2009

Toric Surface Codes and Minkowski Length of Polygons

Ivan Soprunov
Cleveland State University, i.soprunov@csuohio.edu

Jenya Soprunova
Kent State University

Toric Surface Codes and Minkowski Length of Polygons

Article *in* SIAM Journal on Discrete Mathematics · January 2009

DOI: 10.1137/080716554 · Source: DBLP

2 authors, including:

Ivan Soprunov
Cleveland State University
24 PUBLICATIONS **69** CITATIONS

SIAM J. DISCRETE MATH.
Vol. 23, No. 1, pp. 384–400

TORIC SURFACE CODES AND MINKOWSKI LENGTH OF POLYGONS*

IVAN SOPRUNOV† AND JENYA SOPRUNOVA‡

To our teacher Askold Khovanskii on the occasion of his 60th anniversary, with love

Abstract. In this paper we prove new lower bounds for the minimum distance of a toric surface code $\mathcal{C}_P$ defined by a convex lattice polygon $P \subset \mathbb{R}^2$. The bounds involve a geometric invariant $L(P)$, called the full Minkowski length of P. We also show how to compute $L(P)$ in polynomial time in the number of lattice points in P.

Key words. evaluation codes, toric codes, Minkowski sum

AMS subject classifications. 94B27, 14G50, 52B20

DOI. 10.1137/080716554

Introduction. Consider a convex polygon P in $\mathbb{R}^2$ whose vertices lie in the integer lattice $\mathbb{Z}^2$. It determines a vector space $\mathcal{L}_K(P)$ (over a field K) of polynomials $f(t_1, t_2)$ whose monomials correspond to the lattice points in P:

$$\mathcal{L}_K(P) = \operatorname{span}_K\{t_1^{m_1} t_2^{m_2} \mid (m_1, m_2) \in P \cap \mathbb{Z}^n\}.$$

Let $\mathbb{F}_q$ be a finite field and $\overline{\mathbb{F}}_q$ its algebraic closure. The *toric surface code* $\mathcal{C}_P$, first introduced by Hansen in [6], is defined by evaluating the polynomials in $\mathcal{L}_{\mathbb{F}_q}(P)$ at all of the points (t_1, t_2) in the algebraic torus $(\mathbb{F}_q^*)^2$. To be more precise, $\mathcal{C}_P$ is a linear code whose codewords are the strings $(f(t_1, t_2) \mid (t_1, t_2) \in (\mathbb{F}_q^*)^2)$ for $f \in \mathcal{L}_{\mathbb{F}_q}(P)$. It is convenient to assume that P is contained in the square $K_q^2 = [0, q-2]^2$ so that all of the monomials in $\mathcal{L}_{\mathbb{F}_q}(P)$ are linearly independent over $\mathbb{F}_q$. Thus $\mathcal{C}_P$ has block length $(q-1)^2$ and the dimension equal to the number of the lattice points in P.

Note that the weight of each nonzero codeword in $\mathcal{C}_P$ is the number of points $(t_1, t_2) \in (\mathbb{F}_q^*)^2$ where the corresponding polynomial does not vanish. Therefore, the minimum distance of $\mathcal{C}_P$ (which is the minimum weight for linear codes) equals

$$d(\mathcal{C}_P) = (q-1)^2 - \max_{0 \neq f \in \mathcal{L}_{\mathbb{F}_q}(P)} Z(f),$$

where $Z(f)$ is the number of zeros (i.e., points of vanishing) in $(\mathbb{F}_q^*)^2$ of f.

The name *toric surface code* comes from the fact that P defines a toric surface X over $\overline{\mathbb{F}}_q$ (strictly speaking the fan that defines X is a refinement of the normal fan of P), where $\mathcal{L}_{\overline{\mathbb{F}}_q}(P)$ can be identified with the space of global sections of a semiample divisor on X (see, for example, [5]). This allows one to exploit algebraic geometric techniques to produce results about the minimum distance of $\mathcal{C}_P$. In particular, Little and Schenck in [10] used intersection theory on toric surfaces to come up with the following general idea: If q is sufficiently large, then polynomials $f \in \mathcal{L}_{\mathbb{F}_q}(P)$ with

*Received by the editors February 28, 2008; accepted for publication (in revised form) September 15, 2008; published electronically January 14, 2009.
http://www.siam.org/journals/sidma/23-1/71655.html
†Department of Mathematics, Cleveland State University, 2121 Euclid Ave., Cleveland, OH 44115 (i.soprunov@csuohio.edu).
‡Department of Mathematical Sciences, Kent State University, Summit Street, Kent, OH 44242 (soprunova@math.kent.edu).

more absolutely irreducible factors will necessarily have more zeros in $(\mathbb{F}_q^*)^2$ (see [10, Proposition 5.2]).

In this paper we expand this idea to produce explicit bounds for the minimum distance of $\mathcal{C}_P$ in terms of certain geometric invariant $L(P)$, which we call the full Minkowski length of P. Essentially $L(P)$ tells you the largest possible number of absolutely irreducible factors a polynomial $f \in \mathcal{L}_{\mathbb{F}_q}(P)$ can have, but it derives it from the geometry of the polygon P (see Definition 1.1). The number $L(P)$ is easily computable—we give a simple algorithm which is polynomial in the number of lattice points in P. Moreover, we obtain a description of the factorization $f = f_1 \cdots f_{L(P)}$ for $f \in \mathcal{L}_{\mathbb{F}_q}(P)$ with the largest number of factors. More precisely, in Proposition 2.3 we show that the Newton polygon P_{f_i} (which is the convex hull of the exponents of the monomials in f_i) is either a primitive segment, a unit simplex, or a triangle with exactly one interior and three boundary lattice points, called an *exceptional triangle*. This description enables us to prove the following bound.

THEOREM 1. *Let $P \subset K_q^2$ be a lattice polygon with area A and full Minkowski length L. Then for $q \geq \max\left(23, \left(c + \sqrt{c^2 + 5/2}\right)^2\right)$, where $c = A/2 - L + 9/4$, the minimum distance of the toric surface code $\mathcal{C}_P$ satisfies*

$$d(\mathcal{C}_P) \geq (q-1)^2 - L(q-1) - \lfloor 2\sqrt{q} \rfloor + 1.$$

The condition that no factorization $f = f_1 \cdots f_{L(P)}$ contains an exceptional triangle (as the Newton polygon of one of the factors) is geometric and can be easily checked for any given P (we provide a simple algorithm for this which is polynomial in the number of lattice points in P). In this case we have a better bound for the minimum distance of the toric surface code.

THEOREM 2. *Let $P \subset K_q^2$ be a lattice polygon with area A and full Minkowski length L. Under the above condition on P, for $q \geq \max\left(37, \left(c + \sqrt{c^2 + 2}\right)^2\right)$, where $c = A/2 - L + 11/4$, the minimum distance of the toric surface code $\mathcal{C}_P$ satisfies*

$$d(\mathcal{C}_P) \geq (q-1)^2 - L(q-1).$$

We remark that our thresholds for q, where the bounds begin to hold, are much smaller than the ones in Little and Schenck's result (see [10, Proposition 5.2]).

Although, as mentioned above, the minimum distance problem for toric codes is tightly connected to toric varieties, our methods are geometric and combinatorial and do not use algebraic geometry, except for the Hasse–Weil bound adapted to toric surfaces (see section 2.2). In section 1 we define the full Minkowski length $L(P)$ and establish combinatorial properties of polygons with $L(P) = 1, 2$. In section 2 we give a proof of Theorems 1 and 2. Section 3 is devoted to the above mentioned algorithms for computing $L(P)$ and determining the presence of an exceptional triangle. Finally, in section 4 we give a detailed analysis of three toric surface codes which illustrates our methods.

1. Full Minkowski length of polytopes.

1.1. Minkowski sum. Let P and Q be convex polytopes in $\mathbb{R}^n$. Their *Minkowski sum* is

$$P + Q = \{p + q \in \mathbb{R}^n \mid p \in P,\ q \in Q\},$$

which is again a convex polytope. Figure 1 shows the Minkowski sum of a triangle and a square.

