# The Order Bound for Toric Codes*

Peter Beelen[†] Diego Ruano[‡]

**Abstract**

In this paper we investigate the minimum distance of generalized toric codes using an order bound like approach. We apply this technique to a family of codes that includes the Joyner code. For some codes in this family we are able to determine the exact minimum distance.

## 1 Introduction

In 1998 J.P. Hansen considered algebraic geometry codes defined over toric surfaces [7]. Thanks to combinatorial techniques of such varieties he was able to estimate the parameters of the resulting codes. For example, the minimum distance was estimated using intersection theory. Toric geometry studies varieties which contain an algebraic torus as a dense subset and where moreover the torus acts on the variety. The importance of such varieties, called toric varieties, resides in their correspondence with combinatorial objects, which makes the techniques to study the varieties (such as cohomology, intersection theory, resolution of singularities, etc) more precise and at the same time tractable [3, 6].

The order bound gives a way to obtain a lower bound for the minimum distance of linear codes [1, 4, 5, 9]. Especially for codes from algebraic curves this technique has been very successful. In this article we will develop a similar bound for toric codes. Actually our bound also works for the more general class of generalized toric codes (see Section 2). This will give a new way of estimating the minimum distance of toric codes that in some examples give a better bound than intersection theory. Another advantage is that known algorithms [4, 5] can be used to decode the codes up to half the order bound. As an example we will compute the order bound for a family of codes that includes the Joyner codes [11]. For this reason we call these codes generalized Joyner codes. Also we will compute the exact minimum distance for several generalized Joyner codes. It turns out that a combination of previously known techniques and the order bound gives a good estimate of the minimum distance of generalized Joyner codes.

The paper is organized as follows. In Section 2 we will give an introduction to toric codes and generalized toric codes, while in Section 3 the order bound

*The work of D. Ruano is supported in part by DTU, H.C. Oersted post doc. grant (Denmark) and by MEC MTM2007-64704 and Junta de CyL VA065A07 (Spain)

[†]DTU-Mathematics, Technical University of Denmark, Matematiktorvet, Building 303, 2800 Kgs. Lyngby, Denmark. P.Beelen@mat.dtu.dk

[‡]Department of Mathematics, Technical University of Denmark, Matematiktorvet, Building 303, DK-2800, Kgs. Lyngby, Denmark. D.Ruano@mat.dtu.dk

for these codes will be established. The last section of the paper will illustrate the theory by applying the results to generalized Joyner codes.

## 2 Toric Codes and Generalized Toric Codes

Algebraic geometry codes [9, 19] are usually defined evaluating algebraic functions over a non-singular projective variety $X$ defined over a finite field. The functions of $\mathcal{L}(D)$ are evaluated at certain rational points of the curve ($\mathcal{P} = \{P_1, \dots, P_n\}$), where $D$ is a divisor whose support does not contain any of the evaluation points. The zeros and poles of the functions of $\mathcal{L}(D)$ are bounded by $D$. More precisely, the algebraic geometry code $\mathcal{C}(X, D, \mathcal{P})$ is the image of the linear map:

$$\begin{array}{rcl} \mathrm{ev} : \mathcal{L}(D) & \to & \mathbb{F}_q^n \\ f & \mapsto & (f(P_1), \dots, f(P_n)) \end{array}$$

In this section we introduce toric codes, that is, algebraic geometry codes over toric varieties. One can define a toric variety and a Cartier divisor using a convex polytope, namely, a convex polytope is the same datum as a toric variety and Cartier divisor. Let $M$ be a lattice isomorphic to $\mathbb{Z}^r$ for some $r \in \mathbb{Z}$ and $M_{\mathbb{R}} = M \otimes \mathbb{R}$. Let $P$ be an $r$-dimensional rational convex polytope in $M_{\mathbb{R}}$ and let us consider $X_P$ and $D_P$ the toric variety and the Cartier divisor defined by $P$ [15]. We may assume that $X_P$ is non singular, in other case we refine the fan [6, Section 2.6]. Let $\mathcal{L}(D_P)$ be the $\mathbb{F}_q$-vector space of functions $f$ over $X_P$ such that $\mathrm{div}(f) + D_P \succeq 0$.

