Available online at www.sciencedirect.com
ScienceDirect
ELSEVIER
Finite Fields and Their Applications 13 (2007) 962–976
FINITE FIELDS AND THEIR APPLICATIONS
http://www.elsevier.com/locate/ffa

On the parameters of r-dimensional toric codes

Diego Ruano [1]

Department of Algebra, Geometry and Topology, Faculty of Sciences, University of Valladolid, E-47005 Valladolid, Spain

Received 7 December 2005; revised 16 November 2006

Available online 1 March 2007

Communicated by Michael Tsfasman

Abstract

From a rational convex polytope of dimension $r \geqslant 2$ J.P. Hansen constructed an error correcting code of length $n = (q-1)^r$ over the finite field $\mathbb{F}_q$. A rational convex polytope is the same datum as a normal toric variety and a Cartier divisor. The code is obtained evaluating rational functions of the toric variety defined by the polytope at the algebraic torus, and it is an evaluation code in the sense of Goppa. We compute the dimension of the code using cohomology. The minimum distance is estimated using intersection theory and mixed volumes, extending the methods of J.P. Hansen for plane polytopes. Finally we give counterexamples to Joyner's conjectures [D. Joyner, Toric codes over finite fields, Appl. Algebra Engrg. Comm. Comput. 15 (2004) 63–79].

Keywords: Toric varieties; Error correcting codes; Intersection theory

1. Introduction

An important family of error correcting codes are the Algebraic-Geometry codes, introduced by Goppa in 1981. These codes became important in 1982, when Tsfasman, Vlăduţ and Zink constructed a sequence of error correcting codes that exceeds the Gilbert–Varshamov bound. This was the first improvement of that bound in thirty years.

The Algebraic-Geometry codes are defined by evaluating rational functions on a smooth projective curve over a finite field $\mathbb{F}_q$. The functions of $\mathcal{L}(D)$ are evaluated in certain rational points

E-mail address: ruano@agt.uva.es.
[1] Partially supported by MEC MTM2004-00958 and FPU-AP2002-0087 and by Junta de CyL VA068/04, Spain.

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2007.02.002

of the curve, where D is a divisor whose support does not contain any of the rational points we evaluate at. Their parameters are estimated easily using the Riemann–Roch theorem because the points can be seen as divisors.

This construction can be extended to define codes using normal varieties of any dimension [15] giving rise to the called evaluation codes. One can evaluate rational functions but the estimation of the parameters is not easy in general, in particular it is difficult to estimate the minimum distance.

The toric geometry studies varieties that contain an algebraic torus as a dense subset and furthermore the torus acts on the variety. The importance of these varieties, called toric varieties, is based on their correspondence with combinatorial objects, this makes the techniques to study the varieties (such as cohomology theory, intersection theory, resolution of singularities, etc.) more precise and the calculus easier.

J.P. Hansen in 1998 (see [7,8]) considered evaluation codes defined over some toric surfaces, in order to use the proper combinatorial techniques of toric surfaces to estimate the parameters of these codes. D. Joyner in 2004 (see [10]) also considered toric codes over toric surfaces and he gave examples with good parameters using a library in Magma to compute them. He also proposed several questions and conjectures. Recently, other works on toric codes have been published [12,13].

This work treats evaluation codes over toric varieties of arbitrary dimension ($r \geqslant 2$) and length $(q-1)^r$ over the finite field of q elements. A rational convex polytope is the same datum as a normal toric variety and a Cartier divisor. For each rational convex polytope we define an evaluation code over its associated toric variety. The dimension of this code is computed using cohomology theory, by the computation of the kernel of the evaluation map. The minimum distance is estimated using intersection theory and mixed volumes. Finally, we give a counterexample to the two conjectures of Joyner [10].

We mainly use the notation of [5] for toric geometry concepts and for all the toric geometry concepts and results we refer to [5,14].

2. Toric geometry

Let N be a lattice ($N \simeq \mathbb{Z}^r$ for some $r \geqslant 1$). Let $M = \mathrm{Hom}(N, \mathbb{Z})$ be the dual lattice of N. One has the dual pairing $\langle\, ,\rangle : M \times N \to \mathbb{Z}$, $(u, v) \mapsto u(v)$, which is $\mathbb{Z}$-bilinear. Let $N_{\mathbb{R}} = N \otimes \mathbb{R}$ and let $M_{\mathbb{R}} = M \otimes \mathbb{R}$, $M_{\mathbb{R}}$ is the dual vector space of $N_{\mathbb{R}}$. One has the dual pairing $\langle\, ,\rangle : M_{\mathbb{R}} \times N_{\mathbb{R}} \to \mathbb{R}$, $(u, v) \mapsto u(v)$, which is $\mathbb{R}$-bilinear.

Let $\mathbb{F}_q$ be the finite field of q elements and $T = (\mathbb{F}_q^*)^r$ the r-dimensional *algebraic torus*. Let σ be a strongly convex rational cone in $N_{\mathbb{R}}$ ($\sigma \cap (-\sigma) = \{0\}$ and σ is generated by vectors in the lattice), for the sake of simplicity we will just use the word *cone* in this work. And let $\sigma^\vee$ be its dual cone $\sigma^\vee = \{u \in M_{\mathbb{R}} \mid \langle u, v\rangle \geqslant 0\ \forall v \in \sigma\}$. A *face* τ of σ is its intersection with any supporting hyperplane.

Let σ be a cone, then $S_\sigma = \sigma^\vee \cap M$ is a finitely generated semigroup by Gordan's lemma. We define its associated $\mathbb{F}_q$-algebra as $\mathbb{F}_q[S_\sigma] = \bigoplus_{u \in S_\sigma} \mathbb{F}_q \chi^u$ ($\chi^u \chi^{u'} = \chi^{u+u'}$, the unit is χ^0) and one can therefore consider $U_\sigma = \mathrm{Spec}(\mathbb{F}_q[S_\sigma])$ which is the *toric affine variety associated to* σ.

One can consider χ^u as Laurent monomial, $\chi^u(t) = t_1^{u_1} \cdots t_r^{u_r} \in \mathbb{F}_q[t_1, \ldots, t_r]_{t_1 \cdots t_r}$, this also gives a function $T \to \mathbb{F}_q^*$. In algebraic groups theory this is called a *character*.

A *fan* $\triangle$ in N is a finite set of cones in $N_{\mathbb{R}}$ such that each face of a cone in $\triangle$ is also a cone in $\triangle$ and the intersection of two cones in $\triangle$ is a face of each one. For a fan $\triangle$ the *toric variety* $X_\triangle$

is constructed taking the disjoint union of the affine toric varieties U_σ for $\sigma \in \triangle$, and gluing the affine varieties of common faces.

A toric variety is a disjoint union of orbits by the action of the torus T. There is a one to one correspondence between $\triangle$ and the orbits. For a cone σ we denote by $V(\sigma)$ the closure of the orbit of σ, and one has that $\dim \sigma + \dim V(\sigma) = r$.