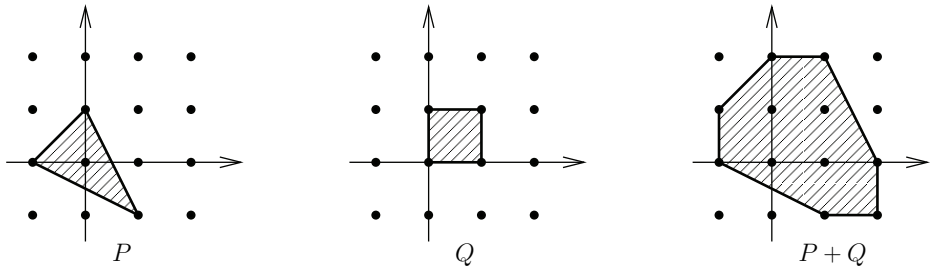

FIG. 1. *The Minkowski sum of two polygons.*

Let f be a Laurent polynomial in $K[t_1^{\pm 1}, \dots, t_n^{\pm 1}]$ (for some field K). Then its *Newton polytope* P_f is the convex hull of the exponent vectors of the monomials appearing in f. Thus P_f is a *lattice polytope* as its vertices belong to the integer lattice $\mathbb{Z}^n \subset \mathbb{R}^n$. Note that if $f, g \in K[t_1^{\pm 1}, \dots, t_n^{\pm 1}]$, then the Newton polytope of their product P_{fg} is the Minkowski sum $P_f + P_g$. A *primitive lattice segment* E is a line segment whose only lattice points are its endpoints. The difference of the endpoints is a vector v_E whose coordinates are relatively prime (v_E is defined up to a sign). A polytope which is the Minkowski sum of primitive lattice segments is called a *(lattice) zonotope*.

The automorphism group of the lattice is the group of affine unimodular transformations, denoted by $\mathrm{AGL}(n, \mathbb{Z})$, which consists of translations by an integer vector and linear transformations in $\mathrm{GL}(n, \mathbb{Z})$. Affine unimodular transformations correspond to monomial changes of variables in $K[t_1^{\pm 1}, \dots, t_n^{\pm 1}]$ and preserve the zero set of f in the algebraic torus $(K^*)^n$.

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

$$P = P_1 + \cdots + P_\ell$$

into lattice polytopes P_i of positive dimension. Clearly, there are only finitely many such decompositions. We let $\ell(P)$ be the largest number of summands in such decompositions of P, and call it the *Minkowski length* of P.

DEFINITION 1.1. *The full Minkowski length of P is the maximum of the Minkowski lengths of all subpolytopes Q in P,*

$$L(P) := \max\{\ell(Q) \,|\, Q \subseteq P\}.$$

A subpolytope $Q \subseteq P$ is called maximal for P if $\ell(Q) = L(P)$. A Minkowski decomposition of Q into $L(P)$ summands of positive dimension will be referred to as a maximal (Minkowski) decomposition in P.

Here are a few simple properties of $L(P)$ and maximal subpolytopes.

PROPOSITION 1.2. *Let P, P_1, P_2, and Q be lattice polytopes in $\mathbb{R}^n$.*

(1) *$L(P)$ is $\mathrm{AGL}(n, \mathbb{Z})$-invariant.*
(2) *$L(P) \geq 1$ if and only if $\dim(P) > 0$.*
(3) *If $P_1 + P_2 \subseteq P$, then $L(P_1) + L(P_2) \leq L(P)$.*
(4) *If Q is maximal for P, then Q contains a zonotope Z maximal for P.*

Proof. The first three statements are trivial. For the fourth one, note that if

$$Q = Q_1 + \cdots + Q_{L(P)}$$

is a maximal Minkowski decomposition in P, then by replacing each Q_i with one of its edges we obtain a zonotope $Z \subseteq Q$ with $\ell(Z) \geq L(P)$. But $Z \subseteq P$, so $\ell(Z) = L(P)$. □

Notice that the summands of every maximal decomposition in P are polytopes of full Minkowski length 1. It seems to be a hard problem to describe polytopes of full Minkowski length 1 in general. However, in dimensions 1 and 2 we do have a simple description for such polytopes (Theorem 1.4).

DEFINITION 1.3. *A lattice polytope P is* strongly indecomposable *if its full Minkowski length $L(P)$ is 1. In other words, no subpolytope $Q \subseteq P$ is a Minkowski sum of lattice polytopes of positive dimensions.*

Clearly, primitive segments are strongly indecomposable and are the only one-dimensional strongly indecomposable polytopes.

Let Δ be the standard 2-simplex and T_0 be the triangle with vertices $(1,0)$, $(0,1)$, and $(2,2)$ (see Figure 2). It is easy to see that they are both strongly indecomposable.

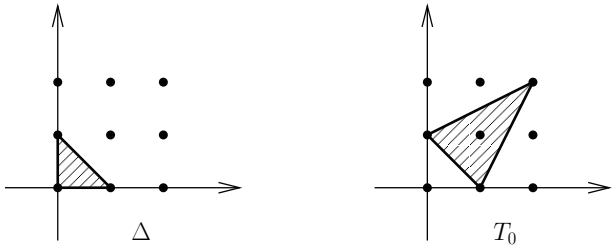

FIG. 2. *Strongly indecomposable polygons.*

The next theorem shows that these are essentially the only strongly indecomposable polygons. In the proof of this theorem and frequently later in the paper we will use Pick's formula: If P is a lattice polygon in $\mathbb{R}^2$, then the area of P equals

$$A = I + \frac{B}{2} - 1,$$

where I is the number of interior lattice points in P and B is the number of boundary points in P. The proof of this formula can be found, for example, in [3].

THEOREM 1.4. *Let P be a strongly indecomposable polygon. Then P is* $\mathrm{AGL}(2,\mathbb{Z})$*-equivalent to either the standard 2-simplex Δ or the triangle T_0 above.*

Proof. First, note that P cannot contain more than four lattice points. Indeed, suppose $a = (a_1, a_2)$ and $b = (b_1, b_2)$ lie in $P \cap \mathbb{Z}^2$. If $a_i \equiv b_i \mod 2$, for $i = 1, 2$, then the segment $[a, b]$ lies in P and is not primitive; hence, $L(P) > 1$. Since there are only four possible pairs of remainders mod 2 and P has at most four lattice points.

Suppose P is a triangle, then its sides must be primitive and either P has no interior lattice points or it has exactly one interior lattice point. In the first case, P has area $1/2$ (by Pick's formula) and so is $\mathrm{AGL}(2,\mathbb{Z})$-equivalent to Δ. In the second case, P has area $3/2$ (by Pick's formula) and hence any two of its sides generate a parallelogram of area 3. Every such triangle is $\mathrm{AGL}(2,\mathbb{Z})$-equivalent to T_0.

Now suppose P is a quadrilateral. Then it has no interior lattice points and so its area is 1 (by Pick's formula). Every such quadrilateral is $\mathrm{AGL}(2,\mathbb{Z})$-equivalent to the unit square. However, the unit square is obviously decomposable. □

DEFINITION 1.5. *A lattice polygon is called a* unit triangle *if it is* $\mathrm{AGL}(2,\mathbb{Z})$*-equivalent to Δ, and an* exceptional triangle *if it is* $\mathrm{AGL}(2,\mathbb{Z})$*-equivalent to T_0.*

The following theorem describes maximal Minkowski decompositions for a given lattice polygon P.

THEOREM 1.6. *Let P be a lattice polygon in $\mathbb{R}^2$ with full Minkowski length $L(P)$. Consider a maximal Minkowski decomposition in P:*

$$Q = Q_1 + \cdots + Q_{L(P)},$$

for some $Q \subseteq P$. Then one of the following holds:

(1) *every Q_i is either a primitive segment or a unit triangle;*
(2) *after an $\mathrm{AGL}(2,\mathbb{Z})$-transformation and reordering of the summands the decomposition is*

$$Q = T_0 + m_1[0,e_1] + m_2[0,e_2] + m_3[0,e_1+e_2],$$

where m_i are nonnegative integers such that $m_1+m_2+m_3 = L(P)-1$ and the e_i are the standard basis vectors.