The toric code $\mathcal{C}(P)$ associated to $P$ is the image of the linear evaluation map

$$\begin{array}{rcl} \mathrm{ev} : \mathcal{L}(D_P) & \to & \mathbb{F}_q^n \\ f & \mapsto & (f(t))_{t \in T} \end{array}$$

where the set of points $\mathcal{P} = T$ is the algebric torus $T = (\mathbb{F}_q^*)^r$. Since we evaluate at $\#T$ points, $\mathcal{C}(P)$ has length $n = (q-1)^r$. One has that $\mathcal{L}(D_P)$ is the $\mathbb{F}_q$-vector space generated by the monomials with exponents in $P \cap M$

$$\mathcal{L}(D_P) = \langle \{X^u = X_1^{u_1} \cdots X_r^{u_r} \mid u \in P \cap M\} \rangle \subset \mathbb{F}_q[X_1, \dots, X_r]$$

The minimum distance of a toric code $\mathcal{C}(P)$ may be estimated using intersection theory [8, 15]. Also, it can be estimated using a multivariate generalization of Vandermonde determinants on the generator matrix [13]. For plane polytopes, $r = 2$, one can estimate the minimum distance using the Hasse-Weil bound and combinatorial invariants of the polytope (the Minkowsky sum [12] and the Minkowsky length [17]).

An extension of toric codes are the so-called generalized toric codes [16]. The generalized toric code $\mathcal{C}(U)$ is the image of the $\mathbb{F}_q$-linear map

$$\begin{array}{rcl} \mathrm{ev} : \mathbb{F}_q[U] & \to & \mathbb{F}_q^n \\ f & \mapsto & (f(t))_{t \in T} \end{array}$$

where $U \subset H = \{0, \dots, q-2\}^r$ and $\mathbb{F}_q[U]$ is the $\mathbb{F}_q$-vector space

$$\mathbb{F}_q[U] = \langle X^u = X_1^{u_1} \cdots X_r^{u_r} \mid u = (u_1, \dots, u_r) \in U \rangle \subset \mathbb{F}_q[X_1, \dots, X_r].$$

Let $\overline{u}$ be $u \mod ((q-1)\mathbb{Z})^r$, that is $\overline{u} = (u_1 \mod (q-1), \ldots, u_r \mod (q-1))$, for $u \in \mathbb{Z}^r$, and $\overline{U} = \{\overline{u} \mid u \in U\}$. The dimension of the code $\mathcal{C}(U)$ is $k = \#\overline{U} = \#U$, since the evaluation map ev is injective.

By [16, Theorem 6], one has that the dual code of $\mathcal{C}(U)$ is $\mathcal{C}(U^\perp)$, where $U^\perp = H \setminus \overline{-U}$, with $\overline{-U} = \{\overline{-u} \,|\, u \in U\}$. Namely, we have

$$\mathrm{ev}(X^u) \cdot \mathrm{ev}(X^{u'}) = \begin{cases} 0 & \text{if } \overline{u+u'} \neq 0 \\ (-1)^r & \text{if } \overline{u+u'} = 0 \end{cases} \tag{1}$$

for $u, u' \in H$, where $\cdot$ denotes the inner product in $\mathbb{F}_q^n$.

The family of generalized toric codes includes the ones obtained evaluating polynomials of an arbitrary subalgebra of $\mathbb{F}_q[X_1, \ldots, X_r]$ at $T$, in particular toric codes. However, there is no estimate so far for the minimum distance in this more general setting, the order bound techniques in this paper will apply to generalized toric codes as well. From now on we will consider generalized toric codes but for the sake of simplicity, we will just call them toric codes.

## 3 The Order Bound for Toric Codes

In this section we follow the order bound approach to estimate the minimum distance of the dual code of a toric code $\mathcal{C}(U)$, for $U \subset H$.

Let $\mathcal{B}_1 = \{g_1, \ldots, g_n\}$ and $\mathcal{B}_2 = \{h_1, \ldots, h_n\}$ be two bases of $\mathbb{F}_q[H]$. For $c = \mathrm{ev}(f) \in \mathcal{C}(U)$, we consider the syndrome matrix $S(c) = (s_{i,j})_{1 \leq i,j \leq n}$, with $s_{i,j} = (\mathrm{ev}(g_i) * \mathrm{ev}(h_j)) \cdot \mathrm{ev}(f) = \mathrm{ev}(g_i h_j) \cdot \mathrm{ev}(f)$, where $*$ denotes the componentwise product. In other words, $S(c) = M_1 D(c) M_2^t$, where $D$ is the diagonal matrix with $c$ in the diagonal and $M_1$ and $M_2$ are the evaluation matrices given by

$$M_1 = \begin{pmatrix} g_1(t_1) & g_1(t_2) & \cdots & g_1(t_n) \\ g_2(t_1) & g_2(t_2) & \cdots & g_2(t_n) \\ \vdots & \vdots & \vdots & \vdots \\ g_n(t_1) & g_n(t_2) & \cdots & g_n(t_n) \end{pmatrix}, \quad M_2 = \begin{pmatrix} h_1(t_1) & h_1(t_2) & \cdots & h_1(t_n) \\ h_2(t_1) & h_2(t_2) & \cdots & h_2(t_n) \\ \vdots & \vdots & \vdots & \vdots \\ h_n(t_1) & h_n(t_2) & \cdots & h_n(t_n) \end{pmatrix}.$$