A toric variety defined from a fan $\triangle$ is non-singular if and only if for each $\sigma \in \triangle$, σ is generated by a subset of a basis of N. We say that a fan $\triangle'$ is a *refinement* of $\triangle$ if each cone of $\triangle$ is a union of cones in $\triangle'$. One has a morphism $X(\triangle') \to X(\triangle)$ that is birational and proper. By refining a fan we can resolve the singularities considering a non-singular refined fan, we assume in this work that a fan is always refined and therefore its associated toric variety is non-singular.

A convex rational polytope in $M_{\mathbb{R}}$ is the convex hull of a finite set of points in M, for the sake of simplicity we just say *polytope*. One can represent a polytope as the intersection of half-spaces. For each facet F (face of codimension 1) there exists $v_F \in N$ inward and primitive and an integer a_F such that

$$P = \bigcap_{F \text{ is a facet}} \left\{ u \in M_{\mathbb{R}} \;\middle|\; \langle u, v_F \rangle \geqslant -a_F \right\}.$$

Given a face p of P, let σ_p be the cone generated by v_F for all the facets F containing p. Then

$$\triangle_P = \{\sigma_p \mid p \text{ is a face of } P\}$$

is a fan which is called *fan associated to* P and its associated toric variety is denoted by X_P. We assume that the associated fan is non-singular, in other case we refine the fan and therefore we consider the half-spaces associated to the new borders (see [6, Section 5.4]).

From a polytope one can define the following T-invariant Weil divisor (which is also a Cartier divisor because the variety is non-singular),

$$D_P = \sum_{F \text{ is a facet}} a_F V(\rho_F)$$

and given $u \in P$

$$\operatorname{div}(\chi^u) = \sum_{F \text{ is a facet}} \langle u, v_F \rangle V(\rho_F).$$

We note that two polytopes with the same inward normal vectors define the same toric variety. For example both a square and a rectangle in $\mathbb{Z}^2$ define $\mathbb{P}^1 \times \mathbb{P}^1$ but they define different Cartier divisors.

A complete fan $\triangle$ and a T-invariant Cartier divisor $D = \sum a_\rho V(\rho)$ define a polytope,

$$P_D = \left\{ u \in M_{\mathbb{R}} \;\middle|\; \langle u, v(\rho) \rangle \geqslant -a_\rho \ \forall \rho \text{ border of } \triangle \right\}.$$

A toric variety defined from a fan $\triangle$ is normal and it is projective if and only if $\triangle$ is a fan associated to a polytope in $M_{\mathbb{R}}$.

The following lemma allows us to compute a basis of $\mathcal{O}(D_P)$.

Lemma 2.1. *Let X_P be the toric variety associated to a polytope P. The set $\mathrm{H}^0(X_P, \mathcal{O}(D_P))$ of global sections of $\mathcal{O}(D_P)$ is a finite-dimensional $\mathbb{F}_q$-vector space with $\{\chi^u \mid u \in M \cap P\}$ as a basis.*

3. Toric codes

Let P be a rational polytope of dimension $r \geqslant 2$, X_P its associated refined variety and D_P its associated Cartier divisor on X_P as in the previous section.

For $t \in T = (\mathbb{F}_q^*)^r$, the rational functions of $\mathrm{H}^0(X_P, \mathcal{O}(D_P))$, i.e. rational functions f over X_P such that $\mathrm{div}(f) + D_P \succcurlyeq 0$, can be evaluated at t

$$\begin{aligned} \mathrm{H}^0\big(X_P, \mathcal{O}(D_P)\big) &\to \mathbb{F}_q \\ f &\mapsto f(t) \end{aligned}$$

since f is a linear combination of characters χ^u that can be considered as Laurent monomials (Lemma 2.1). This map is nothing else than the evaluation of a Laurent polynomial whose monomials have exponents in $P \cap M$ at a point with non-zero coordinates.

We define toric codes in the same way as Hansen [7]. Evaluating at the $(q-1)^r$ points of $T = (\mathbb{F}_q^*)^r$ we obtain the *toric code $\mathcal{C}_P$ associated to P*, which is an evaluation code in the sense of Goppa [15]. $\mathcal{C}_P$ is the image of the $\mathbb{F}_q$-linear evaluation map given by

$$\begin{aligned} \mathrm{ev} : \mathrm{H}^0\big(X_P, \mathcal{O}(D_P)\big) &\to (\mathbb{F}_q)^{\#T} \\ f &\mapsto \big(f(t)\big)_{t\in T}. \end{aligned}$$

Since we evaluate in $\#T$ points, $\mathcal{C}_P$ has *length* $n = \#T = (q-1)^r$.

From Lemma 2.1, it follows that $\mathrm{H}^0(X_P, \mathcal{O}(D_P))$ is a finite-dimensional $\mathbb{F}_q$-vector space with basis $\{\chi^u \mid u \in M \cap P\}$, therefore a generator system of the code $\mathcal{C}_P$ is $\{(\chi^u(t))_{t\in T} \mid u \in M \cap P\}$ which is also a basis of the code if and only if the evaluation map ev is injective.

Remark 3.1. D. Joyner in [10] defines a code for a toric variety coming from a complete fan, a Cartier divisor and a 1-cycle, Joyner uses the 1-cycle to evaluate rational functions at its support. Then he considers the special case where the 1-cycle has support T and he calls these codes *standard toric codes*. As we have seen in the previous section a complete fan and a Cartier divisor is the same data as a polytope P. A polytope P determines the fan $\triangle_P$, the toric variety X_P and the Cartier divisor D_P. Therefore the toric codes defined here, which are the same as Hansen's construction [7], are as general as the standard toric codes [10, Definition 4.5] of Joyner.

The following lemma is used in Theorem 3.3 to compute the kernel of the evaluation map and the dimension of the code is given.

Lemma 3.2. *Let P be a polytope such that $P \cap M$ is contained in $H = \{0, \dots, q-2\} \times \cdots \times \{0, \dots, q-2\} \subset M$. Let*

$$f = \sum_{u \in P\cap M} \lambda_u \chi^u, \quad \lambda_u \in \mathbb{F}_q.$$

Then $(f(t))_{t\in T} = (0)_{t\in T}$ ($f \in \ker(\mathrm{ev})$ for some D) if and only if $\lambda_u = 0$, $\forall u \in P \cap M$.

Proof. Let $f=\sum_{u\in P\cap M}\lambda_u\chi^u$, we can write f as

$$f(t_1,\dots,t_r)=\sum_{0\leqslant u_1,\dots,u_r\leqslant q-2}\lambda_{u_1,\dots,u_r}t_1^{u_1}\cdots t_r^{u_r}\in\mathbb{F}_q[t_1,\dots,t_r]$$

with $\lambda_{u_1,\dots,u_r}\in\mathbb{F}_q$. We shall see that $f=0$.

We prove the result by induction on the number of variables. If $r=1$, $f=\sum_{0\leqslant u_1\leqslant q-2}\lambda_{u_1}t_1^{u_1}$ and since f vanishes in all $\mathbb{F}_q^*$, it belongs to the ideal generated by $t_1^{q-1}-1$, therefore $f=0$ (by degree considerations).