Proof. Since every Q_i must be strongly indecomposable, by Theorem 1.4 it is a primitive segment, a unit triangle, or an exceptional triangle. We claim that if one of the Q_i is an exceptional triangle, then the other summands are primitive segments in only three possible directions. This follows from the two lemmas below. ∎

LEMMA 1.7. *Consider two primitive segments E_1, E_2 in $\mathbb{Z}^2$, and let v_1, v_2 be the corresponding vectors. If $|\det(v_1,v_2)| \geq 3$, then $L(E_1+E_2) \geq 3$.*

Proof. We can assume that $v_1 = (1,0)$ and $v_2 = (a,b)$ with $0 \leq a < b$ and $b = \det(v_1,v_2)$. Cases when $3 \leq b \leq 6$ are easily checked by hand. For $b \geq 7$ we can use the same argument as in the proof of Theorem 1.4 to show that $\Pi = E_1 + E_2$ contains a segment of lattice length 3. Indeed, the area of Π equals $b \geq 7$. By Pick's formula, Π has at least ten lattice points. But then there exist $a = (a_1,a_2)$ and $b = (b_1,b_2)$ in Π such that $a_i \equiv b_i \bmod 3$, for $i = 1,2$. Therefore the segment $[a,b]$ is contained in Π and has lattice length 3. ∎

LEMMA 1.8. *Let $P \subset \mathbb{R}^2$ be strongly indecomposable. Then $L(T_0+P) \geq 3$ unless P is a primitive segment in the direction of e_1, e_2 or e_1+e_2.*

Proof. Let E_1 be an edge of T_0 and E_2 an edge of P, and let v_1, v_2 be the corresponding vectors. If $|\det(v_1,v_2)| \geq 3$, then by Lemma 1.7 $L(E_1+E_2) \geq 3$, and since $E_1+E_2 \subseteq T_0+P$ we also have $L(T_0+P) \geq 3$. Therefore we suppose that $|\det(v_1,v_2)| \leq 2$ for all edges E_1 in T_0. Then we have the following linear inequalities for $v_2 = (s,t)$:

$$-2 \leq s+t \leq 2, \quad -2 \leq 2s-t \leq 2, \quad -2 \leq s-2t \leq 2.$$

Clearly, the only integer solutions (up to central symmetry) are $v_1 = (1,0)$, $(0,1)$, and $(1,1)$. Now if P contains at least 2 edges in these directions, then it must also contain (up to a translation) either $T = \mathrm{span}\{(0,0),(1,0),(1,1)\}$ or $T = \mathrm{span}\{(0,0),(0,1),(1,1)\}$. But in both cases the sum T_0+T contains a 1×2 rectangle which has Minkowski length three. Therefore, $L(T_0+P) \geq 3$. ∎

Remark 1.9. Notice that in Lemma 1.8 the special directions e_1, e_2 or e_1+e_2 have an easy $\mathrm{AGL}(2,\mathbb{Z})$-invariant description: they are obtained by connecting the interior lattice point in T_0 to the vertices.

While classifying polygons of every given full Minkowski length does not seem feasible, we will make a few statements about polygons of full Minkowski length 2, which we will use later.

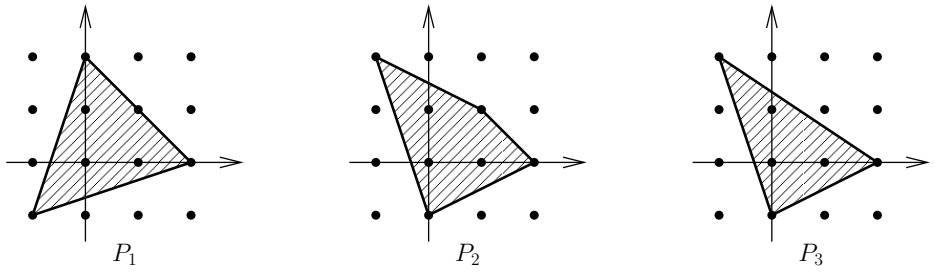

FIG. 3. *Full length two polygons with three interior lattice points.*

PROPOSITION 1.10. *Suppose $L(P) = 2$. Then we have the following:*

(1) *P has at most three interior lattice points, i.e., $I(P) \leq 3$.*
(2) *If $I(P) = 3$, then P is $\mathrm{AGL}(2, \mathbb{Z})$-equivalent to one of the polygons depicted in Figure 3.*
(3) *If $I(P) = 3$, then $L(P + T_0) \geq 4$.*

Proof. (1) The proof is somewhat technical so we will sketch its major steps. Assume P has four or more interior lattice points. First, it is not hard to show that one can choose four interior lattice points in P so that after an $\mathrm{AGL}(2, \mathbb{Z})$-transformation they form either a unit square, $\{(0,0), (1,0), (0,1), (1,1)\}$, or a base 2 isosceles triangle, $\{(-1,0), (0,0), (1,0), (0,1)\}$.

In the first case, note that P must include a lattice point which is distance one from the square and lies on one of the lines containing the sides of the square. By symmetry we can assume it is $(2,0)$. In Figure 4 on the left, the solid dots represent the five points that now belong to P, the crosses represent the points that cannot belong to P (otherwise its length would be greater than 2). Now if point $(0,2)$ does not belong to P (the middle picture in Figure 4), then either $(-1,2)$ or $(1,2)$ does. But in either case the four points of the unit square cannot all lie in the interior of P. If point $(0,2)$ does belong to P, then it produces more forbidden points (the rightmost picture in Figure 4). Then again, it is not hard to see that no such P can exist.

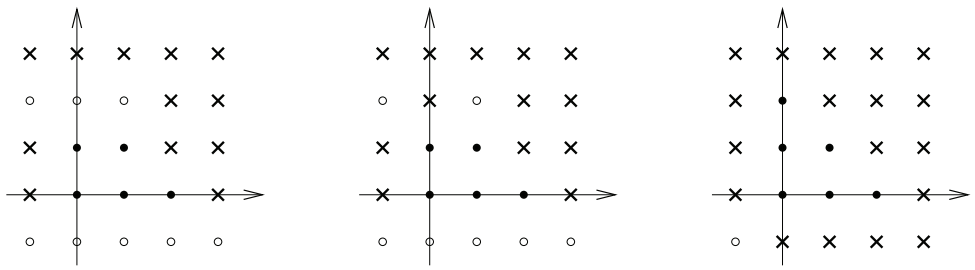

FIG. 4. *Nonexistence of full length two polygons with $I(P) > 3$.*

Playing the same game, one can show that no P exists in the second case as well.

(2) First, one can show that the three interior lattice points cannot be collinear. Thus we can assume that they are $\{(0,0), (1,0), (0,1)\}$. Our first case is when $(1,1)$ also lies in P. Since this must be a boundary point and there are no more interior points in P, we see that $(-1,2)$ and $(0,2)$ are the only possible boundary points of P on the line $y = 2$. Similarly, $(2,0)$ and $(2,-1)$ are the only possible boundary points of P on the line $x = 2$. Since both $(-1,2)$ and $(2,-1)$ cannot belong to P, using symmetry we arrive at two possibilities for the boundary piece of P containing $(1,1)$,

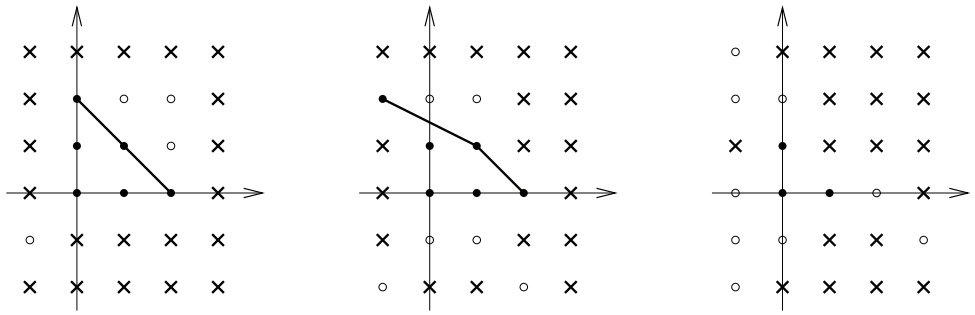

FIG. 5. *Constructing full length two polygons with* $I(P) = 3$.

depicted in Figure 5 on the left. As in part (1), we crossed out the points which cannot appear in P since $L(P) = 2$. Then it becomes clear that the only P (up to symmetry) containing $\{(0,0),(1,0),(0,1)\}$ and $(1,1)$ are P_1 and P_2 in Figure 3.

