discriminant equal 0.

One interesting observation is that the number of polynomials of factorization pattern $\lambda_0 = 1^4$, and with distinct roots, is always divisible by $p - 1$. This follows because the mapping $\mathbb{F}_p^\times \times \mathcal{F} \to \mathcal{F}$ defined by

$$(\beta, f(u)) \mapsto \beta^{-4} f(\beta u)$$

defines an action of $\mathbb{F}_p^\times$ on $\mathcal{F}$ that preserves the factorization pattern, and for which all orbits have order $p - 1$. There are similar actions of $\mathbb{F}_q^\times$ on all $\mathcal{F}$ of the form (3.1) studied here, so this is a general phenomenon. ♢

4. Application to generalized toric codes

In this section we will apply Corollary 3.2 to deduce some results about the minimum distance of generalized toric codes. First we recall the main idea developed in [12] and [17]. Given a polytope P, following [17], we define the *full Minkowski length* of P to be

$$L(P) = \max\{\ell \mid \exists Q = Q_1 + \cdots + Q_\ell \subseteq P, \dim Q_i > 0 \text{ all } i\},$$

where the addition signs refer to the Minkowski sum of polytopes. Theorem 2.6 of [17] shows that for toric surface codes ($m = 2$, so $P \subset \mathbb{R}^2$), the full Minkowski length of P is strongly tied to the minimum distance of $C_P(\mathbb{F}_q)$. In fact, if q is larger than an explicit lower bound depending on $L(P)$ and the area of P, then the minimum distance of the toric code $C_P(\mathbb{F}_q)$ is bounded below as follows:

$$d(C_P(\mathbb{F}_q)) \geq (q-1)^2 - L(P)(q-1) - \lfloor 2\sqrt{q} \rfloor + 1, \tag{4.1}$$

and if no maximally decomposable $Q \subset P$ contains an exceptional triangle term (a triangle lattice equivalent to $T_0 = \text{conv}\{(0,0),(1,2),(2,1)\}$), then

$$d(C_P(\mathbb{F}_q)) \geq (q-1)^2 - L(P)(q-1). \tag{4.2}$$

Example 4.1. For instance, consider the polygon P from Example 2.1. It can be seen that $L(P) = 6$ and there is a unique $Q \subset P$ with 6 Minkowski summands, namely the rectangle $Q = \text{conv}\{(0,2),(4,2),(4,4),(0,4)\}$, which is the Minkowski sum of four primitive lattice segments parallel to the x-axis and two primitive lattice segments parallel to the y-axis. The corresponding reducible sections of the line bundle $\mathcal{O}_{X_P}(D_P)$ have the form

$$y^2(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)(y-\beta_1)(y-\beta_2).$$

So in fact for q large enough, we will have

$$d(C_P(\mathbb{F}_q)) = (q-1)^2 - 6(q-1) + 8$$

in this case. $\diamondsuit$

Suppose we are in the relatively common case in which the minimum weight words in the toric code $C_P(\mathbb{F}_p)$ or $C_P(\mathbb{F}_q)$ come by evaluating polynomials that are linear combinations of monomials corresponding to a collinear string of ℓ consecutive lattice points in the polytope. This gives $Q = Q_1 + \cdots + Q_\ell \subset P$ (a Minkowski sum of ℓ primitive line segments). Say the corresponding monomials are

$$u^a, \ldots, u^{\ell+a}$$

for some monomial $u = x^r y^s$ with $\gcd(r,s) = 1$, and some integers ℓ and $a \geq 0$. The minimum weight codewords then are obtained by evaluating completely reducible polynomials in u:

$$u^a(u-\alpha_1)\cdots(u-\alpha_\ell)$$

where $\alpha_i \in \mathbb{F}_q^\times$ are distinct.