Here $t_1, \ldots, t_n$ denote the points of the algebraic torus. Note that $M_1$ and $M_2$ have full rank, since the evaluation map is injective. This implies that the rank of $S(c)$ equals $\mathrm{wt}(c)$. It is convenient to consider bases of $\mathbb{F}_q[H]$ consisting of monomials, that is, we set $g_i = X^{v_i}$ and $h_i = X^{w_i}$, for $i = 1, \ldots, n$, with $\{v_1, \ldots, v_n\} = \{w_1, \ldots, w_n\} = H$. Then, we can easily compute the syndrome matrix for a codeword using the following lemma.

**Lemma 3.1.** *Let* $f = \sum_{u \in H} \lambda_u X^u$ *and* $S(\mathrm{ev}(f)) = (s_{i,j})_{1 \leq i,j \leq n}$ *the syndrome matrix of* ev$(f)$. *Then, one has that* $s_{i,j} = (-1)^r \lambda_{\overline{-(v_i+w_j)}}$. *In particular,* $s_{i,j}$ *is equal to zero if and only if* $\overline{v_i + w_j} \notin \overline{-\mathrm{supp}(f)}$, *where* supp$(f)$ *denotes the support of* $f$, $\mathrm{supp}(f) = \{u \in H \mid \lambda_u \neq 0\}$.

*Proof.* By definition,

$$\begin{aligned} s_{i,j} &= \mathrm{ev}(X^{\overline{v_i+w_j}}) \cdot \mathrm{ev}(\sum_{u \in H} \lambda_u X^u) = \sum_{u \in H} \mathrm{ev}(X^{\overline{v_i+w_j}}) \cdot \mathrm{ev}(\lambda_u X^u) \\ &= (-1)^r \lambda_{\overline{-(v_i+w_j)}} \quad \text{(by (1))}. \end{aligned}$$

Therefore, $s_{i,j}$ is equal to zero if and only if $\overline{-(v_i + w_j)}$ is not in the support of $f$. Equivalently, $s_{i,j} = 0$ if and only if $\overline{v_i + w_j} \notin \overline{-\mathrm{supp}(f)}$. □ □

To bound the minimum distance using order domain theory, we should give a lower bound for the rank of the syndrome matrix. Since the order bound gives an estimate for the minimum distance of the dual code, we begin by considering $\mathcal{C}(U)^\perp = \mathcal{C}(U^\perp)$ to get a bound for the minimum distance of $\mathcal{C}(U)$.

Let $H = \{u_1, \dots, u_n\}$, with $U^\perp = \{u_1, \dots, u_{n-k}\} \subset H$, notice that $U = \{\overline{-u_{n-k+1}}, \dots, \overline{-u_n}\}$. We are dealing with an arbitrary order on $H$, we only require, for the sake of simplicity, that the first $n-k$ elements of $H$ are the elements of $U^\perp$. For $l \in \{0, \dots, k-1\}$, we consider the following filtration of codes depending on the previous ordering

$$C \subsetneq C_1 \subsetneq C_2 \subsetneq \cdots \subsetneq C_l \subsetneq C_{l+1},$$

where $C = \mathcal{C}(U^\perp)$ and $C_m = \mathcal{C}(U^\perp \cup \{u_{n-k+1}, \dots, u_{n-k+m}\})$, for $m = 1, \dots, l+1$, and their dual codes,

$$C^\perp \supsetneq C_1^\perp \supsetneq C_2^\perp \supsetneq \cdots \supsetneq C_l^\perp \supsetneq C_{l+1}^\perp,$$

with $C^\perp = \mathcal{C}(U)$ and $C_m^\perp = \mathcal{C}(U \setminus \{\overline{-u_{n-k+1}}, \dots, \overline{-u_{n-k+m}}\})$, for $m = 1, \dots, l+1$, since $(U^\perp \cup \{u_{n-k+1}, \dots, u_{n-k+m}\})^\perp = U \setminus \{\overline{-u_{n-k+1}}, \dots, \overline{-u_{n-k+m}}\}$.