In the second case, when $(1,1)$ does not lie in P we can assume that $(1,-1)$ and $(-1,1)$ do not lie in P either, otherwise we can reduce it to the previous case by a unimodular transformation. Also, both $(2,-1)$ and $(-1,2)$ cannot lie in P, therefore by symmetry we can assume that $(2,-1)$ does not. As before, by crossing out forbidden points we obtain the rightmost picture in Figure 5. Now it is easy to see that the only P containing the three points in the interior is P_3 in Figure 3.

(3) By (2) it is enough to check that $L(P_i + T) \geq 4$ for every $1 \leq i \leq 3$ and any exceptional triangle T.

We first look at P_1. By Lemma 1.8 and Remark 1.9 we have $L(E+T) \geq 3$ for any primitive segment E except for the three special segments E_1, E_2, E_3 that connect the interior lattice point of T to its vertices. If $T \neq T_0$, then one of $[0,e_1]$, $[0,e_2]$, $[0,e_1+e_2]$ is not among the E_i. But P_1 contains the segments $2[0,e_1], 2[0,e_2]$, and $(-1,-1)+2[0,e_1+e_2]$. If, say, $[0,e_1]$ is not among the E_i, then $L(2[0,e_1]+T) \geq 4$ and hence $L(P_1+T) \geq 4$. It remains to show that $L(P_1+T_0) \geq 4$, which can easily be checked by hand.

A similar argument works for P_3. We only need to replace T_0 with T_0', the triangle with vertices $(0,0),(1,1)$, and $(-1,2)$. Its special segments $[0,e_1]$, $[0,e_2]$, $[0,-e_1+e_2]$ are contained in P with multiplicity 2. Finally, since $P_3 \subset P_2$ we do not need to do any extra work for P_2. ∎

2. Bounds for toric surface codes.

2.1. Toric surface codes. Fix a finite field $\mathbb{F}_q$ where q is prime power. For any convex lattice polygon P in $\mathbb{R}^2$ we associate a $\mathbb{F}_q$-vector space of bivariate polynomials whose monomials have exponent vectors in $P \cap \mathbb{Z}^2$:

$$\mathcal{L}(P) = \operatorname{span}_{\mathbb{F}_q}\{t^m \mid m \in P \cap \mathbb{Z}^2\}, \quad \text{where } t^m = t_1^{m_1} t_2^{m_2}.$$

If P is contained in the square $K_q^2 = [0, q-2]^2$, then the monomials t^m are linearly independent over $\mathbb{F}_q$ and so $\dim \mathcal{L}(P) = |P \cap \mathbb{Z}^2|$. In what follows we will always assume that $P \subset K_q^2$.

The *toric surface code* $\mathcal{C}_P$ is a linear code whose codewords are the strings of values of $f \in \mathcal{L}(P)$ at all points of the algebraic torus $(\mathbb{F}_q^*)^2$ (in some linear order):

$$\mathcal{C}_P = \{\big(f(t), t \in (\mathbb{F}_q^*)^2\big) \mid f \in \mathcal{L}(P)\}.$$

This is a linear code of block length $(q-1)^2$ and dimension $|P\cap\mathbb{Z}^2|$. The weight of each nontrivial codeword equals the number of points $t \in (\mathbb{F}_q^*)^2$ where the corresponding polynomial does not vanish. Let $Z(f)$ denote the number of points in $(\mathbb{F}_q^*)^2$ where f vanishes. Then the minimum distance $d(\mathcal{C}_P)$, which is also the minimum weight, equals

$$d(\mathcal{C}_P) = (q-1)^2 - \max_{0\neq f\in\mathcal{L}(P)} Z(f).$$

2.2. The Hasse–Weil bound. Consider $f \in \mathcal{L}(P)$. Its *Newton polygon* P_f is the convex hull of the lattice points in $\mathbb{R}^2$ corresponding to the monomials in f. We have

$$f(t) = \sum_{m\in P_f\cap\mathbb{Z}^2} \lambda_m t^m, \quad \text{where } t^m = t_1^{m_1}t_2^{m_2}, \quad \lambda_m \in \mathbb{F}_q.$$

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. Then f can be identified with a global section of a semiample divisor on X. Let C_f be the closure in X of the affine curve given by $f = 0$ in $(\overline{\mathbb{F}}_q^*)^2$. If f is absolutely irreducible, i.e., C_f is irreducible, then the number of $\mathbb{F}_q$-rational points $|C_f(\mathbb{F}_q)|$ satisfies the Hasse–Weil bound:

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

where g is the *arithmetic genus* of C_f. For the case of smooth curves, see, for example, [11]; for singular curves we refer to [1].

Since we are interested in the number $Z(f)$ of zeros of f in the torus $(\mathbb{F}_q^*)^2$, the above bound might be improved by subtracting possible $\mathbb{F}_q$-rational points on C_f at "infinity." More precisely, we have the following proposition.

PROPOSITION 2.1. *Let f be absolutely irreducible with Newton polygon P_f. Then*

$$Z(f) \le q + 1 + \lfloor 2I(P_f)\sqrt{q}\rfloor - B'(P_f), \tag{2.1}$$

where $I(P_f)$ is the number of interior lattice points and $B'(P_f)$ is the number of primitive edges of P_f.

Proof. It is a classical result from the theory of toric varieties that the arithmetic genus g equals the number of interior lattice points in P_f (see [7] for the general case or [10] for the case of curves).

Let $D \subset X$ be the invariant divisor at "infinity," i.e., $D = X \setminus (\overline{\mathbb{F}}_q^*)^2$. Then the Hasse–Weil bound implies

$$Z(f) \le q + 1 + \lfloor 2I(P_f)\sqrt{q}\rfloor - |C_f(\mathbb{F}_q)\cap D|.$$

The divisor D is the disjoint union of zero- and one-dimensional orbits in X. The one-dimensional orbits are isomorphic to $\overline{\mathbb{F}}_q^*$ and correspond to the rays of Σ_X. Since Σ_X is a refinement of the normal fan of P_f, some of the orbits correspond to the edges of P_f. Let E be an edge of P_f and O_E the corresponding orbit in X, and consider the "restriction" of f to E, i.e., a univariate polynomial $f_E(s)$ whose coefficients are λ_m for $m \in E$, ordered counterclockwise. Then the intersection number $C_f \cdot O_E$ equals the number of zeros of f_E in $\overline{\mathbb{F}}_q^*$ (see [9, Theorem 1 of section 2]). Note that if E is primitive, then f_E is linear, hence, has exactly one $\mathbb{F}_q$-rational zero on O_E. Therefore,

$|C_f(\mathbb{F}_q) \cap D|$ is greater than or equal to $B'(P_f)$, the number of primitive edges of P_f, and the proposition follows. ∎

COROLLARY 2.2. *Let $f \in \mathcal{L}(P)$ be absolutely irreducible and P_f its Newton polygon.*

(1) *If P_f is an exceptional triangle, then $Z(f) \leq q - 2 + \lfloor 2\sqrt{q} \rfloor$.*
(2) *If $I(P_f) = 0$, then $Z(f) \leq q - 1$ unless P_f is twice a unit triangle in which case $Z(f) \leq q + 1$.*