Assume that the result holds up to $r-1$ variables. Let $t_1,\dots,t_{r-1}\in\mathbb{F}_q^*$ then

$$f(t_1,\dots,t_{r-1},t_r)=g_{q-2}(t_1,\dots,t_{r-1})t_r^{q-2}+\cdots+g_1(t_1,\dots,t_{r-1})t_r+g_0(t_1,\dots,t_{r-1})$$

with $g_i(t_1,\dots,t_{r-1})\in\mathbb{F}_q[t_1,\dots,t_{r-1}]$.

One has that $f(t_1,\dots,t_{r-1},t_r)\in\mathbb{F}_q[t_r]$ vanishes for all $t_r\in\mathbb{F}_q^*$. Therefore f belongs to the ideal generated by $t_r^{q-1}-1$, then $f=0$ (by degree considerations). Hence $g_i=0$ for all $i=1,\dots,q-2$ and we can apply the induction hypothesis to g_i and we obtain $f=0$. □

The following theorem allows us to compute the kernel of the evaluation map and a basis of the code (and therefore its dimension).

Theorem 3.3. *Let P be a polytope and $\mathcal{C}_P$ be its associated toric code. For all $u\in P\cap M$ we write $u=c_u+b_u$ where $c_u\in H=\{0,\dots,q-2\}\times\cdots\times\{0,\dots,q-2\}\subset M$, and $b_u\in((q-1)\mathbb{Z})^r$. Let $\overline{P}$ be the set, $\overline{P}=\{c_u\mid u\in P\}\subset M$.*

One has that:

(1) *The kernel of the evaluation map* ev *is the $\mathbb{F}_q$-vector space generated by*

$$\{\chi^u-\chi^{u'}\mid u,u'\in P\cap M,\ c_u=c_{u'}\}.$$

(2) *A basis of the code $\mathcal{C}_P$ is*

$$\{(\chi^{c_u}(t))_{t\in T}\mid u\in P\cap M\}=\{(\chi^u(t))_{t\in T}\mid u\in\overline{P}\}$$

and therefore the dimension *of $\mathcal{C}_P$*

$$k=\#\{c_u\mid u\in P\cap M\}=\#\overline{P}.$$

Proof. (1) Let $u,u'\in P\cap M$ such that $c_u=c_{u'}$. Then $\mathrm{ev}(\chi^u)=\mathrm{ev}(\chi^{u'})$ and one has that $\mathrm{ev}(\chi^u-\chi^{u'})\in\ker(\mathrm{ev})$.

On the other hand, let $f\in\mathrm{H}^0(X_P,\mathcal{O}(D_P))$, with $\mathrm{ev}(f)=0$,

$$f=\sum_{u\in P\cap M}\lambda_u\chi^u=\sum_{u\in P\cap M}\lambda_u(\chi^u-\chi^{c_u})+\sum_{u\in P\cap M}\lambda_u\chi^{c_u}.$$

One has for all $t \in T$

$$\underbrace{f(t)}_{=0} = \underbrace{\sum_{u \in P \cap M} \lambda_u \big(\chi^u(t) - \chi^{c_u}(t)\big)}_{=0} + \sum_{u \in P \cap M} \lambda_u \chi^{c_u}(t).$$

Then $\sum_{u \in P \cap M} \lambda_u \chi^{c_u}(t) = 0$ for all $t \in T$, and by Lemma 3.2 ($c_u \in H$, $\forall u$) one has that $\sum_{u \in P \cap M} \lambda_u \chi^{c_u}$ is the zero function. Then f belongs to the vector space generated by $\{\chi^u - \chi^{u'} \mid u, u' \in P \cap M, c_u = c_{u'}\}$.

(2) Let $f \in \mathrm{H}^0(X_P, \mathcal{O}(D_P))$, and let $t \in T$,

$$f(t) = \sum_{u \in P \cap M} \lambda_u \chi^u(t) = \sum_{u \in P \cap M} \lambda_u \chi^{c_u + b_u}(t) = \sum_{u \in P \cap M} \lambda_u \chi^{c_u}(t).$$

Therefore $(f(t))_{t \in T} \in \{(\chi^{c_u}(t))_{t \in T} \mid u \in P \cap M\}$.

And moreover, $\{(\chi^{c_u}(t))_{t \in T} \mid u \in P \cap M\}$ is a linearly independent set by Lemma 3.2 ($c_u \in H, \forall u$). $\square$

Two polytopes P, P' such that $\overline{P} = \overline{P'}$ have the same associated toric code ($\mathcal{C}_P = \mathcal{C}_{P'}$). Computing χ^{c_u} is the same as computing the class of χ^u in $\mathbb{F}_q[X_1, \ldots, X_r]/J$, where $J = (X_1^{q-1} - 1, \ldots, X_r^{q-1} - 1)$. In [3] it is proven that a toric code of dimension 2 is multicyclic, considering the class of χ^u in $\mathbb{F}_q[X_1, \ldots, X_r]/J$ one can see that $\mathcal{C}_P$ is multicyclic for arbitrary dimension.

We say that a polytope P verifies the *injectivity restriction* if for all $u, u' \in P \cap M, u \neq u'$ one has that $c_u \neq c_{u'}$. Using the above theorem, P verifies the injectivity restriction if and only if the evaluation map ev is injective and $\mathcal{C}_P$ has therefore dimension $k = \#(P \cap M)$, which is the number of rational points in the polytope. In [7,8] Hansen restricts the size of the polytopes in order to make the evaluation map injective, by considering the minimal distance bound. The dimension of the code is therefore the number of rational points of the polytope.

A discussion of recent algorithms to compute the number of lattice points in a polytope may be found in [2]. For $r = 2$ one has Pick's formula [5] to compute the number of lattice points:

Lemma 3.4. *Let P be a plane polytope. Then*

$$\#(P \cap M) = \mathrm{vol}_2(P) + \frac{\mathrm{perimeter}(P)}{2} + 1,$$

where vol_2 *is the Lebesgue volume.*

4. Estimates for the minimum distance

Finally in order to compute the parameters of this family of codes we compute the minimum distance. We use the same techniques as [7] for dimension 2, and compute the intersection numbers using mixed volumes. We also extend this computations to arbitrary dimension. In order to compute the *minimum distance d* of the linear code $\mathcal{C}_P$ we should compute the minimum weight of a non-zero word, i.e. the maximum number of zeros of a function f in $\mathrm{H}^0(X_P, \mathcal{O}(D_P)) \setminus \{0\}$ in T. We solve this problem using intersection theory.

Let $u_1 = (1, 0, \ldots, 0), u_2 = (0, 1, 0, \ldots, 0), \ldots, u_r = (0, \ldots, 0, 1)$. Each $\mathbb{F}_q$-rational point of T is contained in one of the $(q-1)^{r-1}$ lines

$$C_{\eta_1,\ldots,\eta_{r-1}} = \mathrm{V}\big(\big\{\chi^{u_i} - \eta_i\colon\ i = 1, \ldots, r-1\big\}\big), \quad \eta_i \in \mathbb{F}_q^* \ \forall i.$$

Let $f \in \mathrm{H}^0(X_P, \mathcal{O}(D_P)) \setminus \{0\}$. Assume that f is identically zero in a of the lines, and denote by A the set of sub-indexes of the a lines where f vanish.

