SMALL POLYGONS AND TORIC CODES

GAVIN BROWN AND ALEXANDER M. KASPRZYK

ABSTRACT. We describe two different approaches to making systematic classifications of plane lattice polygons, and recover the toric codes they generate, over small fields, where these match or exceed the best known minimum distance. This includes a $[36, 19, 12]$-code over $\mathbb{F}_7$ whose minimum distance 12 exceeds that of all previously known codes.

1. INTRODUCTION

We are interested in planar lattice polygons P – not least for their own sake – and, for a finite field $\mathbb{F}_q$, the toric codes $C_P(\mathbb{F}_q)$ that they determine. We recall the construction of such codes, following Hansen [Han00, Han12], in Section 2 below. Briefly, P and q together determine a $k \times n$ integer matrix – the toric code – for integers k, the *dimension*, and n, the *block length*. The important invariant of a code C is its *minimum distance d*, the shortest Hamming distance between any two distinct points of the image of the matrix – that is, the distance between points of the lattice generated by the rows of the matrix. It is this measure which limits the ability of the code to detect and correct errors.

The collection of all toric codes includes some champions among linear codes, in the sense that they have minimum distance greater than that of any other known code with equal block length and dimension. This is exemplified by the paper of Joyner [Joy04] and the recent paper of Little [Lit11], the latter describing a generalised champion $[49, 12, 28]$-code over $\mathbb{F}_8$ (we follow the standard notation and denote the invariants of a code by a triple $[n, k, d]$). We find a new champion, a $[36, 19, 12]$-code over $\mathbb{F}_7$, however the novel part of our paper is the systematic approach to classification of polygons that we use to discover this example. This approach exploits database methods in collaboration with computer-aided polygon computations in a way that seems not to have been pursued in this area. As a spin-off, we classify a certain set of 'small' lattice polygons, as we now explain.

One of the key points when considering toric codes over $\mathbb{F}_q$ is to restrict attention to polygons P that lie in a square of side-length $m \leq q - 2$. In this paper we concentrate on fields $\mathbb{F}_q$ with $q \leq 9$ a prime power, and so we first enumerate all polygons that lie in a square of side-length $m \leq 7$. We regard two polygons P and P' as equivalent if there exists a point $u \in \mathbb{Z}^2$ and change of basis φ of the underlying lattice such that $\varphi(P - u) = P'$. Table 1 summarises our results by listing the number of integral polygons (up to equivalence) that lie in the square $[0, m] \times [0, m]$, but not in a smaller square. It also lists the maximum number of vertices that such a polygon

can have, and the number of polygons that achieve this upper bound. The complete list of polygons is available on the webpage [BK].

The systematic approach described above would certainly exhaust all toric codes over small fields (even the generalised codes of [Rua09, Lit11]), but it obviously becomes less practical as m increases. It is remarkable to us that the number of polygons grows as slowly as it does, although this is presumably an artefact of two dimensions. We seek champion codes, that is, codes exceeding the current largest known minimum distances. Computing the minimum distance is very often too hard (it is certainly computable, but in many cases we have reliable estimates of computation time of the order of a year), but determining whether or not a given code is a champion is much easier: in most cases, simple linear combinations of the rows of the corresponding matrix provide sufficiently short vectors to rule it out. We carry out this calculation for each one of these polygon codes for every applicable field of size at most nine. In this early part of the polygonal classification, there is exactly one champion – the code mentioned above – as well as many examples that match the current best known minimum distance. All but 257 of the polygonal codes have a short vector that is a combination of at most three rows of the generator matrix; only six of these, other than the champion, require more than four rows.

TABLE 1. The number of polygons (up to equivalence) contained in the square $[0, m] \times [0, m]$, but not contained in a smaller square.

m	1	2	3	4	5	6	7
#Polygons	2	15	131	1369	13842	129185	1104895
Max vertices	4	6	8	9	10	12	13
#Max polygons	1	1	1	1	15	2	3

The champion polygon and many of the equal champions are LDP-polygons (lattice polygons associated to log del Pezzo surfaces, explained in detail in Section 4). Motivated by this, we go on to consider codes associated to toric log del Pezzo surfaces, using the classification of all 15,346 LDP-polygons of index $\ell \leq 17$ [KKN10]. The difficulty here is that these polygons are not presented as lying in the smallest possible square, so we describe an algorithm that determines the smallest square that contains a polygon equivalent to a given polygon. This algorithm – an adaptation of the minimum width algorithm – is the main point, since our search through the resulting data for toric log del Pezzo codes over the smallest possible field $\mathbb{F}_q$ reveals no further champions.