Now suppose that we remove some of lattice points between the endpoints in going to a subset $S \subset P \cap \mathbb{Z}^m$. The polynomials evaluated to obtain codewords of $C_S(\mathbb{F}_p)$ will contain linear combinations of some monomials u^ℓ and u^{k_i} with $\ell > k_1 > \cdots > k_{m-1} > k_m = 0$ (after removing the factor u^a that has no zeroes in the torus $(\mathbb{F}_p^\times)^2$). We obtain polynomials of the form

$$f(u) = u^\ell + t_1 u^{k_1} + \ldots + t_m. \tag{4.3}$$

Note that $\ell \leq p-2$ here by our convention that $P \subset [0, p-2]^2$. Hence the condition $p > \ell$ is automatically satisfied. In other words, provided that the other conditions on the exponents k_i are satisfied, we have elements of a family $\mathcal{F}$ of the same form as that considered in (3.1). Then Corollary 3.2 immediately implies the following result.

Theorem 4.2. *Let P be an integral convex polygon in $\mathbb{R}^2$ of full Minkowski length $L(P) = \ell$. Suppose in addition that there is a unique $Q \subset P$ which decomposes as a sum of ℓ nonempty polygons, and that each of them is a copy of a primitive lattice segment I, so $Q = \ell I$. Let $S \subset P \cap \mathbb{Z}^2$ satisfy*

(1) *S contains the endpoints of Q, and*
(2) *The k_i and ℓ are not all multiples of any fixed integer $j > 1$.*

Then for all primes p sufficiently large and all $h \geq 1$, letting $q = p^h$, we have

$$d(C_S(\mathbb{F}_q)) = d(C_P(\mathbb{F}_q)) = (q-1)^2 - \ell(q-1).$$

Moreover, for all q, there exists $h \geq 1$ such that the same statement is true if we replace q by q^h.

Note that hypothesis (2) here rules out the case $m = 1$. This is necessary, since polynomials of the form $u^\ell + t_m$ with $t_m \neq 0$ have ℓ distinct roots only when the field contains ℓth roots of unity, or equivalently when $\ell | (q-1)$. The conclusion of the theorem will also be valid in those cases, however. See Example 4.3 below for some examples.

Proof. Corollary 3.2 implies that if p is sufficiently large the family $\mathcal{F}$ as in (4.3) will contain elements of factorization pattern $\lambda_0 = 1^\ell$ with distinct nonzero roots. The corresponding polynomials in x, y obtained by substituting $u = x^r y^s$ will have the same sort of factorization. Since $\gcd(r, s) = 1$, each factor $x^r y^s - \alpha_i$ has exactly $p-1$ zeroes in $(\mathbb{F}_q^\times)^2$ and the sets of roots for distinct α_i are disjoint. Therefore for all sufficiently large p, the toric code will contain words of weight $(p-1)^2 - \ell(p-1)$, and the minimum distance satisfies

$$d(C_S(\mathbb{F}_p)) \leq (p-1)^2 - \ell(p-1).$$

The generalized toric code $C_S(\mathbb{F}_p)$ is a subcode of the code from the full polygon P. The lower bound from [17] quoted above in (4.2) gives the reverse inequality and the equality claimed in the statement follows for all p sufficiently large. The final part here follows by Remark 3.3. □

Related statements along the lines of Theorem 4.2 apply in different situations depending on the shape of the Q giving the maximally Minkowski-decomposable subpolygon of P. However, we will not pursue them here.

Example 4.3. Consider the generalized toric codes $C_S(\mathbb{F}_q)$ for the set S indicated with solid circles in Figure 2.

The polygon P here is the quadrilateral $P = \mathrm{conv}\{(0,0), (2,0), (3,1), (1,4)\}$. It can be seen that the full Minkowski length of P is $L(P) = 4$, and P contains just one Minkowski sum of 4 indecomposable polygons, namely the line segment $Q = \mathrm{conv}\{(1,0), (1,4)\}$. By the results of Example 3.4, and Theorem 4.2, we expect that

$$d(C_S(\mathbb{F}_p)) = d(C_P(\mathbb{F}_p)) = (p-1)^2 - 4(p-1)$$

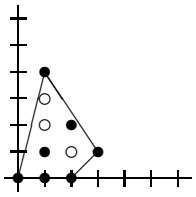

FIGURE 2. The set S and the polygon P in Example 4.3.