Following [9, Proposition 3.2], in the other lines the number of zeros is given by the intersection number of a Cartier divisor with a 1-cycle, the integer $D_P \cdot C_{\eta_1,\ldots,\eta_{r-1}}$. Therefore the number of zeros of f in T is bounded by

$$a(q-1) + \sum_{\eta_i \in \mathbb{F}_q^*,\ (\eta_1,\ldots,\eta_{r-1}) \notin A} (D_P \cdot C_{\eta_1,\ldots,\eta_{r-1}}).$$

In order to compute the maximum number of zeros of f one has to compute the intersection number of the Cartier divisor and the 1-cycle and bound the number of lines where f is 0.

Following [4] $D_P \cdot C_{\eta_1,\ldots,\eta_{r-1}} = D_P \cdot C$ for any C defined above. Therefore the number of zeros of f is bounded by

$$a(q-1) + \big((q-1)^{r-1} - a\big)(D_P \cdot C)$$

and the minimum distance is bounded by

$$d(\mathcal{C}_P) \geqslant n - \big(a(q-1) + \big((q-1)^{r-1} - a\big)(D_P \cdot C)\big).$$

One has that

$$D_P \cdot C = D_P \cdot \big(\mathrm{div}\big(\chi^{u_1}\big)\big)_0 \cdots \big(\mathrm{div}\big(\chi^{u_{r-1}}\big)\big)_0$$

and following [5] one see that this intersection number is the mixed volume of the associated polytopes

$$r! V_r(P, P_{(\mathrm{div}(\chi^{u_1}))_0}, \ldots, P_{(\mathrm{div}(\chi^{u_{r-1}}))_0}).$$

The *mixed volume* V_r of r polytopes $P_1, \ldots, P_r$ is

$$V_r(P_1, \ldots, P_r) = \frac{1}{r!} \sum_{j=1}^{r} (-1)^{r-j} \sum_{1 \leqslant i_1 < \cdots < i_j \leqslant r} \mathrm{vol}_r(P_{i_1} + \cdots + P_{i_j}),$$

where vol_r is the Lebesgue volume. An algorithm to compute the Lebesgue volume of a polytope may be found in [1]. Moreover, under certain hypothesis the mixed volume can be computed directly [11].

Let $f \in \mathrm{H}^0(X_P, \mathcal{O}(D_P))$, since $\mathcal{C}_P = \mathcal{C}_{P'}$ if and only if $\overline{P} = \overline{P'}$ we assume without loss of generality that $\deg_{t_i} f \leqslant q-2$. We have

$$f(t_1, \ldots, t_r) = f_0(t_1, \ldots, t_{r-1}) + f_1(t_1, \ldots, t_{r-1})t_r + \cdots + f_{q-2}(t_1, \ldots, t_{r-1})t_r^{q-2}.$$

Let $C_{\eta_1,\dots,\eta_{r-1}}$ be a line where f vanishes, $f(\eta_1,\dots,\eta_{r-1},t_r)\in\mathbb{F}_q[t_r]$ and $\deg f(\eta_1,\dots,\eta_{r-1},t_r)<t_r^{q-1}$ therefore since $f(\eta_1,\dots,\eta_{r-1},t_r)=0\ \forall t_r\in\mathbb{F}_q^*$ it follows $f_i(\eta_1,\dots,\eta_{r-1})=0$ $\forall i$.

The number a is less than or equal to the maximum number of zeros of a non zero function $f\in \mathrm{H}^0(X_{P'},\mathcal{O}(D_{P'}))$ where P' is the r-projection of the polytope P. This can be repeated until we reach dimension 2.

For a *plane polytope* we compute the minimum distance as in [8].

Let us consider P a plane polytope and let us bound the minimum distance. In dimension 2 we can improve the previous computation. Let $f\in \mathrm{H}^0(X_P,\mathcal{O}(D_P))\setminus\{0\}$, and let us assume that f is identically 0 in a lines. Therefore following [9, Proposition 3.2] in the other $(q-1-a)$ lines the maximum number of zeros is $D_P\cdot \operatorname{div}(\chi^{u_1})$.

In dimension 2 a 1-cycle is a Weil divisor and since f vanish in a of the previous lines one has that

$$\operatorname{div}(f)+D_P-a\big(\operatorname{div}\big(\chi^{u_1}\big)\big)_0\succcurlyeq 0.$$

Or equivalently, $f\in \mathrm{H}^0(X_P,\mathcal{O}(D_P-a(\operatorname{div}(\chi^{u_1}))_0))$, and the maximum number of zeros of f in the other $(q-1-a)$ lines is $D_P-a(\operatorname{div}(\chi^{u_1}))_0\cdot(\operatorname{div}(\chi^{u_1}))_0$, which is smaller than or equal to the previous one. This will probably allow us to give a sharper bound.

From Lemma 2.1 one has that

$$a\leqslant \max\big\{u_2-u_2' \bigm| u_1=u_1',\ (u_1,u_2)\in P,\ (u_1',u_2')\in P\big\}.$$

Finally we compute the intersection number of the two Cartier divisors just in the same way as for $r>2$, using the mixed volume of the associated polytopes:

$$D_P-a\big(\operatorname{div}\big(\chi^{u_1}\big)\big)_0\cdot\big(\operatorname{div}\big(\chi^{u_1}\big)\big)_0=2V_2(P_{D_P-a(\operatorname{div}(\chi^{u_1}))_0},P_{(\operatorname{div}(\chi^{u_1}))_0}).$$

Remark 4.1. For a polytope P large enough one can obtain a trivial bound for the minimum distance, which is not the case when the injectivity restriction is satisfied. For instance if we consider a rectangle P with a basis of length greater than $q-1$ we obtain a negative bound for the minimum distance. Another possibility may be to apply the above computations to $\overline{P}$ to obtain a non-trivial bound but unfortunately $\overline{P}$ is not in general a convex polytope. This is similar to the situation for an AG-code $L(D,G)$ when $n\leqslant 2g-2\deg(G)$ [15].

The following proposition gives an *upper bound* for the minimum distance and in particular it may be used to check if the previous bound is sharp. This result extends the computations of [8,10].

Proposition 4.2. *Let P be a polytope and C_P its associated linear code. Let $u\in M$ and Q be $\{0,1,\dots,l_1\}\times\cdots\times\{0,1,\dots,l_r\}\subset M$, where $0\leqslant l_i\leqslant q-2$ (some l_i can be equal to zero). If $\overline{u+Q}$ is contained into the set $\overline{P}$ (where $u=c_u+b_u$, $c_u\in H$, $b_u\in((q-1)\mathbb{Z})^r$, $\overline{P}=\{c_u\mid u\in P\cap M\}$ as in Theorem* 3.3) *then*

$$d\leqslant n-\sum_{j=1}^{r}(-1)^{j+1}\sum_{i_1<\cdots<i_j} l_{i_1}\cdots l_{i_j}(q-1)^{r-j}.$$

Proof. Let $a_1^i, a_2^i, \dots, a_{l_i}^i \in \mathbb{F}_q^*$ be pairwise different elements for $i = 1, \dots, r$.