2. TORIC CODES

Let $M \cong \mathbb{Z}^2$ be a two-dimensional lattice, and let $P \subset M \otimes_{\mathbb{Z}} \mathbb{Q}$ be a convex lattice polygon with vertices in M. Let $\mathbb{F}_q$ be a finite field such that, up to translation, P is contained in the square $\mathrm{conv}\{(0,0), (0, q-2), (q-2, 0), (q-2, q-2)\}$. Hansen demonstrated in [Han00, Han12] how one can associate a linear code to P. Let $\varepsilon \in \mathbb{F}_q$ be a primitive element of the field, and for

each lattice point $u := (u_1, u_2) \in P \cap M$ define:

$$e(u) : \mathbb{F}_q^* \times \mathbb{F}_q^* \to \mathbb{F}_q$$
$$(\varepsilon^i, \varepsilon^j) \mapsto (\varepsilon^i)^{u_1}(\varepsilon^j)^{u_2}.$$

The set of vectors

$$\{(e(u)(\varepsilon^i, \varepsilon^j))_{0 \leq i,j \leq q-2} \mid u \in P \cap M\}$$

then generates a linear code of block length $n = (q-1)^2$ and dimension $k = |P \cap M|$, denoted by $C_P(\mathbb{F}_q)$.

We sketch the connection with toric geometry. For the details see [Han00, Han02, Joy04]. Associated with any polygon P is a non-singular fan Δ in $N := \mathrm{Hom}\,(M, \mathbb{Z})$ given by the following construction. Let $h_P : N_{\mathbb{Q}} \to \mathbb{Q}$ be the support function defined by

$$h_P(v) := \inf\{\langle u, v \rangle \mid u \in P\}.$$

This is a piecewise linear function, and partitions $N_{\mathbb{Q}}$ into a finite collection of strictly convex polyhedral cones; in other words, h_P defines a fan Δ' in $N_{\mathbb{Q}}$. We can refine Δ' to a non-singular fan Δ by inserting rays via a well-known process (see, for example, [Oda78]). Notice that, for any cone $\sigma \in \Delta$, there exists a lattice point $l_\sigma \in M$ such that

$$h_P(v) = \langle l_\sigma, v \rangle, \qquad \text{for all } v \in \sigma.$$

Let X_P be the complete smooth toric surface associated with Δ, where the algebraic torus T_N is defined by $T_N := \mathrm{Hom}\left(M, \overline{\mathbb{F}_q}^*\right)$. The polygon P is associated with the Cartier divisor

$$D_h := -\sum_{\text{Rays } \rho \text{ of } \Delta} \langle l_\rho, \rho \rangle \cdot \mathrm{vert}(\rho),$$

where $\mathrm{vert}(\rho) \cong \mathbb{P}^1$ is the closure of the T_N orbit of ρ in X_P (again, see [Oda78] for the details) as follows. The space of global sections $H^0(X_P, \mathcal{O}_{X_P}(D_h))$ has dimension $|P \cap M|$ with basis $\{e(u) \mid u \in P \cap M\}$. Thus the code $C_P(\mathbb{F}_q)$ can be obtained via:

$$(2.1) \qquad \begin{aligned} H^0(X_P, \mathcal{O}_{X_P}(D_h))^{\mathrm{Frob}} &\to C_P(\mathbb{F}_q) \\ f &\mapsto (f(t))_{t \in T_N}. \end{aligned}$$

The generators of the code are given by the image of the basis; i.e.

$$\{(e(u)(t))_{t \in T_N} \mid u \in P \cap M\}.$$

The toric codes $C_P(\mathbb{F}_q)$ obtained via translation of P, or more generally by any affine linear isomorphism of $M \cong \mathbb{Z}^2$, are monomially equivalent [LS07, Theorem 4], hence it is sufficient to consider P up to equivalence. Following [Rua09, Lit11] one can restrict the evaluation map (2.1) to a subspace of the Riemann–Roch space to construct *generalised* toric codes.