for all $p > 19$ and all $q = p^s$ for $s \geq 4$. The following results of Magma computations indicate what happens for $p \leq 19$, and also for the prime powers $7 \leq q \leq 19$:

$$\begin{aligned}
d(C_S(\mathbb{F}_7)) = 18 \quad &\text{vs.} \quad 6^2 - 4 \cdot 6 = 12 \\
d(C_S(\mathbb{F}_8)) = 33 \quad &\text{vs.} \quad 7^2 - 4 \cdot 7 = 21 \\
d(C_S(\mathbb{F}_9)) = 32 \quad &\text{vs.} \quad 8^2 - 4 \cdot 8 = 32 \\
d(C_S(\mathbb{F}_{11})) = 70 \quad &\text{vs.} \quad 10^2 - 4 \cdot 10 = 60 \\
d(C_S(\mathbb{F}_{13})) = 96 \quad &\text{vs.} \quad 12^2 - 4 \cdot 12 = 96 \\
d(C_S(\mathbb{F}_{16})) = 165 \quad &\text{vs.} \quad 15^2 - 4 \cdot 15 = 165 \\
d(C_S(\mathbb{F}_{17})) = 192 \quad &\text{vs.} \quad 16^2 - 4 \cdot 16 = 192 \\
d(C_S(\mathbb{F}_{19})) = 270 \quad &\text{vs.} \quad 18^2 - 4 \cdot 18 = 252.
\end{aligned}$$

Over $\mathbb{F}_7$, there are no polynomials $u^4 + t_1 u + t_2$ with $t_2 \neq 0$ and factorization pattern $\lambda_0 = 1^4$. Since $7 \equiv 1 \bmod 3$, however, $\mathbb{F}_7$ contains cube roots of unity. Hence, minimum weight codewords in that case come from polynomials of the form $xy(y^3 - \beta)$.

Over $\mathbb{F}_8$, the minimum weight codewords come from genus 5 curves with 16 $\mathbb{F}_8$-rational points in the torus $(\mathbb{F}_8^\times)^2$.

The codes over $\mathbb{F}_9, \mathbb{F}_{13}$, and $\mathbb{F}_{17}$ all have $d = (q-1)^2 - 4(q-1)$. Since these q all satisfy $q \equiv 1 \bmod 4$, these fields contain 4th roots of unity and hence there are $u^4 + t_1 u + t_2$ with factorization pattern $\lambda_0 = 1^4$ with $t_1 = 0$ and $t_2 \neq 0$. Minimum weight codewords come from polynomials of the form $x(y^4 - \beta)$ with $\beta \neq 0$.

The code over $\mathbb{F}_{11}$ illustrates the fact that while there are polynomials $u^4 + t_1 u + t_2$ with factorization pattern $\lambda_0 = 1^4$ over this field, all such polynomials have a repeated root. Therefore the minimum codeword weight is $(q-1)^2 - 3(q-1)$ rather than $(q-1)^2 - 4(q-1)$.

The code over $\mathbb{F}_{16}$ illustrates the comment from Remark 3.3. Note that $\mathbb{F}_{16}$ is the splitting field of the polynomial $y^4 + y + 1$ over $\mathbb{F}_2$. Hence we obtain words of weight $15^2 - 4 \cdot 15$ in this code too.

Finally, the code over $\mathbb{F}_{19}$ has some words of weight 270 from evaluation of polynomials $xy(y^3 - \beta)$ since $19 \equiv 1 \bmod 3$. (There are also several polynomials $y^4 + t_1 y + t_2$ that have factorization patterns $\lambda_0 = 1^4$. However all of the polynomials that do factor that way have repeated roots.) $\diamondsuit$

5. The exceptional triangle

We will now consider what happens for polygons P where a maximal Minkowski-decomposable subpolygon Q has a Minkowski decomposition involving the triangle $T_0 = \text{conv}\{(0,0), (1,2), (2,1)\}$. This is affine equivalent to the triangle used in [17]

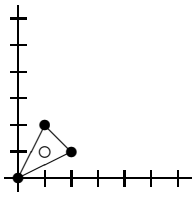

FIGURE 3. The exceptional triangle T_0 and the set S.

(see Figure 3). We will use this form because of its relation to the well-known Hessian family of elliptic curves.