Let $f(t_1, \dots, t_r) = t_1^{u_1} \cdots t_r^{u_r} \prod (t_i - a_1^i) \cdots (t_i - a_{l_i}^i)$. The number of zeros of f in T is equal to $\sum_{j=1}^{r} (-1)^{j+1} \sum_{i_1 < \cdots < i_j} l_{i_1} \cdots l_{i_j} (q-1)^{r-j}$ (by the inclusion–exclusion principle).

Since f is a linear combination of monomials with exponents in $(u + Q) \cap M$ and $\overline{u + Q} \subset \overline{P}$ one has that for each monomial χ^{c_u} in f there exists $b_u \in ((q-1)\mathbb{Z})^r$ such that $\chi^{c_u + b_u} \in \mathrm{H}^0(X_P, \mathcal{O}(D_P))$, and both polynomials take the same values in T. Proceeding in the same way with all the monomials of f one obtains a function f' such that $f'(t) = f(t)$, $\forall t \in T$ and $f' \in \mathrm{H}^0(X_P, \mathcal{O}(D_P))$. Therefore an upper bound for the minimum distance is

$$d \leqslant n - \sum_{j=1}^{r} (-1)^{j+1} \sum_{i_1 < \cdots < i_j} l_{i_1} \cdots l_{i_j} (q-1)^{r-j}. \qquad \square$$

5. Examples

We consider two examples. We first illustrate the computations of the parameters for a sequence of polytopes $(P_r)_{r \geqslant 2}$ with $\dim(P_r) = r$ and where the r-projection of P_r is P_{r-1}. The second example shows that the bound for the minimum distance, using intersection theory, is not equal to the upper bound of Proposition 4.2.

Example 5.1. Let P_2 be the plane polytope of vertices $(0,0)$, $(b_1, 0)$, (b_1, b_2), $(0, b_2)$ with $b_1, b_2 < q - 1$. This is the code of [7, Proposition 3.2].

The fan $\triangle_{P_2}$ associated to P_2 is generated by cones with edges generated by $v(\rho_1) = (1,0)$, $v(\rho_2) = (0,1)$, $v(\rho_3) = (-1, 0)$ and $v(\rho_4) = (0, -1)$. The toric variety X_{P_2} is non-singular.

$$P_2 = \bigcap_{i=1}^{4} \bigl\{ \langle u, \rho_i \rangle \geqslant -a_i \bigr\},$$

where $a_1 = 0$, $a_2 = 0$, $a_3 = b_1$, $a_4 = b_2$. Therefore $D_P = \sum a_i V(\rho_i) = b_1 V(\rho_3) + b_2 V(\rho_4)$.

Since P_2 is a plane polytope the code $\mathcal{C}_{P_2}$ has length $n = (q-1)^2$. The evaluation map ev is injective since $b_1, b_2 < q - 1$ and P_2 verifies the injectivity restriction 3.3. Therefore one has that the dimension of $\mathcal{C}_{P_2}$ is

$$k = \dim \mathrm{H}^0\bigl(X_{P_2}, \mathcal{O}(D_{P_2})\bigr) = \# P_2 \cap M = (b_1 + 1)(b_2 + 1).$$

From Section 4 we get that the maximum number of zeros of a function f in $\mathrm{H}^0(X_{P_2}, \mathcal{O}(D_{P_2}))$ is smaller than or equal to

$$a(q-1) + (q-1-a)\bigl(D_{P_2} - a\bigl(\operatorname{div}\bigl(\chi^{u_1}\bigr)\bigr)_0 \cdot \bigl(\operatorname{div}\bigl(\chi^{u_1}\bigr)\bigr)_0\bigr),$$

where $a \leqslant b_1$.

One has that $\operatorname{div}(\chi^{u_1}) = \sum \langle u_1, v(\rho_i) \rangle V(\rho_i) = V(\rho_1) - V(\rho_3)$. Therefore $(\operatorname{div}(\chi^{u_1}))_0 = V(\rho_1)$.

$$\begin{aligned} &D_{P_2} - a\bigl(\operatorname{div}\bigl(\chi^{u_1}\bigr)\bigr)_0 \cdot \bigl(\operatorname{div}\bigl(\chi^{u_1}\bigr)\bigr)_0 \\ &\quad = 2V_2\bigl(P_{D_{P_2} - a(\operatorname{div}(\chi^{u_1}))_0}, P_{(\operatorname{div}(\chi^{u_1}))_0}\bigr) \end{aligned}$$

$$= \mathrm{vol}_2(P_{D_{P_2}-a(\mathrm{div}(\chi^{u_1}))_0} + P_{(\mathrm{div}(\chi^{u_1}))_0}) - \mathrm{vol}_2(P_{D_{P_2}-a(\mathrm{div}(\chi^{u_1}))_0}) - \mathrm{vol}_2(P_{(\mathrm{div}(\chi^{u_1}))_0})$$
$$= \big((b_1 - a + 1)b_2\big) - \big((b_1 - a)b_2\big) - (0) = b_2$$

because of

- $P_{D_{P_2}-a(\mathrm{div}(\chi^{u_1}))_0} + P_{(\mathrm{div}(\chi^{u_1}))_0}$ is the polytope of vertices $(a-1,0)$, $(b_1,0)$, (b_1,b_2) and $(a-1,b_2)$;
- $P_{D_{P_2}-a(\mathrm{div}(\chi^{u_1}))_0}$ is the polytope of vertices $(a,0)$, $(b_1,0)$, (b_1,b_2) and (a,b_2);
- $P_{(\mathrm{div}(\chi^{u_1}))_0}$ is the polytope of vertices $(-1,0)$ and $(0,0)$.

Therefore the minimum distance is bounded by

$$d \geqslant (q-1)^2 - \big(b_1(q-1-b_2) + (q-1)b_2\big) = (q-1-b_1)(q-1-b_2).$$

We then apply Proposition 4.2, with $u = 0$ and $l_1 = b_1$, $l_2 = b_2$; $u + Q \subset P_2$, then indeed $u + Q = P_2$, and we obtain

$$d \leqslant (q-1)^2 - b_1(q-1) - b_2(q-1) + b_1 b_2 = (q-1-b_1)(q-1-b_2).$$

And therefore $d = (q-1-b_1)(q-1-b_2)$.

Let P_3 be the 3-dimensional polytope of vertices $(0,0,0)$, $(b_1,0,0)$, $(b_1,b_2,0)$, $(0,b_2,0)$, $(0,0,b_3)$, $(b_1,0,b_3)$, (b_1,b_2,b_3), $(0,b_2,b_3)$ with $b_1,b_2,b_3 < q-1$.