3. Classifying small polygons

Definition 3.1. *Let $P \subset M_{\mathbb{Q}}$ be a lattice polytope, and let $v \in \mathrm{vert}(P)$ be a vertex of P. If the polytope $P_v := \mathrm{conv}((P \cap M) \setminus \{v\})$ satisfies $\dim P_v = \dim P$, then P_v is said to have been obtained from P by* shaving. *Given a polytope Q we say that Q can be obtained from P via* successive shaving *if there exists a sequence of shavings $Q = P^{(0)} \subset \cdots \subset P^{(n)} = P$, where $P^{(i-1)} = P_{v_i}^{(i)}$ for some $v_i \in \mathrm{vert}(P^{(i)})$, $0 < i \leq n$.*

Lemma 3.2. *Any lattice polygon Q in the box $B_m := [0, m] \times [0, m]$ can be obtained from B_m via successive shaving.*

Proof. Let $Q \subset B_m$. If $Q \neq B_m$, then we can certainly shave a vertex v of B_m to obtain a polygon P_v that contains Q. Continuing inductively, suppose $P \subset B_m$ is a polygon with $Q \subset P$. If $P \neq Q$ then there exists some vertex $v \in \mathrm{vert}(P)$ such that $v \notin Q$ and $Q \subseteq P' := P_v$. But

$$\mathrm{Vol}(Q) \leq \mathrm{Vol}(P') < \mathrm{Vol}(P).$$

Since these normalised volumes are integers, this process must terminate after finitely many steps. $\qquad\square$

Remark 3.3. The normalised volume $\mathrm{Vol}(P)$ of a lattice polygon P is twice the Euclidean volume $\mathrm{vol}(P)$; when P is a lattice polygon, $\mathrm{vol}(P) \in (1/2)\mathbb{Z}$.

It is clear how this lemma presents an algorithm for classifying small polygons. Choose a box B_m and initialise a sequence containing that box as a polygon:

```
Ps:=[Polytope([[0,0],[0,m],[m,0],[m,m]])];
```

The algorithm now extends `Ps` recursively by shaving the vertices from each polygon in the sequence, checking for equivalence before appending each new polygon.

```
idx:=1;
while idx le #Ps do
    for v in Vertices(Ps[idx]) do
        P:=Polytope(Exclude(Points(Ps[idx]),v));
        if Dimension(P) eq 2 and not &or[IsEquivalent(P,Q) : Q in Ps] then
            Append(~Ps,P);
        end if;
    end for;
    idx +:= 1;
end while;
```

The appeal to `IsEquivalent` is simply checking that the new polygon P is not equivalent to a polygon already contained in the sequence. This is the basic algorithm (after checking simple invariants, attempt to build an isomorphism working up from low-valency vertices), which works well for small values of m; larger boxes require some straightforward optimisations that we do not describe.

4. LOG DEL PEZZO CODES

A polygon $P \subset N \otimes_{\mathbb{Z}} \mathbb{Q}$ is said to be an *LDP-polygon* if it contains the origin strictly in its interior, and if each vertex of P is a primitive lattice point in $N := \mathrm{Hom}\,(M, \mathbb{Z})$. In this case the corresponding toric variety is a log del Pezzo surface: it has only cyclic quotient singularities and $-K_X$ is ample. For example, the polygon $\mathrm{conv}\{(1,0), (0,1), (-1,-1)\}$ is an LDP-polygon corresponding to the projective plane $\mathbb{P}^2$. For such P, the dual polygon P^* is defined by

$$P^* := \{v \in M_{\mathbb{Q}} \mid \langle v, u \rangle \geq -1 \text{ for all } u \in P\}.$$

Typically P^* is not a *lattice* polygon, but there exists a smallest integer $\ell \geq 1$ for which the vertices of ℓP^* are lattice points. This integer ℓ is called the *index* of P. It equals the Gorenstein index of the corresponding log del Pezzo surface.

There are infinitely many LDP-polygons, but finitely many for any fixed index ℓ. Figure 1 shows an LDP-polygon with vertices $(-1, 2)$, $(1, 2)$, $(1, 0)$, $(-1, -1)$, $(-2, -1)$. It has index $\ell = 10$; the dual is a lattice polygon after dilating by a factor of 10.
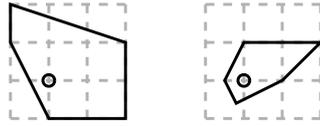
FIGURE 1. An LDP-polygon of index $\ell = 10$, with its dual rational polygon.