Proof. Part (1) follows immediately from Proposition 2.1. For (2) we use the classification of polygons with no interior lattice points (see, for example, [9] or [2]): P_f is $\mathrm{AGL}(2, \mathbb{Z})$-equivalent to either (a) 2Δ or (b) a trapezoid (see Figure 6) where $0 \leq a \leq b$ (this includes primitive segments when $a = b = 0$ and unit triangles when $a = 0$, $b = 1$). In the first case $Z(f) \leq q + 1$ by (2.1). In the second case P_f has at least two primitive edges, so $Z(f) \leq q - 1$, again by (2.1). ∎

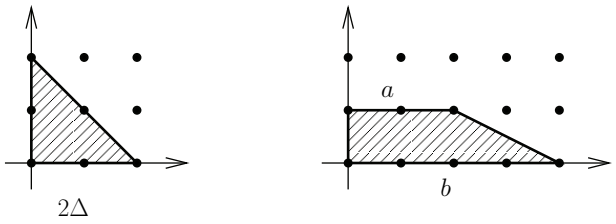

FIG. 6. *Polygons with no interior lattice points.*

2.3. Bounds for the minimum distance. Let $\mathcal{C}_P$ be the toric surface code defined by a lattice polygon P in K_q^2. In this section we prove bounds for the minimum distance of $\mathcal{C}_P$ in terms of the full Minkowski length $L(P)$ of the polygon P.

Here is our first application of the results of the previous section.

PROPOSITION 2.3. *Let $f \in \mathcal{L}(P)$ be a polynomial with the largest number of absolutely irreducible factors, $f = f_1 \cdots f_L$. Then we have the following:*

(1) *$L = L(P)$ and every $P(f_i)$ is either a primitive segment, a unit triangle, or an exceptional triangle.*
(2) *The number of zeros of f in $(\mathbb{F}_q^*)^2$ satisfies*

$$Z(f) \leq L(q-1) + \lfloor 2\sqrt{q} \rfloor - 1.$$

(3) *If $P(f_i)$ is not an exceptional triangle for any $1 \leq i \leq L$, then*

$$Z(f) \leq L(q-1).$$

Proof. Part (1) follows directly from Theorem 1.6. Moreover, the theorem implies that either (a) all P_i are primitive segments or unit triangles or (b) one of the P_i is an exceptional triangle and the others are primitive segments. In the first case every f_i has at most $q - 1$ zeros in $(\mathbb{F}_q^*)^2$ by Corollary 2.2. Not accounting for possible common zeroes of the f_i we obtain the bound in (3). In the second case one of the f_i has at most $q - 2 + \lfloor 2\sqrt{q} \rfloor$ zeros and the others have at most $q - 1$ zeros, again by Corollary 2.2. As before, disregarding possible common zeros of the f_i we get the bound in (2). ∎

The next proposition deals with polynomials f whose number of absolutely irreducible factors is $L(P) - 1$.

PROPOSITION 2.4. *Let P have full Minkowski length L, and let $f \in \mathcal{L}(P)$ have $L-1$ absolutely irreducible factors. Then*

$$Z(f) \leq (L-1)(q-1) + \lfloor 6\sqrt{q} \rfloor.$$

Proof. As before, let $f = f_1 \cdots f_{L-1}$ be the decomposition of f into absolutely irreducible factors, and let P_i be the Newton polygon of f_i. First, by Proposition 1.2

$$k+1 = L \geq \sum_{i=1}^{k} L(P_i) \geq k;$$

hence, up to renumbering, $L(P_1) \leq 2$ and $L(P_i) = 1$ for $2 \leq i \leq k$.

Assume $L(P_1) = 1$. Then every P_i is either a strongly indecomposable triangle or a lattice segment. We claim that at most three of the P_i are exceptional triangles, and so the statement follows from Corollary 2.2. Indeed, if, say, $P_1, \ldots, P_4$ are exceptional triangles, then by Lemma 1.8 $L(P_1 + \cdots + P_4) \geq 6$. Applying Proposition 1.2 again we get

$$k+1 = L \geq L(P_1 + \cdots + P_4) + \sum_{i=5}^{k} L(P_i) \geq 6 + (k-4) = k+2,$$

a contradiction.

Now assume $L(P_1) = 2$. According to (1) in Proposition 1.10, we have $I(P_1) \leq 3$. Also since $L(P_1) = 2$, at most one of the other P_i is an exceptional triangle. This follows from Lemma 1.8 using arguments similar to the previous case. We now have three subcases.

- If $I(P_1) = 1$, then we have

$$Z(f) \leq (q+1+\lfloor 2\sqrt{q} \rfloor) + (q-2+\lfloor 2\sqrt{q} \rfloor) + (L-3)(q-1) \leq (L-1)(q-1) + \lfloor 6\sqrt{q} \rfloor.$$

- If $I(P_1) = 2$, then P_1 has at least one primitive edge which we prove in Lemma 2.5 below. Therefore by Proposition 2.1 we have

$$Z(f) \leq (q+\lfloor 4\sqrt{q} \rfloor) + (q-2+\lfloor 2\sqrt{q} \rfloor) + (L-3)(q-1) \leq (L-1)(q-1) + \lfloor 6\sqrt{q} \rfloor.$$

- Finally, if $I(P_1) = 3$, then none of the other P_i is an exceptional triangle. This follows from Proposition 1.10, (3), and the above arguments. In this case P_1 has at least two primitive edges by Proposition 1.10, (2). Therefore by Proposition 2.1 we have

$$Z(f) \leq (q-1+\lfloor 6\sqrt{q} \rfloor) + (L-2)(q-1) = (L-1)(q-1) + \lfloor 6\sqrt{q} \rfloor. \qquad \square$$

LEMMA 2.5. *If $L(P) = 2$ and $I(P) = 2$, then P has a primitive edge.*

Proof. Since $L(P) = 2$, no edge can have more than 3 lattice points. If P has 4 or more edges, in which none are primitive, then P has at least 8 boundary lattice points and, hence, at least 10 lattice points total. But then P contains a lattice segment of lattice length 3 (see the proof of Lemma 1.7), which contradicts the assumption $L(P) = 2$.

It remains to show that triangles with no primitive edges, 2 interior lattice points, and 6 boundary lattice points do not exist. Let T be such a triangle and let $2E_1$, $2E_2$ be two of its edges, where E_1 and E_2 are primitive. Then E_1, E_2 form a triangle T' of area $A(T') = \frac{1}{4}A(T)$. On the other hand, by Pick's formula $A(P) = 4$, and hence

$A(T') = 1$. This implies that up to an $\mathrm{AGL}(2,\mathbb{Z})$-transformation $E_1 = [0, e_1]$ and $E_2 = [0, e_1 + 2e_2]$, but then $I(T) = 1$, a contradiction. □

Now we are ready for the main result of this section.

THEOREM 2.6. *Let $P \subset K^2_{q-1}$ be a lattice polygon with area $A = A(P)$ and full Minkowski length $L = L(P)$. Then*

(1) *for $q \geq \max\big(23, \big(c+\sqrt{c^2+5/2}\big)^2\big)$, where $c = A/2-L+9/4$, every polynomial $f \in \mathcal{L}(P)$ has at most $L(q-1)+\lfloor 2\sqrt{q}\rfloor - 1$ zeros in $(\mathbb{F}_q^*)^2$. Consequently, the minimum distance for the toric surface code $\mathcal{C}_P$ satisfies*

$$d(\mathcal{C}_P) \geq (q-1)^2 - L(q-1) - \lfloor 2\sqrt{q}\rfloor + 1.$$

(2) *If no maximal decomposition in P contains an exceptional triangle, then for $q \geq \max\big(37, \big(c+\sqrt{c^2+2}\big)^2\big)$, where $c = A/2 - L + 11/4$, every polynomial $f \in \mathcal{L}(P)$ has at most $L(q-1)$ zeros in $(\mathbb{F}_q^*)^2$. Consequently, the minimum distance for the toric surface code $\mathcal{C}_P$ satisfies*

$$d(\mathcal{C}_P) \geq (q-1)^2 - L(q-1).$$

Proof. (1) As we have seen in Proposition 2.3, (2), the bound holds for the polynomials with the largest number of irreducible factors. We are going to show that for large enough q every polynomial with fewer irreducible factors will have no greater than $L(q-1)+\lfloor 2\sqrt{q}\rfloor - 1$ zeros in $(\mathbb{F}_q^*)^2$.