The fan $\triangle_{P_3}$ associated to P_3 is generated by cones with edges generated by $v(\rho_1) = (1,0,0)$, $v(\rho_2) = (-1,0,0)$, $v(\rho_3) = (0,1,0)$, $v(\rho_4) = (0,-1,0)$, $v(\rho_5) = (0,0,1)$, $v(\rho_6) = (0,0,-1)$. The toric variety X_{P_3} is non-singular.

$$P_3 = \bigcap_{i=1}^{6} \big\{ \langle u, \rho_i \rangle \geqslant -a_i \big\},$$

where $a_1 = 0$, $a_2 = b_1$, $a_3 = 0$, $a_4 = b_2$, $a_5 = 0$, $a_6 = b_3$. Therefore $D_P = \sum a_i V(\rho_i) = b_1 V(\rho_2) + b_2 V(\rho_4) + b_3 V(\rho_6)$.

Since P_3 is a 3-dimensional polytope the code $\mathcal{C}_{P_3}$ has length $n = (q-1)^3$. The evaluation map ev is injective since $b_1, b_2, b_3 < q-1$ and P_3 verifies the injectivity restriction 3.3. Therefore one has that the dimension of $\mathcal{C}_{P_3}$ is

$$k = \dim \mathrm{H}^0\big(X_{P_3}, \mathcal{O}(D_{P_3})\big) = \# P_3 \cap M = (b_1+1)(b_2+1)(b_3+1).$$

From Section 4 the maximum number of zeros of a function $f \in \mathrm{H}^0(X_{P_3}, \mathcal{O}(D_{P_3}))$ is smaller than or equal to

$$a(q-1) + \big((q-1)^2 - a\big)(D_{P_3} \cdot C),$$

where $C = \mathrm{V}(\{\chi^{u_1}, \chi^{u_2}\})$ and a is smaller than or equal to the maximum number of zeros of a function defined by the 3-projection of P_3, i.e. P_2. Therefore $a \leqslant b_1(q-1-b_2) + (q-1)b_2$.

One has that $\mathrm{div}(\chi^{u_1}) = \sum \langle u_1, v(\rho_i)\rangle V(\rho_i) = V(\rho_1) - V(\rho_2)$. Therefore $(\mathrm{div}(\chi^{u_1}))_0 = V(\rho_1)$, $\mathrm{div}(\chi^{u_2}) = \sum \langle u_1, v(\rho_i)\rangle V(\rho_i) = V(\rho_3) - V(\rho_4)$. Hence $(\mathrm{div}(\chi^{u_2}))_0 = V(\rho_3)$.

$$\begin{aligned}
D_{P_3}\cdot C &= D_{P_3}\cdot \bigl(\operatorname{div}\bigl(\chi^{u_1}\bigr)\bigr)_0\cdot \bigl(\operatorname{div}\bigl(\chi^{u_2}\bigr)\bigr)_0\\
&= 3!V_3(P, P_{(\operatorname{div}(\chi^{u_1}))_0}, P_{(\operatorname{div}(\chi^{u_2}))_0})\\
&= \operatorname{vol}_3(P_3 + P_{(\operatorname{div}(\chi^{u_1}))_0} + P_{(\operatorname{div}(\chi^{u_2}))_0}) - \operatorname{vol}_3(P_3 + P_{(\operatorname{div}(\chi^{u_1}))_0})\\
&\quad - \operatorname{vol}_3(P_3 + P_{(\operatorname{div}(\chi^{u_2}))_0}) - \operatorname{vol}_3(P_{(\operatorname{div}(\chi^{u_1}))_0} + P_{(\operatorname{div}(\chi^{u_2}))_0}) + \operatorname{vol}_3(P_3)\\
&\quad + \operatorname{vol}_3(P_{(\operatorname{div}(\chi^{u_1}))_0}) + \operatorname{vol}_3(P_{(\operatorname{div}(\chi^{u_2}))_0})\\
&= \bigl((b_1+1)(b_2+1)(b_3)\bigr) - \bigl((b_1+1)b_2b_3\bigr) - \bigl(b_1(b_2+1)b_3\bigr)\\
&\quad - (0) + (b_1b_2b_3) + (0) + (0) = b_3
\end{aligned}$$

because of

- $P_3 + P_{(\operatorname{div}(\chi^{u_1}))_0} + P_{(\operatorname{div}(\chi^{u_2}))_0}$ is the polytope of vertices $(-1,-1,0)$, $(b_1,-1,0)$, $(b_1,b_2,0)$, $(-1,b_2,0)$, $(-1,-1,b_3)$, $(b_1,-1,b_3)$, (b_1,b_2,b_3) and $(-1,b_2,b_3)$;
- $P_3 + P_{(\operatorname{div}(\chi^{u_1}))_0}$ is the polytope of vertices $(-1,0,0)$, $(b_1,0,0)$, $(b_1,b_2,0)$, $(-1,b_2,0)$, $(-1,0,b_3)$, $(b_1,0,b_3)$, (b_1,b_2,b_3) and $(-1,b_2,b_3)$;
- $P_3 + P_{(\operatorname{div}(\chi^{u_2}))_0}$ is the polytope of vertices $(0,-1,0)$, $(b_1,-1,0)$, $(b_1,b_2,0)$, $(0,b_2,0)$, $(0,-1,b_3)$, $(b_1,-1,b_3)$, (b_1,b_2,b_3) and $(0,b_2,b_3)$;
- $P_{(\operatorname{div}(\chi^{u_1}))_0} + P_{(\operatorname{div}(\chi^{u_2}))_0}$ is the polytope of vertices $(0,0,0)$, $(-1,0,0)$, $(-1,-1,0)$ and $(0,-1,0)$;
- P_3 is the polytope of vertices $(0,0,0)$, $(b_1,0,0)$, $(b_1,b_2,0)$, $(0,b_2,0)$, $(0,0,b_3)$, $(b_1,0,b_3)$, (b_1,b_2,b_3) and $(0,b_2,b_3)$;
- $P_{(\operatorname{div}(\chi^{u_1}))_0}$ is the polytope of vertices $(-1,0,0)$ and $(0,0,0)$;
- $P_{(\operatorname{div}(\chi^{u_2}))_0}$ is the polytope of vertices $(0,-1,0)$ and $(0,0,0)$.

Therefore the minimum distance is bounded by

$$\begin{aligned}
d &\geqslant n - \bigl(\bigl(b_1(q-1-b_2) + (q-1)b_2\bigr)(q-1-b_3) + (q-1)^2 b_3\bigr)\\
&= (q-1-b_1)(q-1-b_2)(q-1-b_3).
\end{aligned}$$

We then apply Proposition 4.2, with $u = 0$ and $l_1 = b_1$, $l_2 = b_2$, $l_3 = b_3$; $u + Q \subset P_3$, then indeed $u + Q = P_3$, and we obtain

$$d \leqslant (q-1-b_1)(q-1-b_2)(q-1-b_3).$$

And therefore $d = (q-1-b_1)(q-1-b_2)(q-1-b_3)$.