The classification of LDP-polygons of indices $1 \leq \ell \leq 17$ is given in [KKN10] and available online at [BK]; the example in Figure 1 is No. 523 in the classification. To use these for toric codes, we allow for translation, and must find equivalent polygons that lie in a box B_m, rather than containing the origin as given. The representative polygons in the database are not necessarily the smallest, so we describe an algorithm to determine, for given polygon P, the smallest m for which there is a polygon $P' \subset B_m$ equivalent to P. (We treat LDP-polygons simply as a source of interesting examples to generate codes, and therefore regard P as lying in $M_{\mathbb{Q}}$, rather than in terms of algebraic geometry, where they should be viewed as lying in $N_{\mathbb{Q}}$. Our work here is entirely in terms of $M_{\mathbb{Q}}$, so no confusion arises from the name.)

Lemma 4.1. *There is a constructive algorithm that, for any given polygon $P \subset M_{\mathbb{Q}}$, determines the smallest m for which there is a polygon $P' \subset B_m$ equivalent to P, without enumerating any other polygons.*

Proof. We use a modification of the standard minimal width algorithm. Begin by considering $w_i := \mathrm{wd}_{e_i^*}(P)$ for each dual basis vector $e_i^* \in N := \mathrm{Hom}\,(M, \mathbb{Z})$. If $w_i \leq m$ for all i, then, after possible translation, P is contained in B_m.

Suppose without loss of generality that $w_1 > m$. Translate P so that the (rational) point

$$\frac{1}{|\mathrm{vert}(P)|} \sum_{v \in \mathrm{vert}(P)} v \in P^{\mathrm{int}}$$

is at the origin. Let $\bigcirc \subset P$ be the largest disc, centred at the origin, that is contained in P. Then $d := \mathrm{wd}_{e_1^*}(\bigcirc)$ satisfies $0 < d \le w_1$. In the dual space $N_{\mathbb{Q}}$, consider the disc D centred at the origin of radius w_1/d. We claim that $\mathrm{wd}_u(P) > w_1$ for any primitive lattice point $u \in N \setminus D$. Indeed

$$\mathrm{wd}_u(P) \ge \mathrm{wd}_u(\bigcirc) > \mathrm{wd}_{u'}(\bigcirc) = \frac{w_1}{d} \cdot d = w_1,$$

where u' is the unique rational point lying on the boundary of D in the direction of u. Thus P is equivalent to some $P' \subset B_m$ if and only if there exists a dual basis $\mathcal{B}_m$ contained in D such that $\mathrm{wd}_v(P) \le m$ for each $v \in \mathcal{B}_m$, and this is a finite search. □

Applying this to the LDP-polygons, we find they distribute over m as in Table 2; we have cut the table short, but it could be continued to list all 15,346 polygons, with maximum $m = 68$.

TABLE 2. The number of LDP-polygons (up to equivalence) of index $\ell \le 17$ contained in the box $[0, m] \times [0, m]$, but not contained in a smaller box, for small values of m.

m	2	3	4	5	6	7	8	9	10
#	11	62	364	591	1125	777	1277	904	1187

5. The computations and champion polygons

We use the computer algebra system MAGMA [BCP97], and in particular its convex polytope [BBK11] and linear codes packages. The polygons are harvested from the Graded Ring Database [BK], which can be queried from within MAGMA via an XML interface. Since the number of calculations are rather large, they were run in parallel on a cluster of 144 processor cores at Imperial College, London.

The LDP-polygon number 75 in the Graded Ring Database gives a code over $\mathbb{F}_7$ that has length 36, dimension 19 and minimum distance 12 (see Figure 2; this corresponds to a unique LDP-polygon, since the only point that could serve as an origin is $(2, 2)$). The previous best known minimum distance was 11, according to Grassl's online database of linear codes [Gra] (also accessible from within MAGMA); the theoretical maximum is 15.
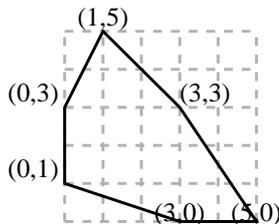
FIGURE 2. The translated LDP-polygon with database id 75.