This is the only case in the plane where a Minkowski-indecomposable polygon contains an interior lattice point, namely $(1,1)$. Hence we will begin by comparing $d(C_{T_0}(\mathbb{F}_q))$ and $d(C_S(\mathbb{F}_q))$ where $S = \{(0,0),(1,2),(2,1)\}$, omitting the interior lattice point. The presence of the interior lattice point in $T_0 \cap \mathbb{Z}^2$ shows that we are considering curves of (arithmetic) genus 1. Hence the theory of elliptic curves will be important. The facts about elliptic curves over finite fields that we will need can be found in [16] and [10].

The projective completions of the curves defined by the linear combinations of monomials corresponding to the lattice points in T_0 form the family of cubic curves defined by homogeneous equations:

$$ax^2y + bxy^2 + cxyz + dz^3 = 0. \tag{5.1}$$

If at least one of the coefficients a, b, d vanishes, there are at most $q-1$ affine $\mathbb{F}_q$-rational points with nonzero coordinates on the corresponding curve. It follows that

$$d(C_{T_0}(\mathbb{F}_q)) \leq (q-1)^2 - (q-1)$$

and similarly

$$d(C_S(\mathbb{F}_q)) \leq (q-1)^2 - (q-1). \tag{5.2}$$

Hence, we want to concentrate on the cases with $abd \neq 0$, but c possibly 0 in the case of T_0, and $c = 0$ for the case of S. Thinking along the lines of our earlier results, we pose the following question.

Question 5.1. For sufficiently large primes p, or sufficiently high powers $q = p^h$, is

$$d(C_S(\mathbb{F}_q)) = d(C_{T_0})?$$

Equivalently, do we expect curves in the family (5.1) with $c = 0$ to achieve the maximum number of $\mathbb{F}_p$- or $\mathbb{F}_q$-rational points (among curves in the family)?

Example 5.2. Some experimentation using Magma reveals that the answer to this question is not at all clear at first. As in the discussion above, T_0 is the exceptional

triangle, and S is the set of vertices, omitting the interior lattice point.

$$\begin{aligned}
d(C_S(\mathbb{F}_5)) = 12 \quad &\text{vs.} \quad d(C_{T_0}(\mathbb{F}_5)) = 10\\
d(C_S(\mathbb{F}_7)) = 27 \quad &\text{vs.} \quad d(C_{T_0}(\mathbb{F}_7)) = 27\\
d(C_S(\mathbb{F}_8)) = 42 \quad &\text{vs.} \quad d(C_{T_0}(\mathbb{F}_8)) = 40\\
d(C_S(\mathbb{F}_9)) = 56 \quad &\text{vs.} \quad d(C_{T_0}(\mathbb{F}_9)) = 52\\
d(C_S(\mathbb{F}_{11})) = 90 \quad &\text{vs.} \quad d(C_{T_0}(\mathbb{F}_{11})) = 85\\
d(C_S(\mathbb{F}_{13})) = 126 \quad &\text{vs.} \quad d(C_{T_0}(\mathbb{F}_{13})) = 126\\
d(C_S(\mathbb{F}_{16})) = 207 \quad &\text{vs.} \quad d(C_{T_0}(\mathbb{F}_{16})) = 204\\
d(C_S(\mathbb{F}_{17})) = 240 \quad &\text{vs.} \quad d(C_{T_0}(\mathbb{F}_{17})) = 235\\
d(C_S(\mathbb{F}_{19})) = 300 \quad &\text{vs.} \quad d(C_{T_0}(\mathbb{F}_{19})) = 300\\
d(C_S(\mathbb{F}_{23})) = 462 \quad &\text{vs.} \quad d(C_{T_0}(\mathbb{F}_{23})) = 454.
\end{aligned}$$

Note that the minimum distance of the code from S is sometimes greater, and sometimes the same as the minimum distance of the code from T_0. $\diamondsuit$

We will see that there are arbitrarily large q for which $d(C_S(\mathbb{F}_q)) > d(C_{T_0}(\mathbb{F}_q))$. To prove this, we begin with some general observations. Much of this has been noted before in Theorem 2 of [1], but not in the context of the possible Minkowski decompositions studied in [17]. Since we assume $abd \neq 0$, to normalize, we will take $d = 1$.