We wish to bound the weight of $c \in C_l^\perp \setminus C_{l+1}^\perp$. Let $\nu_l$ be the largest integer (in $\{1, \dots, n\}$) such that

- $\overline{v_i + w_i} = u_{n-k+l+1}$, for $i = 1, \dots, \nu_l$.
- $\overline{v_i + w_j} \in U^\perp \cup \{u_{n-k+1}, \dots, u_{n-k+l}\}$, for $i = 1, \dots, \nu_l$ and $j < i$.

**Proposition 3.2.** *Let $c \in \mathcal{C}_l^\perp \setminus \mathcal{C}_{l+1}^\perp$, then $wt(c) \geq \nu_l$.*

*Proof.* Let $c = ev(f)$, then $f = \sum \lambda_u X^u$, where $u \in U \setminus \{\overline{-u_{n-k+1}}, \dots, \overline{-u_{n-k+l}}\}$. Notice that $\lambda_{\overline{-u_{n-k+l+1}}} \neq 0$, since $c \notin C_{l+1}^\perp$. Hence we have by Lemma 3.1 that,

- $s_{i,i} \neq 0$, for $i = 1, \dots, \nu_l$, since $\overline{v_i + w_i} = u_{n-k+l+1} \in \overline{-\mathrm{supp}(f)}$, for $i = 1, \dots, \nu_l$.
- $s_{i,j} = 0$, for $i = 1, \dots, \nu_l$, since $\overline{v_i + w_j} \in U^\perp \cup \{u_{n-k+1}, \dots, u_{n-k+l}\}$, for $j < i$. That is, $\overline{v_i + w_j} \notin \overline{-\mathrm{supp}(f)}$ because
$$H \setminus (U^\perp \cup \{u_{n-k+1}, \dots, u_{n-k+l}\}) = \overline{-U} \setminus \{u_{n-k+1}, \dots, u_{n-k+l}\}$$

Therefore, the submatrix of $S(c)$ consisting of the first $\nu_l$ rows and columns has full rank. In particular, the rank of $S(c)$ is at least $\nu_l$ and the result holds since the rank of $S(c)$ is equal to the weight of $c$. □ □

For every $l$ in $\{0, \dots, k-1\}$ we consider a filtration and we obtain a bound for the weight of a word in $\mathcal{C}_l^\perp \setminus \mathcal{C}_{l+1}^\perp$. Therefore, we have obtained the following bound for the minimum distance of $C^\perp = \mathcal{C}(U)$.

**Theorem 3.3.** *Let $\mathcal{C}(U)$ be a toric code with $U \subset H$. Then,*

$$d(\mathcal{C}(U)) \geq \min\{\nu_l \mid l = 0, \dots, k-1\}.$$

**Remark 3.4.** We can apply known decoding algorithms [4, 5] to decode a toric code $\mathcal{C}(U)$ up to half of the order bound obtained in the previous theorem.

In the next section we will use the above approach to estimate the minimum distance of a family of toric codes.

# 4 Generalized Joyner Codes

In this section we will introduce a class of toric codes that includes the well-known Joyner code [11, Example 3.9]. After introducing these codes, we will calculate a lower bound for their minimum distances using techniques from Section 3. Then we will calculate another lower bound for the minimum distance using a combination of the order bound and Serre's improvement of Hasse-Weil's theorem on the number of rational points on a curve [18]. In some cases we are able to compute the exact minimum distance. In this section we will always assume that $r = 2$, so that $H = \{0, \dots, q-2\} \times \{0, \dots, q-2\}$.

**Definition 4.1.** Let $q$ be a power of a prime and $a$ an integer satisfying $2 \leq a \leq q-2$. We define the sets

$$U_a = \{(u_1, u_2) \in H \mid u_1 + u_2 \leq a+1, u_1 - au_2 \leq 0, -au_1 + u_2 \leq 0\},$$

$$T_a = \{(u_1, u_2) \in H \mid u_1 + u_2 \leq a+1, u_1 \geq 1, u_2 \geq 1\},$$

$$V_a = U_a \backslash \{(1, a)\}, \text{ and } W_a = U_a \backslash \{(a, 1)\}.$$

The set $U_a$ consists of all elements of $H$ lying in or on the boundary of the triangle with vertices $(0, 0)$, $(1, a)$ and $(a, 1)$. Note that the condition on $a$ ensures that the points $(1, a)$ and $(a, 1)$ are in $H$. Also note that the set $U_a$ can be obtained by joining $(0, 0)$ to the set $T_a$. All sets in the above definition are actually sets of integral points in a polytope, so the corresponding codes are classical toric codes.