A curiosity about polygons falls out of the classification. Among those having the maximal number of vertices for their box size, there is a unique one of minimal volume that is homogeneous (by which we mean that all vertices are locally isomorphic to one another). We sketch the polygons with maximal number of vertices for $m \leq 7$ in Figure 3; notice that for $m = 7$ there are two polygons, but only the first is homogeneous.
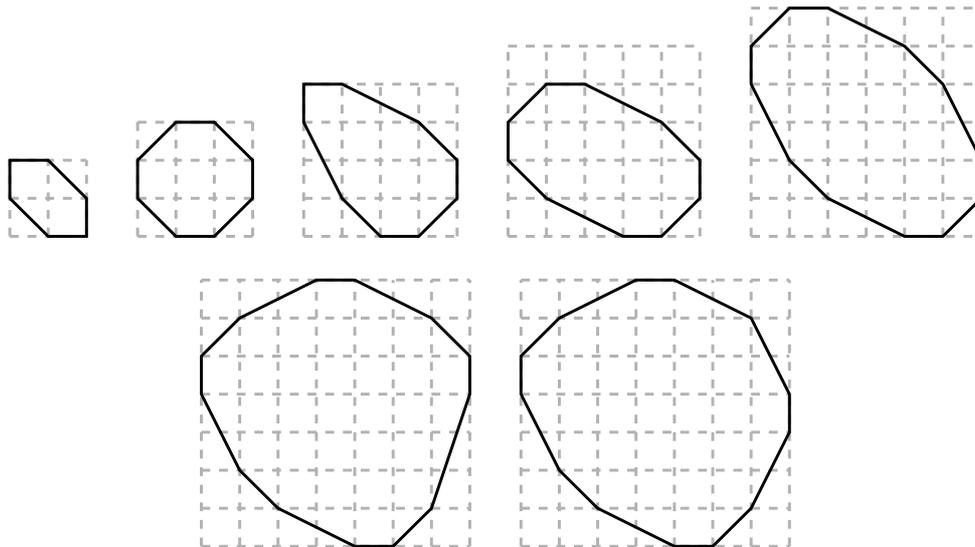
FIGURE 3. The polygons with maximal number of vertices for each box size which have the smallest volume.

We reinterpret this geometrically as the following statement, which holds for box size up to seven.

Conjecture 5.1. *Fix $m \in \mathbb{Z}_{>0}$. Consider all toric surfaces S with $-K_S$ ample (but no conditions on the singularities) for which the anticanonical polygon of monomials in $H^0(S, -K_S)$ lies in an $m \times m$ box. Among such S, consider those with maximum Picard rank. Then among these there is a unique surface S which is both smooth and has minimum anticanonical degree.*

6. HIGHER PRIME POWERS

We cannot calculate minimum distances, or indeed champions, for higher prime powers: for many polygons with the potential for a large minimum distance, the computation time required to prove this is in the order of millions of years. For specific polygons there exist results on the minimum distance for general prime powers q [LS07, YZ09], and more can be said when the polygon is Minkowski decomposable [LS06], however we do not pursue these techniques here.

Instead, we begin to estimate minimum distances using linear combinations of four rows of the generator matrix. Recall from the introduction that amongst the 1,249,439 toric codes generated by polygons in boxes of size up to $m = 7$, all but six are either shown not to be an equal champion, or to have a prohibitively short vector witnessed by some linear combination of rows involving at most only four rows.

We work with the next two possible values $q = 11$ and 13, with box sizes 8–9 and 10–11 respectively. In each case, we find all LDP-polygons from the database (of index ≤ 17) whose minimum box has size m for which q is minimal satisfying $q - 2 \geq m$. In other words, each known LDP-polygon will be considered in a minimum box and with respect to its minimum q.

We partition these LDP-polygons by their number of points, k. For each k, we work through the polygons and find the length of the shortest vector that is a linear combination of up to four rows of the generator matrix, obtaining an upper bound d_b on the best minimum distance that could be achieved. These bounds are listed in Tables 3–4.

Remark 6.1. In theory the bound d_b depends on the choice of embedding of P in the box B_m; some embeddings may give sharper bounds than others. Lemma 4.1 can generate all possible embeddings in B_m, and experimentation suggests that for practical purposes d_b is insensitive to the choices made.