There are three distinct points on the curve on the line at infinity $z = 0$ in all cases (that is, whether or not $c = 0$). All three of them are flexes, and the lines $x = 0$, $y = 0$, $ax + by + cz = 0$ are the inflectional tangents. So the points in the torus $(\mathbb{F}_q^\times)^2$ are all the affine points of the curve.

If $abd \neq 0$ but $c = 0$, then the curve is smooth of genus 1. This can be seen since the system defining the Jacobian ideal:

$$\begin{aligned}
2axy + by^2 = y(2ax + by) = 0\\
ax^2 + 2bxy = x(ax + 2by) = 0\\
3z^2 = 0.
\end{aligned}$$

implies $z = 0$. But, by (1), the curve must be smooth, since all three points on the line at infinity are smooth points.

If $c \neq 0$, there are also singular (nodal) cubics in the family. In this case the Jacobian system has the solution

$$x = \frac{-c}{3a}, \quad y = \frac{-c}{3b}, \quad z = 1.$$

Substituting into the equation of the curve, we get:

$$\frac{-c^3}{27ab} - \frac{c^3}{27ab} + \frac{c^3}{9ab} + 1 = 0.$$

so if $c^3 = -27ab$, the curve has a singular point at the point with homogeneous coordinates

$$(x : y : z) = \left(\frac{-c}{3a} : \frac{-c}{3b} : 1\right).$$

If the origin of the group structure on the points of a smooth cubic curve is placed at an inflection point, the other inflection points are points have order 3.

Since the 3-torsion points form a subgroup of the group of $\mathbb{F}_q$-rational points, we have the following statement.

Lemma 5.3. *For all the smooth elements E of the family (5.1) over $\mathbb{F}_q$, the number of $\mathbb{F}_q$-rational points is* divisible by 3.

The discussion of §4.2 of [10] shows, in fact, that the family (5.1) is a sort of universal family for elliptic curves over $\mathbb{F}_q$ with nontrivial 3-torsion subgroups. Every isomorphism class of such curves is represented by some element of our family.

If $p \geq 3$, by an easy change of coordinates, the equations (5.1) can be put into Weierstrass form. Namely, dehomogenize with respect to x, and complete the square in y. If $p \geq 5$, by a further change of coordinates, the Weierstrass form can be taken to

$$u^2 = v^3 + Av + B.$$

If $c = 0$ to start, then after this change of coordinates it will be true that $A = 0$.

The j-invariant of an elliptic curve in this form is

$$j = 1728\frac{4A^3}{4A^3 + 27B^2}.$$

Hence $j = 0$ if and only if $A = 0$. .

When $q \equiv 2 \bmod 3$ for an odd prime power q, elliptic curves with $j = 0$ are *supersingular* elliptic curves (see Proposition 4.31 of [18]). There are many equivalent characterizations of this property and it follows that

$$|E(\mathbb{F}_{q^h})| = \begin{cases} q^h + 1 & h \text{ odd} \\ q^h + 1 + 2q^{h/2} & \text{if } h \equiv 2 \bmod 4 \\ q^h + 1 - 2q^{h/2} & \text{if } h \equiv 0 \bmod 4. \end{cases}$$

In other words, supersingular elliptic curves defined over $\mathbb{F}_q$ achieve the Hasse-Weil *upper* bound over $\mathbb{F}_{q^h}$ when $h \equiv 2 \bmod 4$. On the other hand, they achieve the Hasse-Weil *lower* bound over $\mathbb{F}_{q^h}$ when $h \equiv 0 \bmod 4$.

The above observations show that the answer to our Question 5.1 is negative, because of some subtle arithmetic facts concerning the numbers of points on certain elliptic curves! Some of the following reasoning also appears in the proof of Theorem 2 in [1].

Theorem 5.4. *Let q be odd and $q \equiv 2 \bmod 3$. Then*

$$d(C_S(\mathbb{F}_q)) = (q-1)^2 - (q-1) > d(C_{T_0}(\mathbb{F}_q)).$$

Proof. If q is odd and $q \equiv 2 \bmod 3$, then because the corresponding elliptic curves are supersingular (and recalling that we must subtract the three points at infinity) all of the codewords of $C_S(\mathbb{F}_q)$ obtained from evaluation of $axy^2 + bxy^2 + d$ with $abd \neq 0$ will have weight

$$(q-1)^2 - (q+1-3) > (q-1)^2 - (q-1).$$

On the other hand, by (5.2) there are also codewords of weight $(q-1)^2 - (q-1)$ from polynomials with one coefficient equal to zero. Those give the minimum weight words in this case.