Let $f \in \mathcal{L}(P)$ have $k < L$ absolutely irreducible factors $f = f_1 \cdots f_k$, and let P_i be the Newton polygon of f_i. If $k = L-1$, then we can use the bound in Proposition 2.4:

$$Z(f) \leq (L-1)(q-1) + \lfloor 6\sqrt{q}\rfloor. \tag{2.2}$$

The latter is at most $L(q-1)+\lfloor 2\sqrt{q}\rfloor - 1$ for all $q \geq 19$.

Now suppose $1 \leq k \leq L-2$. First, assume $I(P_i) = 0$ for all $1 \leq i \leq k$. Then by Corollary 2.2 (2),

$$Z(f) \leq s(q+1) + (k-s)(q-1) = 2s + k(q-1),$$

where s is the number of twice unit triangles among the P_i. Since the sum of the full Minkowski lengths of the P_i cannot exceed L we have $2s+(k-s) \leq L$, i.e., $s \leq L-k$. Using this inequality along with $k \leq L-2$, we obtain

$$Z(f) \leq 2s + k(q-1) \leq 2L + k(q-3) \leq (L-2)(q-1) + 4.$$

The latter is at most $L(q-1)$ for all $q \geq 3$ and the bounds follow.

Suppose $I(P_i) > 0$ for at least one of the P_i. Then, as we will show in Lemma 2.7,

$$Z(f) \leq k(q-1) + 2\big(A + 3/2 - 2k\big)\sqrt{q} + 2. \tag{2.3}$$

Now the right-hand side will be at most $L(q-1)+2\sqrt{q}-1$ whenever q satisfies

$$(L-k)q - 2(A+1/2-2k)\sqrt{q} - (L-k+3) \geq 0. \tag{2.4}$$

Before proceeding we introduce the following notation: $m = L-k$, $d = A/2-L+1/4$. Then (2.4) becomes

$$mq - 4(d+m)\sqrt{q} - (m+3) \geq 0, \quad 2 \leq m \leq L-1.$$

Since this is a quadratic inequality in $\sqrt{q}$, it will hold if

$$\sqrt{q} \geq C + \sqrt{C^2 + 1 + 3/m}, \quad \text{where } C = 2 + 2d/m.$$

Since $m \geq 2$, it is enough to choose $\sqrt{q} \geq C + \sqrt{C^2 + 5/2}$. Finally, if $d \geq 0$, then $C \leq 2 + d$, since $m \geq 2$, and it is enough to choose

$$q \geq \left(c + \sqrt{c^2 + 5/2}\right)^2, \quad \text{where} \quad c = 2 + d = A/2 - L + 9/4.$$

If $d < 0$, then $C < 2$ and it is enough to choose $q \geq 23$.

(2) The proof of the second statement is completely analogous. First, if f has L irreducible factors, then the bound holds by Proposition 2.3, (3). Second, if f has fewer than L factors we choose q large enough so that the right-hand sides of (2.2) and (2.3) are no greater than $L(q-1)$. The same arguments as before show that it is enough to choose

$$q \geq \max\left(37, \left(c + \sqrt{c^2 + 2}\right)^2\right), \quad \text{where} \quad c = A/2 - L + 11/4. \qquad \square$$

It remains to prove the following lemma.

LEMMA 2.7. *Let* $f = f_1 \cdots f_k$, *for* $1 \leq k \leq L-2$, *and* $I(P_i) > 0$ *for at least one* i. *Then*

$$Z(f) \leq k(q-1) + 2\big(A + 3/2 - 2k\big)\sqrt{q} + 2.$$

Proof. We order the P_i so that for $1 \leq i \leq t$ every P_i either has interior lattice points or is twice a unit triangle. Then, according to Proposition 2.1 and Corollary 2.2, we have

$$Z(f) \leq t(q+1) + 2\sqrt{q}\sum_{i=1}^{t} I(P_i) + (k-t)(q-1). \tag{2.5}$$

Now we want to get a bound for $\sum_{i=1}^{t} I(P_i)$. Recall that given two polytopes Q_1 and Q_2 in $\mathbb{R}^2$, their normalized *mixed volume* (two-dimensional) is

$$V(Q_1, Q_2) = A(Q_1 + Q_2) - A(Q_1) - A(Q_2).$$

The mixed volume is symmetric; bilinear with respect to Minkowski addition; monotone increasing (i.e., if $Q_1' \subset Q_1$, then $V(Q_1', Q_2) \leq V(Q_1, Q_2)$); and $\mathrm{AGL}(2,\mathbb{Z})$-invariant (see, for example, [4, p. 138]). This implies that

$$V(P_i, P_j) \geq 2 \quad \text{for } 1 \leq i \leq t \quad \text{and } 1 \leq j \leq k. \tag{2.6}$$

Indeed, by monotonicity it is enough to show that $V(P_i, E) \geq 2$ for any lattice segment E, and by $\mathrm{AGL}(2,\mathbb{Z})$-invariance we can assume that E is horizontal. It follows readily from the definition that $V(P_i, E) = h(P_i)|E|$, where $h(P_i)$ is the length of the horizontal projection of P_i (the height of P_i) and $|E|$ is the length of E. Clearly, $|E| \geq 1$ and $h(P_i) \geq 2$ if P_i has at least one interior lattice point or is twice a unit triangle.

Using (2.6) and bilinearity of the mixed volume, by induction we obtain

$$A \geq A\Big(\sum_{i=1}^{k} P_i\Big) = A(P_1) + A\Big(\sum_{i=2}^{k} P_i\Big) + V\Big(P_1, \sum_{i=2}^{k} P_i\Big)$$

$$\geq A(P_1) + A\Big(\sum_{i=2}^{k} P_i\Big) + 2(k-1) \geq \cdots$$

$$\geq \sum_{i=1}^{t} A(P_i) + A\Big(\sum_{i=t+1}^{k} P_i\Big) + 2\sum_{i=1}^{t}(k-i) \geq \sum_{i=1}^{t} A(P_i) + 2kt - t^2 - t.$$

Now, by Pick's formula $A(P_i) = I(P_i) + \frac{1}{2}B(P_i) - 1 \geq I(P_i) + \frac{1}{2}$ since $B(P_i)$, the number of boundary lattice points, is at least 3. Therefore

$$\sum_{i=1}^{t} I(P_i) \leq A + t^2 + \frac{t}{2} - 2kt.$$

Substituting this into (2.5) and simplifying, we obtain

$$Z(f) \leq k(q-1) + 2\sqrt{q}\left(A + t^2 + \frac{t}{2} - 2kt\right) + 2t. \tag{2.7}$$

It remains to note that the maximum of the right-hand side of (2.7) is attained at $t = 1$, provided $k \geq 1$ and $q \geq 4$, which establishes the required inequality. □

3. Two algorithms. Given a polytope P, to make use of our bounds in Theorem 2.6 it remains to understand

(1) how to find $L(P)$, the full Minkowski length of P, and
(2) how to determine whether there is a maximal Minkowski decomposition in P one of whose summands is an exceptional triangle.

Here we provide algorithms that answer these questions in polynomial time in $|P \cap \mathbb{Z}^2|$.

Recall that a zonotope $Z = \sum_{i=1}^{k} E_j \subseteq P$ is called *maximal for* P if k, the number of nontrivial Minkowski summands (counting their multiplicities), is equal to $L(P)$.

It follows from Proposition 1.2 that a maximal zonotope always exists although it is usually not unique. It turns out that any maximal zonotope of P has at most four distinct summands and among them there are maximal zonotopes with a particularly easy description.