Computing the lower and upper bound of the minimum distance for an hypercube P_r of dimension r with sides $b_1,\dots,b_r < q-1$ one obtains that for all $r \geqslant 2$ the minimum distance d_r of $\mathcal{C}_{P_r}$ is equal to

$$\begin{gathered}
d_2 = (q-1-b_1)(q-1-b_2),\\
d_r = (q-1)^r - \bigl((q-1)^{r-1} - d_{r-1}\bigr)(q-1-b_r) - b_r(q-1)^{r-1}, \quad \forall r \geqslant 3.
\end{gathered}$$

One can easily see (by induction on r) that it is equal to

$$d_r = (q-1-b_1)\cdots(q-1-b_r).$$

Therefore, the code $\mathcal{C}_{P_r}$ associated to the hypercube of sides $b_1, \ldots, b_r$ has parameters $[(q-1)^r, \prod(b_i+1), \prod(q-1-b_i)]$. In Ref. [13] this example is also considered, but the distance there is computed using Vandermonde determinants.

In Hansen's examples [8] for plane polytopes and also in the previous example the lower bound of the minimum distance, using intersection theory, is equal to the upper bound of the Proposition 4.2. One could think that the previous bound is always sharp. The following example shows this is not true.

Example 5.2. Let P be the plane polytope of vertices $(0,0)$, $(b,0)$, $(2b,b)$, $(2b,2b)$, $(b,2b)$, $(0,b)$ with $b < q-1$.

The fan $\triangle_P$ associated to P is generated by cones with edges generated by $v(\rho_1)=(1,0)$, $v(\rho_2)=(0,1)$, $v(\rho_3)=(-1,1)$, $v(\rho_4)=(-1,0)$, $v(\rho_5)=(0,-1)$, $v(\rho_6)=(1,-1)$. The toric variety X_P is non-singular.

$$P = \bigcap_{i=1}^{6} \bigl\{ \bigl\langle u, v(\rho_i) \bigr\rangle \geqslant -a_i \bigr\},$$

where $a_1=0$, $a_2=0$, $a_3=b$, $a_4=2b$, $a_5=2b$, $a_6=b$. Therefore $D_P = \sum a_i V(\rho_i) = bV(\rho_3) + 2bV(\rho_4) + 2bV(\rho_5) + V(\rho_6)$.

Since P is a plane polytope the code $\mathcal{C}_P$ has length $n=(q-1)^2$. The evaluation map ev is injective since $b < q-1$ and P verifies the injectivity restriction. Therefore one has that the dimension of $\mathcal{C}_P$ is

$$k = \dim \mathrm{H}^0\bigl(X_P, \mathcal{O}(D_P)\bigr) = \mathrm{vol}_2(P) + \frac{\mathrm{Perimeter}(P)}{2} + 1 = 3b^2 + 3b + 1.$$

From Section 4 the maximum number of zeros of a function $f \in \mathrm{H}^0(X_P, \mathcal{O}(D_P))$ is smaller than or equal to

$$a(q-1) + (q-1-a)\bigl(D_P - a\bigl(\mathrm{div}\bigl(\chi^{u_1}\bigr)\bigr)_0 \cdot \bigl(\mathrm{div}\bigl(\chi^{u_1}\bigr)\bigr)_0\bigr),$$

where $a \leqslant 2b$.

One has that $\mathrm{div}(\chi^{u_1}) = \sum \langle u_1, v(\rho_i)\rangle V(\rho_i) = V(\rho_1) - V(\rho_3) - V(\rho_4) + V(\rho_6)$. Therefore $(\mathrm{div}(\chi^{u_1}))_0 = V(\rho_1) + V(\rho_6)$.

$$\begin{aligned}
&D_P - a\bigl(\mathrm{div}\bigl(\chi^{u_1}\bigr)\bigr)_0 \cdot \bigl(\mathrm{div}\bigl(\chi^{u_1}\bigr)\bigr)_0 \\
&\quad = 2V_2(P_{D_P - a(\mathrm{div}(\chi^{u_1}))_0}, P_{(\mathrm{div}(\chi^{u_1}))_0}) \\
&\quad = \mathrm{vol}_2(P_{D_P - a(\mathrm{div}(\chi^{u_1}))_0} + P_{(\mathrm{div}(\chi^{u_1}))_0}) - \mathrm{vol}_2(P_{D_P - a(\mathrm{div}(\chi^{u_1}))_0}) - \mathrm{vol}_2(P_{(\mathrm{div}(\chi^{u_1}))_0}) \\
&\quad = \bigl(3b^2 - 2ab + 2b\bigr) - \bigl(3b^2 - 2ab\bigr) - (0) \\
&\quad = 2b
\end{aligned}$$

because of

- $P_{D_P - a(\mathrm{div}(\chi^{u_1}))_0} + P_{(\mathrm{div}(\chi^{u_1}))_0}$ is the polytope of vertices $(a-1,0)$, $(b,0)$, $(2b,b)$, $(2b,2b)$, $(b+a-1,2b)$ and $(a-1,b-a)$;
- $P_{D_P - a(\mathrm{div}(\chi^{u_1}))_0}$ is the polytope of vertices $(a,0)$, $(b,0)$, $(2b,b)$, $(2b,2b)$, $(b+a,2b)$ and $(a,b-a)$;
- $P_{(\mathrm{div}(\chi^{u_1}))_0}$ is the polytope of vertices $(-1,0)$ and $(0,0)$.

Therefore the minimum distance is bounded by

$$d \geqslant n - \bigl(2b(q-1-2b) + (q-1)2b\bigr) = (q-1)^2 - 4b(q-1) + 4b^2.$$

As we claimed before in this example the lower bound is different from the upper bounds. One can apply Proposition 4.2 by considering a segment of length at most $2b$ and a square of side at most b inside P.

Let $u = (0,b)$ and $Q = \{0,1,\dots,2b\} \times \{0\}$, $u + Q \subset P$. Therefore $d \leqslant (q-1)^2 - 2b(q-1)$.

Let $u = (0,0)$ and $Q = \{0,1,\dots,b\} \times \{0,1,\dots,b\}$, $u + Q \subset P$. Therefore $d \leqslant (q-1)^2 - (2b(q-1) - b^2)$.

Then $(q-1)^2 - 4b(q-1) + 4b^2 < (q-1)^2 - 2b(q-1) < (q-1)^2 - (2b(q-1) - b^2)$.

6. Joyner's questions and conjectures

Question 3.4 of [10] asks "*Under what conditions* (*if any*) *is the map* ev *an injection*?". Our Theorem 3.3 answers completely this question for standard toric codes.

We shall prove that Conjectures 4.2 and 4.3 of [10] are not true. As a counterexample we consider a code from [8, Theorem 1.2] and a code from [8, Theorem 1.3], respectively.

Conjecture 6.1. *(See [10, Conjecture 4.2].) Let* $\mathcal{C}(E, D, X)$ [10, *Section* 3.1, *definition* (5)] *be the toric code associated to the* 1*-cycle* E*, the* T*-invariant Cartier divisor* D *and the toric variety* X*. Let*

- *X be a non-singular toric variety of dimension r,*
- *n be so large that there is an integer $N > 1$ such that $2N\mathrm{vol}_r(P_D) \leqslant n \leqslant 2N^2\mathrm{vol}_r(P_D)$.*

If q is "sufficiently large" then any $f \in \mathrm{H}^0(X, \mathcal{O}(D))$ has no more than n zeros in the rational points of X. Consequently,

$$d \geqslant n - 2N\mathrm{vol}_r(P_D).$$

Here "sufficiently large" may depend on X, C and D but not on f.