On the other hand, we need to determine the minimum distance of $C_{T_0}(\mathbb{F}_q)$. By the theorem of Waterhouse (Theorem 4.1 of [19]), we know that there are elliptic curves over $\mathbb{F}_q$ with

$$|E(\mathbb{F}_q)| = q + 1 + t$$

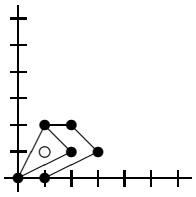

FIGURE 4. A Minkowski sum with the exceptional triangle.

for all integers t with $t \leq \lfloor 2\sqrt{q} \rfloor$ and $\gcd(t,q) = 1$ (as well as some other possibilities). By Lemma 5.3 and the universality of our family (3.1) for curves with nontrivial 3-torsion, there will be curves here with $q+1+t$ points rational over $\mathbb{F}_q$ if t is the *largest* integer satisfying $t \leq \lfloor 2\sqrt{q} \rfloor$, t prime to q, and such that $3|(q+1+t)$. These give codewords of considerably smaller weight, in some cases close to

$$(q-1)^2 - (q+1+2\sqrt{q}-3).$$

So the minimum distance of the code from S will be strictly larger than that of the code from T_0 for all such q. □

Example 5.5. For instance, refer again to Example 5.2. With $p = 17 \equiv 2 \bmod 3$, Theorem 5.4 applies. The largest t such that $t \leq \lfloor 2\sqrt{17} \rfloor$ and $3|(17+1+t)$ is $t = 6$. There are elliptic curves in the family (3.1) with 24 $\mathbb{F}_{17}$-rational points and hence 21 points in $(\mathbb{F}_{17}^{\times})^2$ disregarding the three points at infinity. This gives $d(C_{T_0}(\mathbb{F}_{17})) = 16^2 - 21 = 235$. However, $d(C_S(\mathbb{F}_{17})) = 16^2 - 16 = 240$.

On the other hand, when q is odd and $\equiv 1 \bmod 3$, the elliptic curves with $j = 0$ are not supersingular. And in fact the minimum weight words in $C_{T_0}(\mathbb{F}_q)$ sometimes come from $C_S(\mathbb{F}_q)$ in this case. ♢

We conclude with a final remark. Phenomena similar to those seen in Theorem 5.4, in which $d(C_S(\mathbb{F}_q)) > d(C_P(\mathbb{F}_q))$ can occur for arbitrarily large q, also occur in polygons for which the maximal Minkowski-reducible subpolygon Q contains a T_0 summand.

Example 5.6. Consider the Minkowski sum $P = T_0 + I$, where I is the interval $I = \text{conv}\{(0,0),(1,0)\}$, shown in Figure 4. We study the generalized toric codes for

$$S = (P \cap \mathbb{Z}^2) \setminus \{(1,1)\}$$

obtained by removing one of the two interior lattice points from P.

For all odd $q \equiv 2 \bmod 3$, we will again have $d(C_S(\mathbb{F}_q)) > d(C_P(\mathbb{F}_q))$. The minimum distances of the two codes over small fields are as follows.

$$\begin{aligned}
d(C_S(\mathbb{F}_7)) = 22 \quad &\text{vs.} \quad d(C_P(\mathbb{F}_7)) = 21 \\
d(C_S(\mathbb{F}_8)) = 36 \quad &\text{vs.} \quad d(C_P(\mathbb{F}_8)) = 33 \\
d(C_S(\mathbb{F}_9)) = 48 \quad &\text{vs.} \quad d(C_P(\mathbb{F}_9)) = 44 \\
d(C_S(\mathbb{F}_{11})) = 80 \quad &\text{vs.} \quad d(C_P(\mathbb{F}_{11})) = 75 \\
d(C_S(\mathbb{F}_{13})) = 114 \quad &\text{vs.} \quad d(C_P(\mathbb{F}_{13})) = 114 \\
d(C_S(\mathbb{F}_{16})) = 192 \quad &\text{vs.} \quad d(C_P(\mathbb{F}_{16})) = 189 \\
d(C_S(\mathbb{F}_{17})) = 224 \quad &\text{vs.} \quad d(C_P(\mathbb{F}_{17})) = 219 \\
d(C_S(\mathbb{F}_{19})) = 282 \quad &\text{vs.} \quad d(C_P(\mathbb{F}_{19})) = 282.
\end{aligned}$$