TABLE 3. The number of LDP-polygonal codes with (minimal) $q = 11$. The first row is the dimension k of the code; the second, the length of a known vector, and so an upper bound for the largest minimum distance; the third, the number of polygons (up to equivalence) having such a vector achieving this bound.

k	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
d_b	30	30	30	30	30	30	30	30	30	30	30	40	40	40	30	40	40	30
#	1	1	2	2	3	5	5	4	5	6	6	2	1	1	6	2	1	11
k	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
d_b	40	36	40	40	40	40	40	40	40	40	38	35	35	30	32	39	36	30
#	1	1	2	5	4	1	2	2	3	2	1	2	1	11	1	1	1	2
k	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
d_b	30	27	27	20	27	27	25	25	18	16	16	12	10	–	–	12	–	8
#	2	4	2	6	1	2	1	1	1	2	1	2	1	–	–	2	–	1

REFERENCES

[BBK11]   Gavin Brown, Jarosław Buczyński, and Alexander M. Kasprzyk, *Convex polytopes and polyhedra*, Handbook of Magma Functions, Edition 2.17, 2011, available online at `http://magma.maths.usyd.edu.au/`.

[BCP97]   Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993).

TABLE 4. The number of LDP-polygonal codes with (minimal) $q = 13$; rows as in Table 3.

k	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
d_{b}	36	36	36	36	36	36	36	36	36	36	36	36	36	48	36	36	36
#	1	1	2	2	3	3	4	4	5	4	5	3	3	1	2	1	3
k	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
d_{b}	40	36	48	48	48	36	36	40	48	48	48	63	63	63	63	51	54
#	1	2	6	2	2	8	2	1	3	2	7	2	2	1	1	1	1
k	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62
d_{b}	60	56	60	56	56	45	48	48	48	48	48	40	36	36	36	45	33
#	1	1	1	1	2	2	1	1	3	1	2	3	3	5	1	1	1
k	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	
d_{b}	42	40	48	36	30	30	22	12	12	12	33	12	24	12	12	12	
#	1	1	1	1	1	1	1	6	3	4	1	3	2	1	3	1	

[BK]   Gavin Brown and Alexander M Kasprzyk, *The graded ring database homepage*, online, access via `http://grdb.lboro.ac.uk/`.

[Gra]   Markus Grassl, *Bounds on the minimum distance of linear codes and quantum codes*, online, access via `http://www.codetables.de/`.

[Han00] Johan P. Hansen, *Toric surfaces and error-correcting codes*, Coding theory, cryptography and related areas (Guanajuato, 1998), Springer, Berlin, 2000, pp. 132–142.

[Han02] _____, *Toric varieties, Hirzebruch surfaces and error-correcting codes*, Appl. Algebra Engrg. Comm. Comput. **13** (2002), no. 4, 289–300.

[Han12] _____, *Quantum codes from toric surfaces*, `arXiv:1203.4544v1 [math.AG]`, March 2012.

[Joy04] David Joyner, *Toric codes over finite fields*, Appl. Algebra Engrg. Comm. Comput. **15** (2004), no. 1, 63–79.

[KKN10] Alexander M. Kasprzyk, Maximilian Kreuzer, and Benjamin Nill, *On the combinatorial classification of toric log del pezzo surfaces*, LMS Journal of Computation and Mathematics **13** (2010), 33–46.

[Lit11]   John B. Little, *Remarks on generalized toric codes*, `arXiv:1107.4530v2 [cs.IT]`.

[LS06]   John Little and Hal Schenck, *Toric surface codes and Minkowski sums*, SIAM J. Discrete Math. **20** (2006), no. 4, 999–1014 (electronic).

[LS07]   John Little and Ryan Schwarz, *On toric codes and multivariate Vandermonde matrices*, Appl. Algebra Engrg. Comm. Comput. **18** (2007), no. 4, 349–367.

[Oda78] Tadao Oda, *Torus embeddings and applications*, Tata Inst. Fund. Res. Stud. Math., vol. 57, Tata Institute of Fundamental Research, Bombay, 1978.

[Rua09] Diego Ruano, *On the structure of generalized toric codes*, J. Symbolic Comput. **44** (2009), no. 5, 499–506.

[YZ09]   Stephen S.-T. Yau and Huaiqing Zuo, *Notes on classification of toric surface codes of dimension 5*, Appl. Algebra Engrg. Comm. Comput. **20** (2009), no. 2, 175–185.

DEPARTMENT OF MATHEMATICAL SCIENCES, LOUGHBOROUGH UNIVERSITY, LOUGHBOROUGH, LE11 3TU, UNITED KINGDOM

E-mail address: `G.D.Brown@lboro.ac.uk`

DEPARTMENT OF MATHEMATICS, IMPERIAL COLLEGE LONDON, LONDON, SW7 2AZ, UNITED KINGDOM

E-mail address: `a.m.kasprzyk@imperial.ac.uk`