Counterexample 6.2. We give a counterexample to the previous conjecture. Let $\mathcal{C}_P$ be the code associated to the plane polytope P of vertices $(0,0)$, $(1,1)$, $(0,2)$. Following [8] $\mathcal{C}_P$ has the length $n = (q-1)^2$ and the minimum distance equal to $d = (q-1)^2 - 2(q-1)$. The non-singular toric variety X is $X_\triangle$, where $\triangle$ is the fan generated by cones with edges generated by $v(\rho_1) = (1,0)$, $v(\rho_2) = (-1,1)$, $v(\rho_3) = (-1,0)$, $v(\rho_4) = (-1,-1)$. E is the formal sum of all the points of T because $\mathcal{C}_P$ is a standard toric code. We consider $D = D_P$, that is the Cartier divisor associated to P, $D = V(\rho_3) + V(\rho_4)$ and that $\mathrm{vol}_r(P_D) = \mathrm{vol}_r(P) = 1$.

From Theorem 3.3 we know that q "sufficiently large" means $q \geqslant 3$. We claim that the conjecture does not hold for $q \geqslant 5$, let q be greater or equal than 5 and $N = q - 2$.

$$2N\mathrm{vol}_r(P_D) \leqslant n \leqslant 2N^2\mathrm{vol}_r(P_D) \quad \Leftrightarrow \quad 2(q-2) \leqslant (q-1)^2 \leqslant 2(q-2)^2$$

that holds for $q \geqslant 5$.

The conjecture claims that the minimum distance satisfies

$$d \geqslant n - 2N\mathrm{vol}_r(P_D) = (q-1)^2 - 2(q-2) > (q-1)^2 - 2(q-1) = d$$

therefore for $q \geqslant 5$ the conjecture gives a lower bound strictly greater than the minimum distance, a contradiction.

Conjecture 6.3. *(See [10, Conjecture 4.3].) Let $\mathcal{C}(E, D, X)$ [10, Section 3.1, definition (5)] be the toric code associated to the 1-cycle E, the T-invariant Cartier divisor D and the toric variety X. Let*

- *X be a non-singular toric variety of dimension r,*
- *$\psi_D(v) = \min_{u \in P_D \cap M} \langle u, v\rangle$ be strictly convex,*
- $\deg(E) > \deg(D^r)$.

If q is "sufficiently large" then any $f \in \mathrm{H}^0(X, \mathcal{O}(D))$ has no more than n zeros in the rational points of X. Consequently,

$$k \geqslant \dim \mathrm{H}^0\bigl(X, \mathcal{O}(D)\bigr) = \#P_D \cap M,$$
$$d \geqslant n - r!(\#P_D \cap M).$$

Moreover, if $n > r!(\#P_D \cap M)$ then $\dim \mathrm{H}^0(X, \mathcal{O}(D)) = \#P_D \cap M$.

Counterexample 6.4. We give a counterexample to the previous conjecture. Let $\mathcal{C}_P$ be the code associated to the plane polytope P of vertices $(0,0)$, $(1,0)$, $(0,1)$. Following [8] $\mathcal{C}_P$ has length $n = (q-1)^2$ and minimum distance equal to $d = (q-1)^2 - (q-1)$. The non-singular toric variety X is $X_\triangle$, where $\triangle$ is the fan generated by cones with edges generated by $v(\rho_1) = (1,0)$, $v(\rho_2) = (0,1)$, $v(\rho_3) = (-1,-1)$, i.e. $X = \mathbb{P}^2$. E is the formal sum of all the points of T because $\mathcal{C}$ is a standard toric code. We consider $D = D_P$, that is the Cartier divisor associated to P, $D = V(\rho_3)$, therefore one has that ψ_D is strictly convex (see [5, p. 70]). One has for $P = P_D$ that $\#P \cap M = 3$ and $(q-1)^2 = \deg(E) > \deg(D) = 1$.

From Theorem 3.3 we know that "sufficiently large" means $q \geqslant 3$. We claim that the conjecture does not hold for $q \geqslant 8$.

Let q be greater or equal than 8. The conjecture claims that the minimum distance satisfies

$$d \geqslant n - r!(\#P_D \cap M) = (q-1)^2 - 2 \cdot 3 > (q-1)^2 - (q-1) = d.$$

Therefore for $q \geqslant 8$ the conjecture gives a lower bound strictly greater than the minimum distance, a contradiction.

Acknowledgments

The author wishes to thank T. Høholdt and F.J. Monserrat for helpful comments on this paper.

References

[1] A.I. Barvinok, Computing the volume, counting integral points, and exponential sums, Discrete Comput. Geom. 10 (1993) 123–141.
[2] J.A. De Loera, The many aspects of counting lattice points in polytopes, Math. Semesterber. 52 (2) (2005) 175–195.
[3] V. Díaz, C. Guevara, M. Vath, Codes from n-dimensional polyhedra and n-dimensional cyclic codes, in: Proceedings of SIMU Summer Institute, 2001.
[4] W. Fulton, Intersection Theory, Ergeb. Math. Grenzgeb., vol. 2, Springer-Verlag, 1984.
[5] W. Fulton, Introduction to Toric Varieties, Ann. of Math. Stud., Princeton Univ. Press, 1993.
[6] I.M. Gelfand, M.M. Kapranov, A.V. Zelevinsky, Discriminants, Resultants and Multidimensional Determinants, Math. Theory Appl., Birkhäuser, 1994.
[7] J.P. Hansen, Toric surfaces and error-correcting codes, in: Coding Theory, Cryptography and Related Areas, Guanajuato, 1998, 2000, pp. 132–142.
[8] J.P. Hansen, Toric varieties Hirzebruch surfaces and error-correcting codes, Appl. Algebra Engrg. Comm. Comput. 13 (2002) 289–300.
[9] S.H. Hansen, Error-correcting codes from higher-dimensional varieties, Finite Fields Appl. 7 (2001) 530–552.
[10] D. Joyner, Toric codes over finite fields, Appl. Algebra Engrg. Comm. Comput. 15 (2004) 63–79.
[11] A.G. Khovanskii, Newton polyhedra, a new formula for mixed volume, product of roots of a system equations, in: Fields Inst. Commun., vol. 24, Amer. Math. Soc., Providence, RI, 1999, pp. 325–364.
[12] J. Little, H. Schenck, Toric surface codes and Minkowski sums, SIAM J. Discrete Math. 20 (4) (2006) 999–1014.
[13] J. Little, R. Schwarz, On m-dimensional toric codes, arXiv: cs.IT/0506102.
[14] T. Oda, Convex Bodies and Algebraic Geometry. An Introduction to the Theory of Toric Varieties, Ergeb. Math. Grenzgeb., vol. 15, Springer-Verlag, 1984.
[15] M.A. Tsfasman, S.G. Vlăduţ, Algebraic Geometry Codes, Math. Appl., vol. 15, Kluwer, Dordrecht, 1991.