We wish to investigate the toric code $\mathcal{C}(U_a)$ and begin by establishing some elementary properties:

**Lemma 4.2.** *The code $\mathcal{C}(U_a)$ is an $[(q-1)^2, 1 + a(a+1)/2, d]$ code over $\mathbb{F}_q$ and we have $d \leq (q-1)(q-a)$.*

*Proof.* Since the set $U_a$ is contained in $H$, the dimension of the corresponding code is equal to the number of elements in $U_a$. Since $U_a$ can be obtained by joining $\{(0, 0)\}$ to the set $T_a$ the formula for the dimension follows by a counting argument.

To prove the result on the minimum distance first note that the code $\mathcal{C}(T_a)$ is a subcode of $\mathcal{C}(U_a)$. It is well known, [8, Theorem 1.3], that $d(\mathcal{C}(T_a)) = (q-1)(q-a)$, so the result follows. □ □

The code $\mathcal{C}(U_4)$ is the Joyner code over $\mathbb{F}_q$, see [11]. It is known that for $q \geq 37$ its minimum distance is equal to $(q-1)(q-4)$, [17], meaning that the upper bound in the previous lemma is attained. In fact equality already holds for much smaller $q$. Using a computer one finds that $q = 8$ is the smallest value of $q$ for which equality holds. It is conjectured that for all $q \geq 8$ one has that $d(\mathcal{C}(U_4)) = (q-1)(q-4)$. This behavior turns out to happen as well for other values of $a$. This is the reason we study these codes in this section. We proceed our investigation by calculating two lower bounds for the minimum distance of the codes $\mathcal{C}(U_a)$. The first one holds for any $q$, while the second one turns out to be interesting only for large $q$.

**Proposition 4.3.** *The minimum distance $d$ of the $\mathbb{F}_q$-linear code $\mathcal{C}(U_a)$ satisfies $d \geq (q-1)(q-a-1)$.*

*Proof.* Since $d(\mathcal{C}(T_a)) = (q-1)(q-a)$, the proposition follows once we have shown that $\mathrm{wt}(c) \geq (q-1)(q-a-1)$ for any $c \in \mathcal{C}(U_a)\backslash\mathcal{C}(T_a)$. For such $c$ it holds that $c = \mathrm{ev}(f)$ for some $f \in \mathbb{F}_q[U_a]$ satisfying that $(0,0) \in \mathrm{supp}(f)$. We will now use Proposition 3.2. Any number $i$ between 0 and $(q-1)(q-a-1)-1$ can be written uniquely as $i = \beta_i \cdot (q-1) + \alpha_i$ with $\alpha_i$ and $\beta_i$ integers satisfying $0 \leq \alpha_i \leq q-2$ and $0 \leq \beta_i \leq q-a-2$. For $i$ between 0 and $(q-1)(q-a-1)-1$ we then define $v_i = (\alpha_i, \beta_i)$ and $w_i = \overline{-v_i}$. By construction of $w_i$ it then holds that $\overline{v_i + w_i} = (0,0)$. On the other hand, if $j < i$, then $\overline{v_i + w_j} \neq (0,0)$ and $0 \leq \beta_i - \beta_j \leq q-a-2$ implying that $\overline{v_i + w_j} \notin \overline{-U_a}$. By Proposition 3.2, we get that $\mathrm{wt}(c) \geq (q-1)(q-a-1)$. □ □

For $q = 8$ and $a = 4$, the Joyner code case, we obtain that $d \geq 21$. An other method to obtain a lower bound for the minimum distance of toric codes is to use intersection theory. For the Joyner code over $\mathbb{F}_8$ one can prove in this way that $d \geq 12$, [14]. The bound we get compares favorably to it. Another advantage of the order bound techniques is that they are valid for generalized toric codes as well.

Now we obtain a second lower bound on the minimum distance of the code $\mathcal{C}(U_a)$. First we need a lemma.