PROPOSITION 3.1. *Let P be a lattice polygon. Then we have the following:*

(1) *Any zonotope Z maximal for P has at most 4 different summands.*
(2) *There exists a zonotope Z maximal for P with at most 3 different summands. Moreover, up to an $\mathrm{AGL}(2,\mathbb{Z})$-transformation these summands are $[0, e_1]$, $[0, e_2]$, and $[0, e_1 + e_2]$.*

Proof. Let $Z = \sum_{i=1}^{L} E_j$ be a zonotope maximal for P, and let v_j be the vector of E_j. According to Lemma 1.7, $|\det(v_i, v_j)| \leq 2$ for any $1 \leq i, j \leq k$.

The case when all v_i are the same is trivial. Suppose there are exactly two different summands; i.e., $Z = m_1E_1 + m_2E_2$ for some positive integers $m_1 \geq m_2$ and $E_1 \neq E_2$. If $|\det(v_1, v_2)| = 1$, then we can transform (v_1, v_2) to the standard basis (e_1, e_2) and (2) follows. If $|\det(v_1, v_2)| = 2$, then we can assume that $v_1 = e_1$ and $v_2 = e_1 + 2e_2$.

However, $E_1 + E_2$ contains $2[0, e_2]$, therefore we can pass to $Z' = (m_1 - m_2)[0, e_1] + 2m_2[0, e_2]$. Clearly, $Z' \subseteq Z$ and Z' is maximal.

Now suppose that Z has at least three different summands. First, let us assume that $|\det(v_i, v_j)| = 2$ for all $i \neq j$. As before, without loss of generality, $v_1 = e_1$ and $v_2 = e_1 + 2e_2$. Consider $v_3 = (s, t)$. By looking at the determinants $\det(v_i, v_3)$ for $i = 1, 2$, we have $|t| = 2$ and $|t - 2s| = 2$. This implies that v_3 is not primitive, a contradiction. Therefore, $|\det(v_i, v_j)| = 1$ for some $i \neq j$, and we can assume that $v_1 = e_1$ and $v_2 = e_2$. Again, we let $v_3 = (s, t)$ and look at the determinants $\det(v_i, v_3)$ for $i = 1, 2$. We see that the only vectors v_3 (up to central symmetry) that may appear are $(1, 1)$, $(1, -1)$, $(2, 1)$, $(2, -1)$, $(1, 2)$, $(1, -2)$. No two of the last four vectors can appear together as they generate parallelograms of area at least 3. For the same reason $(1, 1)$ cannot appear with $(2, -1)$ or $(1, -2)$, and $(1, -1)$ cannot appear with $(2, 1)$ or $(1, 2)$. We have three possible combinations:

(a) $v_1 = (1, 0), v_2 = (0, 1), v_3 = (1, 1), v_4 = (1, -1)$;
(b) $v_1 = (1, 0), v_2 = (0, 1), v_3 = (1, 1)$, and $v_4 = (1, 2)$ or $v_4 = (2, 1)$;
(c) $v_1 = (1, 0), v_2 = (0, 1), v_3 = (1, -1)$, and $v_4 = (1, -2)$ or $v_4 = (2, -1)$.

We have proved our first claim. To prove the second, note that we can actually reduce the number of distinct segments E_j. In case (a), $2E_1 \subset E_3 + E_4$, and we will be able to get rid of either E_3 or E_4 by replacing $E_3 + E_4$ with $2E_1$. In either case, the remaining segments are $\mathrm{AGL}(2, \mathbb{Z})$-equivalent to $[0, e_1]$, $[0, e_2]$, and $[0, e_1 + e_2]$.

In case (b) we can assume that $v_4 = (1, 2)$. Since $2E_2 \subset E_1 + E_4$, we will be able to get rid of either E_1 or E_4 and the remaining segments are $\mathrm{AGL}(2, \mathbb{Z})$-equivalent to $[0, e_1]$, $[0, e_2]$, and $[0, e_1 + e_2]$. Case (c) is obtained from (b) by flipping the second coordinate. ∎

To find $L(P)$ we only need to look at all of the zonotopes $Z \subseteq P$ with at most three different summands $\mathrm{AGL}(2, \mathbb{Z})$-equivalent to $[0, e_1]$, $[0, e_2]$, and $[0, e_1 + e_2]$ and find the one that has the largest number of summands (counting multiplicities).

THEOREM 3.2. *Let P be a lattice polygon, and let $|P \cap \mathbb{Z}^2|$ be the number of lattice points in P. Then the full Minkowski length $L(P)$ can be found in polynomial time in $|P \cap \mathbb{Z}^2|$.*

Proof. The case when P is one-dimensional is trivial so we will be assuming that P has dimension two.

For every triple of points $\{A, B, C\} \subseteq P \cap \mathbb{Z}^2$, where it is important which point goes first and the order of the other two does not matter, we check if $E_1 = [A, B]$ and $E_2 = [A, C]$ generate a parallelogram of area one. If so, we want to construct various zonotopes whose summands are E_1, E_2, and $E_3 = [A, B + C]$. We do this in the most straightforward way.

First, for every $1 \leq i \leq 3$, we find M_i, the largest integer such that a lattice translate of $M_i E_i$ is contained in P. For this we find the maximum number of lattice points in the linear sections of P with lines in the direction of E_i (there are finitely many such lines with at least one lattice point of P).

Second, for each triple of integers $m = (m_1, m_2, m_3)$, where $0 \leq m_i \leq M_i$, we check if some lattice translate of the zonotope $Z_m = m_1 E_1 + m_2 E_2 + m_3 E_3$ is contained in P (we run through lattice points D in P to check if $D + Z_m$ is contained in P). For all such zonotopes that fit into P we look at $m_1 + m_2 + m_3$ and find the maximal possible value M of this sum.

Finally, the largest such sum M over all choices of $\{A, B, C\} \subseteq P \cap \mathbb{Z}^2$ is $L(P)$, by Proposition 3.1. Clearly, this algorithm is polynomial in $|P \cap \mathbb{Z}^2|$.

Notice that in the previous argument we have taken care of the maximal zonotopes that are possibly multiples of a single segment. Indeed, if $[A, B]$ is a primitive segment connecting two lattice points in P, then unless P is one-dimensional there is a lattice point C in P such that $[A, B]$ and $[A, C]$ generate a parallelogram of area one. We can assume that A is the origin and $B = (1, 0)$. Let $C = (k, l)$ be a lattice point in P with smallest positive l (flip P with respect to the x-axis if necessary). By the minimality of l the triangle ABC has no lattice points except its vertices. By Pick's formula, its area is $1/2$ and we have found the required third vertex C. ∎

THEOREM 3.3. *Let P be a lattice polygon in $\mathbb{R}^n$. Then we can decide in polynomial time in $|P \cap \mathbb{Z}^2|$ if there is a maximal Minkowski decomposition in P one of whose summands is an exceptional triangle.*

Proof. We first run the algorithm from Theorem 3.2 to find $L(P)$. Next, for each triple of points $A, B, C \in P \cap \mathbb{Z}^2$ we check if the triangle T_{ABC} has exactly four lattice points—the three vertices A, B, C and one point D strictly inside the triangle. If so, this triangle is exceptional. If this triangle is a summand in some maximal Minkowski decomposition in P, then the other summands that may appear in this decomposition are the primitive segments E_1, E_2, and E_3 connecting D to the vertices A, B, C (see Remark 1.9).

Now it remains to look at all Minkowski sums $T_{ABC} + m_1E_1 + m_2E_2 + m_3E_3$ with $m_1 + m_2 + m_3 = L(P) - 1$ and check if any of them fits into P. If this indeed happens for some T_{ABC}, then there is a maximal decomposition in P with an exceptional triangle. Otherwise any maximal decomposition is a sum of primitive segments and unit triangles. Clearly, this algorithm is polynomial in $|P \cap \mathbb{Z}^2|$. ∎

4. Three examples. In this section we illustrate our methods with three examples. Example 2 was given by Joyner in [8]. Example 3 appears in Little and Schenck's paper [10].