Note that P contains the two term Minkowski sum $\mathrm{conv}(\{(1,0),(1,2)\})$, as well as several other Minkowski decomposable parallelograms. If instead of this S we consider R consisting of the 5 noninterior lattice points in P, then codewords obtained by evaluating reducible linear combinations of the corresponding monomials have the minimum possible weights

$$(q-1)^2 - 2(q-1)$$

in many of these cases, since there are reducible polynomials of the form

$$x(y-\alpha_1)(y-\alpha_2)$$

with $\alpha_1 \neq \alpha_2$ and $\alpha_1 + \alpha_2 = 0$ whenever q is odd. These have $2(q-1)$ zeroes in $(\mathbb{F}_q^{\times})^2$. $\diamondsuit$

Acknowledgements. The work reported here began during a visit to the University of Illinois at Urbana-Champaign, hosted by Hal Schenck. The author would like to thank him for his hospitality and valuable comments.

References

[1] P. Beelen, D. Ruano, *The order bound for toric codes*, in M. Bras-Amoros and T. Høholdt, eds. *AAECC 2009*, Springer Lecture Notes in Computer Science 5527, 1–10.

[2] S. Cohen, *Uniform distribution of polynomials over finite fields*, J. London Math. Soc. Series 2, **6** (1972), 93–102.

[3] M. Fried, J. Smith, J, *Irreducible discriminant components of coefficient spaces*. Acta Arith. **44** (1984), 59–72.

[4] M. Grassl, *Code Tables: Bounds on the parameters of various types of codes*, online at *www.codetables.de*, consulted July 21, 2011.

[5] S. Gao, J. Howell, D. Panario, *Irreducible polynomials of given forms*, in: *Finite fields: theory, applications, and algorithms (Waterloo, ON, 1997)*, 43 – 54, Contemp. Math., 225, Amer. Math. Soc., Providence, RI, 1999.

[6] S. Ghorpade, G. Lachaud, *Étale cohomology, Lefschetz theorem, and number of points of singular varieties over finite fields*, online *arXiv:0808.2169*

[7] J. Hansen, *Toric surfaces and error-correcting codes*, in Coding theory, cryptography and related areas (Guanajuato, 1998), 132–142, Springer, Berlin, 2000.

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

[9] W. C. Huffman, V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, Cambridge, 2003.

[10] D. Husemöller, *Elliptic Curves*, 2nd ed. Graduate Texts in Mathematics, **111**, Springer, New York, 2004.

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

[12] J. Little, H. Schenck, *Toric surface codes and Minkowski sums*, SIAM J. Discrete Math. **20** (2006), 999–1014.
[13] E. Martínez-Moro, Ruano, D. *Toric codes* in *Advances in algebraic geometry codes*, Series in Coding Theory and Cryptology **5**, World Scientific, Singapore, 2008.
[14] D. Ruano, *On the parameters of r-dimensional toric codes*, Finite Fields Appl. **13** (2007), 962–976.
[15] D. Ruano, *On the structure of generalized toric codes*, J. Symb. Comp. **45** (2009), 499–506.
[16] J. Silverman *The arithmetic of elliptic curves*, 2nd ed. Springer Graduate Texts in Mathematics 106, Springer, New York, 2009.
[17] I. Soprunov, E. Soprunova, *Toric surface codes and Minkowski length of polygons*, SIAM J. Discrete Math. **23** (2009), 384–400.
[18] L. Washington, *Elliptic Curves: Number Theory and Cryptography*, Chapman & Hall/CRC, Boca Raton, 2003.
[19] W. Waterhouse, William, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 521–560.

E-mail address: little@mathcs.holycross.edu
URL: http://mathcs.holycross.edu/~little/homepage.html

Department of Mathematics and Computer Science, College of the Holy Cross, Worcester, MA 01610