**Lemma 4.4.** *Let $c$ be a nonzero codeword from the code $\mathcal{C}(V_a)$ or the code $\mathcal{C}(W_a)$. Then $\mathrm{wt}(c) \geq (q-1)(q-a)$.*

*Proof.* Suppose that $c \in \mathcal{C}(V_a)$ (the case that $c \in \mathcal{C}(W_a)$ can be dealt with similarly by symmetry and will not be discussed below). If $c \in \mathcal{C}(T_a)$, we are done. Therefore we can suppose that $c \in \mathcal{C}(V_a)\backslash\mathcal{C}(T_a)$. Exactly as in the proof of Proposition 4.3 we now define for $i$ between 0 and $(q-1)(q-a)-1$ the tuple $u_i = (\alpha_i, \beta_i)$. The only difference is that now $\beta_i$ is also allowed to be $q-a$, otherwise everything is the same. Further we also define $w_i = \overline{-v_i}$. Then we have that $\overline{v_i + w_i} = (0,0)$ and for $j < i$, we obtain that $\overline{v_i + w_j} \neq (0,0)$ and $0 \leq \beta_i - \beta_j \leq q-a-1$. This implies that $\overline{v_i + w_j} \notin \overline{-V_a}$. The lemma now follows. □ □

One can use Lemma 4.4 and the fact that $d(\mathcal{C}(T_a)) = (q-1)(q-a)$ [8], to restrict the number of possibilities for a non-zero codeword of weight less than $(q-1)(q-a)$. Namely, it has to be the evaluation of a function $f = \sum \lambda_u X^u$ with non-zero coefficients $\lambda_{(a,1)}, \lambda_{(0,0)}, \lambda_{(1,a)}$. We will use this in the following proposition. We distinguish cases between $a = 2$ and $a > 2$.

**Proposition 4.5.** *Let $U_a$ be the set from Definition 4.1 and let $a > 2$. The minimum distance $d$ of the code $\mathcal{C}(U_a)$ satisfies*

$$d \geq \min\left\{(q-1)(q-a), q^2 - 3q + 2 - \frac{a(a-1)}{2}\lfloor 2\sqrt{q} \rfloor\right\}.$$

*Proof.* Let $c \in \mathcal{C}(U_a)$ be a nonzero codeword and suppose that $c = \mathrm{ev}(f)$. If $\mathrm{supp}(f) \subset T_a$ then we know that $\mathrm{wt}(c) \geq (q-1)(q-a)$ from [8] as noted before. If $\mathrm{supp}(f) \subset V_a$ or $\mathrm{supp}(f) \subset W_a$ then $\mathrm{wt}(c) \geq (q-1)(q-a)$ by Lemma 4.4.

We are left with the case that $\{(0,0), (1,a), (a,1)\} \subset \mathrm{supp}(f)$. In this case the Newton-polygon of the polynomial $f$ is Minkowski-indecomposable which implies that the polynomial $f$ is absolutely irreducible. We can therefore consider the algebraic curve $C_f$ defined by the equation $f = 0$. From Newton-polygon theory it follows that this curve has geometric genus at most $a(a-1)/2$

and that the edges from $(0,0)$ to $(1,a)$ and from $(0,0)$ to $(a,1)$ correspond to two rational points at infinity using projective coordinates (see [2, Remark 3.18 and Theorem 4.2]). We denote by $N$ the total number of pairs $(\alpha,\beta) \in \mathbb{F}_q^2$ such that $f(\alpha,\beta) = 0$. We claim that $N \leq q - 1 + a(a-1)/2\lfloor\sqrt{q}\rfloor$. If the curve $C$ has no singularities, all solutions $(\alpha,\beta)$ correspond one-to-one to all affine $\mathbb{F}_q$-rational points. Taking into account that there at least 2 rational points at infinity (in fact at least 3 if $a = 2$), the claim follows from Serre's bound (and can be slightly improved if $a = 2$). If there are singularities, a solution $(\alpha,\beta)$ may not correspond to a rational point on $C$, but for every such solution the genus will drop at least one, so the claim still follows from Serre's bound. The proposition now follows, since $\mathrm{wt}(c) \geq (q-1)^2 - N$. □ □

For $a = 2$ we can determine the exact minimum distance. We will do so in the following theorem. This theorem is formulated using the existence or non-existence of an elliptic curve with a certain number of points. The theorem is completely constructive, since it is very easy to determine if an elliptic curve defined over $\mathbb{F}_q$ with a certain number of points exists. To this end one can use the following fact [20, Theorem 4.1]:
Let $q$ be a power of a prime $p$ and let $t$ be an integer. There exists an elliptic curve defined over $\mathbb{F}_q$ with $q + 1 + t$ points if and only if the following holds:

1. $p \not| t$ and $t^2 \leq 4q$,
2. $e$ is odd and one of the following holds
   (a) $t = 0$,
   (b) $t^2 = 2q$ and $p = 2$,
   (c) $t^2 = 3q$ and $p = 3$ ,
3. $e$ is even and one of the following holds
   (a) $t^2 = 4q$,
   (b) $t^2 = q$ and $p \not\equiv 1 \bmod 3$,
   (c) $t = 0$ and $p \not\equiv 1 \bmod 4$.