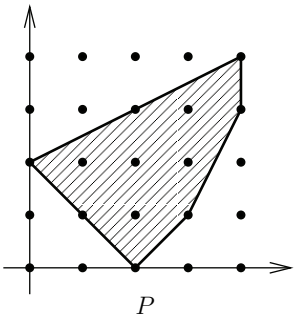

FIG. 7. *Pentagon.*

Example 1. Consider the pentagon P with vertices $(2, 0)$, $(0, 2)$, $(4, 4)$, $(4, 3)$, and $(3, 1)$ as in Figure 7. One can easily check that $L(P) = 3$ and there is a maximal decomposition in P containing T_0 (in fact, P contains $T_0 + [0, e_2] + [0, e_1 + e_2]$). Note that P defines a toric surface code of dimension $n = |P \cap \mathbb{Z}^2| = 12$. To apply Theorem 2.6 we compute $A = 15/2$, so $c = 3$. Therefore,

$$d(C_P) \geq (q-1)^2 - 3(q-1) - 2\sqrt{q} + 1$$

for all $q \geq 41$. In this particular example we can establish a better lower bound for q, namely $q \geq 19$. Indeed, we have already seen in the proof of Theorem 2.6 that every

f with 2 absolutely irreducible factors will have at most $3(q-1)+2\sqrt{q}-1$ zeros for all $q \geq 19$ (see (2.2)). If f is absolutely irreducible, then we use (2.1). Then it has at most $q+1+\lfloor 10\sqrt{q} \rfloor - 2$ zeros since $P_f \subseteq P$ has at most 5 interior lattice points in which case it will have at least two primitive edges. It remains to notice that

$$q+1+\lfloor 10\sqrt{q} \rfloor - 2 \leq 3(q-1)+2\sqrt{q}-1$$

for all $q \geq 19$.

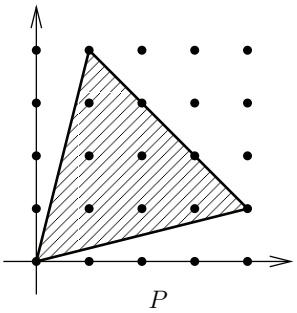

FIG. 8. *Triangle.*

Example 2. Consider the triangle P with vertices $(0,0)$, $(4,1)$, and $(1,4)$ (see Figure 8). This example is similar to the previous one. We also have $L(P) = 3$, $A = 15/2$, but the dimension of the corresponding toric surface code is slightly smaller, $n = |P \cap \mathbb{Z}^2| = 11$. However, in this case P has no exceptional triangles in any maximal decomposition. Therefore, Theorem 2.6 provides a better bound for the minimum distance

$$d(C_P) \geq (q-1)^2 - 3(q-1),$$

which holds for all $q \geq 53$. As before, this can be improved to $q \geq 37$ using (2.1) and the fact that $I(P) = 6$. Note that $f = xy(x-a)(x-b)(x-c)$, for $a, b, c \in \mathbb{F}_q^*$ distinct, has exactly $3(q-1)$ zeros in $(\mathbb{F}_q^*)^2$, hence for $q \geq 37$ the above bound is exact

$$d(C_P) = (q-1)^2 - 3(q-1). \tag{4.1}$$

For $q = 8$ this was previously established by Joyner [8]. Also (4.1) follows from Little and Schenck's result [10] for all $q \geq (4I(P)+3)^2 = 729$.

Example 3. Let P be the hexagon with vertices $(1,0)$, $(0,1)$, $(1,2)$, $(3,3)$, $(3,2)$, and $(2,0)$ (see Figure 9). We have $L(P) = 3$, $A = 5$, and $\mathcal{C}_P$ has dimension nine. Also P has no maximal decomposition with an exceptional triangle. Therefore, Theorem 2.6 implies

$$d(C_P) \geq (q-1)^2 - 3(q-1)$$

for all $q \geq 37$. Little and Schenck's result [10] proves this bound for $q > 225$. In fact we can show more in this example: for all $q \geq 11$

$$d(C_P) = (q-1)^2 - 3(q-1) + 2. \tag{4.2}$$

To see this, first note that $f = x(x-a)(y-b)(y-c)$, for $a, b, c \in \mathbb{F}_q^*$ distinct, has exactly $3(q-1)-2$ zeros in $(\mathbb{F}_q^*)^2$. Furthermore, every maximal decomposition in P

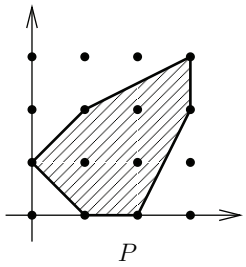

FIG. 9. *Hexagon.*

is of the form $E_1 + 2E_2$, where E_i is a primitive segment in the direction of e_1, e_2, or $e_1 + e_2$. This implies that every polynomial f with the largest number of absolutely irreducible factors (three) will have at most $3(q-1)-2$ zeros in $(\mathbb{F}_q^*)^2$ (here we take into account the intersections of the irreducible curves defined by the factors of f).

Now we claim that for $q \geq 11$ polynomials with fewer factors (one or two) will have at most $3(q-1)-2$ zeros in $(\mathbb{F}_q^*)^2$ as well. Indeed, decompositions with two summands in P can have at most one exceptional triangle, hence, $Z(f) \leq 2(q-1) + \lfloor 2\sqrt{q} \rfloor$ for every f with two irreducible factors. This will be no greater than $3(q-1)-2$ for $q \geq 9$. If f is absolutely irreducible, then by (2.1) $Z(f) \leq q + 1 + \lfloor 6\sqrt{q} \rfloor - 3$, which is no greater than $3(q-1)-2$ starting with $q = 11$.

The computations preformed in [10] show the validity of (4.2) for all $5 \leq q \leq 11$ except for $q = 8$ when the answer is $d(C_P) = (q-1)^2 - 3(q-1) = 28$. For example, the polynomial $x^2 + y + x^3y^3$ has exactly 21 zeros in $(\mathbb{F}_8^*)^2$, and so the corresponding codeword has weight 28. We now have a complete understanding of this example.

Acknowledgments. We thank Leah Gold and Felipe Martins for helpful discussions on coding theory.

REFERENCES

[1] Y. AUBRY AND M. PERRET, *A Weil theorem for singular curves*, in Arithmetic, Geometry and Coding Theory (Luminy, 1993), de Gruyter, Berlin, 1996, pp. 1–7.

[2] V. BATYREV AND B. NILL, *Multiples of lattice polytopes without interior lattice points*, Mosc. Math. J., 7 (2007), pp. 195–207, 349.

[3] M. BECK AND S. ROBINS, *Computing the continuous discretely. Integer-point enumeration in polyhedra*, Undergraduate Texts in Mathematics, Springer, New York, 2007.

[4] YU. D. BURAGO AND V. A. ZALGALLER, *Geometric Inequalities*, Springer-Verlag, Berlin, 1988.

[5] W. FULTON, *Introduction to Toric Varieties*, Ann. of Math. Stud. 131, Princeton University Press, Princeton, NJ, 1993.

[6] J. HANSEN, *Toric surfaces and error-correcting codes*, in Coding Theory, Cryptography, and Related Areas, Springer, Berlin, 2000, pp. 132–142.

[7] A. G. HOVANSKII, *Newton polyhedra, and the genus of complete intersections*, Funktsional. Anal. i Prilozhen., 12 (1978), pp. 51–61 (in Russian).

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

[9] A. G. KHOVANSKII, *Newton polytopes, curves on toric surfaces, and inversion of Weil's theorem*, Russian Math. Surveys, 52 (1997), pp. 1251–1279.

[10] J. LITTLE AND H. SCHENCK, *Toric surface codes and Minkowski sums*, SIAM J. Discrete Math., 20 (2006), pp. 999–1014.

[11] M. TSFASMAN, S. VLĂDUŢ, AND D. NOGIN, *Algebraic Geometric Codes: Basic Notions*, Mathematical Surveys and Monographs 139, AMS, Providence, RI, 2007.