**Theorem 4.6.** *Denote by $d$ the minimum distance of the $\mathbb{F}_q$-linear code $\mathcal{C}(U_2)$. Further let $t$ be the largest integer such that*

*1.* $3 \mid q + 1 + t$,

*2. there exists an elliptic curve defined over $\mathbb{F}_q$ with $q + 1 + t$ points.*

*Then we have:* $d = q^2 - 3q + 3 - t$.

*Proof.* Analogously as in the previous proposition we only have to consider codewords coming from functions $f$ such that $\{(0,0),(1,2),(2,1)\} \subset \mathrm{supp}(f)$. We again consider the curve $C_f$ given by the equation $f = 0$. In this case all three edges of the Newton polygon of $f$ correspond to rational points at infinity.

The polynomial $f$ can be written as $\alpha + \beta X_1X_2 + \gamma X_1X_2^2 + \delta X_1^2X_2$, where $\alpha$, $\gamma$ and $\delta$ are nonzero. We may assume that the curve does not have singularities, since otherwise the geometric genus of $C_f$ is zero, which implies that the equation $f = 0$ has at most $1 + (q+1) - 3 = q - 1$ solutions in $\mathbb{F}_q^2$ (the first term represents the singular point which could have rational coordinates). This would give rise to a codeword of weight at least $(q-1)^2-(q-1)=q^2-3q+2$.

By changing variables to $U=-\gamma X_1X_2/\delta$ and $V=\gamma X_1^2X_2/\delta$ (or equivalently $X_1=-V/U$ and $X_2=\delta U^2/(\gamma V)$) one can show that the curve $C_f$ is also given by the equation $V^2-\beta UV/\delta+\alpha\gamma V/\delta^2=U^3$. Since we have assumed that the curve $C_f$ is nonsingular, it is an elliptic curve and we already found a Weierstrass equation for it. In $(U,V)$ coordinates one sees that $(0,0)$ is a point on the elliptic curve and using the addition formula one checks that this point has order three in the elliptic curve group.

Denote the total number of rational points on $C_f$ by $q+1+t$, then clearly there exists an elliptic curve with $q+1+t$ points. Since the point $(0,0)$ has order three, the total number of rational points has to be a multiple of three and it follows that $3|q+1+t$. Reasoning back we see that the total number of affine solutions to the equation $f=0$ in $\mathbb{F}_q^2$ equals $q+1+t-3=q-2+t$. On the other hand there are no solutions with zero coordinates, so we have that $\mathrm{wt}(\mathrm{ev}(f))=(q-1)^2-(q-2+t)$.

It remains to be shown which values of $t$ are possible when the polynomial $f$ is varied. It is shown in [10, Section 4.2] that any elliptic curve having $(0,0)$ as a point of order three has a Weierstrass equation of the form $V^2+a_1UV+a_3V=U^3$, with $a_3\neq 0$. This implies that $t$ can be any value satisfying the two conditions stated in the formulation of the theorem. Choosing the maximal one among these values gives a codeword of lowest possible nonzero weight. This concludes the proof. □ □

If $a>2$ the situation is more complicated. Given a fixed $a$ the lower bound from Proposition 4.3 is good for relatively small $q$, while the lower bound from Proposition 4.5 becomes better as $q$ becomes larger. A combination of the techniques from Section 3 and this section gives an in general good lower bound for the minimum distance. In some cases we are able to determine the minimum distance and we describe when this happens in the following theorem.

**Theorem 4.7.** *Let $q$ be a prime power and consider a natural number $a$ satisfying $2<a\leq q-2$. Define the set $U_a$ as in Definition 4.1. Then we have the following for the minimum distance $d$ of the $\mathbb{F}_q$-linear code $\mathcal{C}(U_a)$:*

$$d=(q-1)(q-a) \text{ if } 2(a-2)(q-1)\geq(a-1)a\lfloor 2\sqrt{q}\rfloor.$$

*Proof.* If $(q-1)(q-a)\leq q^2-3q+2-a(a-1)\lfloor 2\sqrt{q}\rfloor/2$, then it follows from Lemma 4.2 and Proposition 4.5 that $d=(q-1)(q-a)$. The theorem follows after some manipulation of this inequality. □ □

For small values of $a$ we obtain the following corollary. Note that the results for $a=4$ are the same as in [17].

**Corollary 4.8.** *We have*
$d(\mathcal{C}(U_3))=(q-1)(q-3)$ *if* $q\geq 37$,
$d(\mathcal{C}(U_4))=(q-1)(q-4)$ *if* $q\geq 37$,
$d(\mathcal{C}(U_5))=(q-1)(q-5)$ *if* $q=41$ *or* $q\geq 47$,
$d(\mathcal{C}(U_6))=(q-1)(q-6)$ *if* $q\geq 59$.

As in the case for the Joyner code it seems that the for many small values of $q$ it also holds that $d(\mathcal{C}(U_a))=(q-1)(q-a)$. We know by Corollary 4.8

and some computer calculations that $d(\mathcal{C}(U_3)) = (q-1)(q-3)$ if $q \geq 23$. It is known for the Joyner code that $d(\mathcal{C}(U_4)) = (q-1)(q-4)$ if $q \geq 8$. Finally we conjecture that $d(\mathcal{C}(U_5)) = (q-1)(q-5)$ if $q \geq 9$. It remains future work to prove this conjecture without the aid of a computer and to establish what happens for larger values of $a$.

# References

[1] Beelen, P.: The order bound for general algebraic geometric codes. Finite Fields Appl. **13**(3) (2007), 665–680.

[2] Beelen, P., Pellikaan, R.: The Newton polygon of plane curves with many rational points. Des. Codes Cryptogr. **21**(1-3) (2000), 41–67.

[3] Danilov, V.I.: The geometry of toric varieties. Russian Math. Surverys **33**(2) (1978), 97–154.

[4] Duursma, I.M.: Majority coset decoding. IEEE Trans. Inform. Theory **39**(3) (1993), 1067–1070.

[5] Feng, G.L., Rao, T.R.N.: Improved geometric Goppa codes. I. Basic theory. IEEE Trans. Inform. Theory **41**(6, part 1) (1995), 1678–1693.

[6] Fulton, W.: Introduction to toric varieties. Volume 131 of Annals of Mathematics Studies. Princeton University Press, Princeton, NJ (1993).

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

[8] Hansen, J.P.: Toric varieties Hirzebruch surfaces and error-correcting codes. Appl. Algebra Engrg. Comm. Comput. **13**(4) (2002), 289–300.

[9] Høholdt, T., van Lint, J.H., Pellikaan, R.: Algebraic geometry of codes. In: Handbook of coding theory, Vol. I, II. North-Holland, Amsterdam (1998), 871–961.

[10] Husemöller, D.: Elliptic curves. Second edn. Volume 111 of Graduate Texts in Mathematics. Springer-Verlag, New York (2004).

[11] Joyner, D.: Toric codes over finite fields. Appl. Algebra Engrg. Comm. Comput. **15**(1) (2004), 63–79.

[12] Little, J., Schenck, H.: Toric surface codes and Minkowski sums. SIAM J. Discrete Math. **20**(4) (2006), 999–1014.

[13] Little, J., Schwarz, R.: On toric codes and multivariate Vandermonde matrices. Appl. Algebra Engrg. Comm. Comput. **18**(4) (2007), 349–367.

[14] Martínez-Moro, E., Ruano, D.: Toric codes. In: Advances in Algebraic Geometry Codes. Volume 5 of Series on Coding Theory and Cryptology. World Scientific (2008), 295–322.

[15] Ruano, D.: On the parameters of $r$-dimensional toric codes. Finite Fields Appl. **13**(4) (2007), 962–976.

[16] Ruano, D.: On the structure of generalized toric codes. Journal of Symbolic Computation (2008) In Press, Corrected Proof. DOI: 10.1016/j.jsc.2007.07.018.

[17] Soprunov, I., Soprunova, E.: Toric surface codes and minkowski length of polygons. arXiv:0802.2088v1 [math.AG] (2008).

[18] Serre, J.-P.: Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini. C. R. Acad. Sci. Paris Sér. I Math. **296**(9) (1983), 397–402.

[19] Tsfasman, M.A., Vlăduţ, S.G.: Algebraic-geometric codes. Volume 58 of Mathematics and its Applications (Soviet Series), Dordrecht (1991).

[20] Waterhouse, W.C.: Abelian varieties over finite fields. Ann. Sci. École Norm. Sup. (4) **2** (1969), 521–560.