3-1-2013

Toric Complete Intersection Codes

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

Toric complete intersection codes

Ivan Soprunov

1. Introduction

This work is inspired by the results of Gold et al. (2005) and Ballico and Fontanari (2006) on evaluation codes on complete intersections in the projective space. Examples of evaluation codes include Reed–Muller codes on points in affine and projective spaces and Goppa codes on points in algebraic curves. Here is a general definition. Let X be an algebraic variety over a finite field $\mathbb{F}_q$ and let $S = \{p_1, \dots, p_N\}$ be a finite set of $\mathbb{F}_q$-rational points of X. Furthermore, let $\mathcal{L}$ be a finite-dimensional space of regular functions over $\mathbb{F}_q$ defined on an open subset of X containing S. This defines an *evaluation map*

$$\mathrm{ev}_S : \mathcal{L} \to (\mathbb{F}_q)^N, \quad f \mapsto \big(f(p_1), \dots, f(p_N)\big).$$

Its image is a linear code $\mathcal{C}_{S,\mathcal{L}}$ of block length N. In the situation when X is a projective toric variety, the set S is the algebraic torus $(\mathbb{F}_q^*)^n$, and $\mathcal{L}$ is the space of linear sections of a Cartier divisor on X we obtain what is called a *toric code*. In this case $\mathcal{L}$ is spanned by monomials whose exponents are lattice points in a convex lattice polytope. The minimum distance for toric codes was studied in

Hansen (2000); Joyner (2004); Little and Schenck (2006); Little and Schwarz (2007); Ruano (2007); Soprunov and Soprunova (2009, 2010).

Duursma et al. (2001) considered the situation when $X = \mathbb{P}^n$, the set S is an arbitrary zero-dimensional complete intersection in $\mathbb{P}^n(\mathbb{F}_q)$, and $\mathcal{L} = \mathcal{L}_a$ is the space of homogeneous polynomials of degree a. Their paper is concerned with computing the dimension of the corresponding evaluation codes $\mathcal{C}_{S,\mathcal{L}_a}$. Later Gold et al. (2005) found a very nice application of the Cayley–Bacharach theorem that gave a lower bound for the minimum distance of $\mathcal{C}_{S,\mathcal{L}_a}$, generalizing the 2-dimensional result of Hansen (2003). They showed that the minimum distance satisfies

$$d(\mathcal{C}_{S,\mathcal{L}_a}) \geqslant s - a + 2,$$

where $s = \sum_{i=1}^{n} d_i - (n+1)$ and $d_1, \ldots, d_n$ are the degrees of the polynomials defining S. Ballico and Fontanari (2006) then gave a significantly better bound

$$d(\mathcal{C}_{S,\mathcal{L}_a}) \geqslant n(s-a) + 2,$$

which holds for complete intersections S satisfying a "generality" condition: no $n+1$ points of S lie on a hyperplane in $\mathbb{P}^n$.

In this paper we combine the two situations: X is a projective toric variety, S is a zero-dimensional complete intersection in X, and $\mathcal{L}$ is a space of global sections of a Cartier divisor on X. The corresponding evaluation code we call a *toric complete intersection code*. We give two lower bounds for the minimum distance of such codes: for sets S with and without a "generality" condition. Our bounds generalize the ones in Gold et al. (2005) and Ballico and Fontanari (2006). Although we largely adopted methods from these papers, the difficulty is that no analog of the Cayley–Bacharach theorem for toric varieties is currently known. It turned out that the Toric Euler–Jacobi theorem (Theorem 2.4) on global residues (which can be thought of as a weak toric analog of the Cayley–Bacharach theorem, see Corollary 2.5) provides enough information for applications to evaluation codes.

In our exposition we decided to use not the language of toric geometry but rather the more explicit language of Laurent polynomial systems and Newton polytopes. The relationship between the two is discussed in Section 2.3. Section 2 gives the necessary preliminaries and states the Toric Euler–Jacobi theorem and its immediate applications. Section 3 contains the main results on the minimum distance of toric complete intersection codes: Theorem 3.5 does not use any additional assumptions, and Theorem 3.9 assumes a certain "generality" property of S. In Section 4 we give geometric conditions on the Newton polytopes of polynomials defining S which guarantee that this property holds when the coefficients of the polynomials are generic. The paper concludes with applications and concrete examples in Section 5 and remarks about further work.

2. Preliminaries

2.1. Evaluation codes

In this section we will define evaluation codes we will be dealing with throughout the paper. First let us introduce some standard definitions and notation from the theory of Newton polytopes. Let $\mathbb{K}$ be a field and $\overline{\mathbb{K}}$ be its algebraic closure. Consider a Laurent polynomial $f \in \mathbb{K}[t_1^{\pm 1}, \ldots, t_n^{\pm 1}]$. Its *Newton polytope* $P(f)$ is the convex hull of the exponent vectors of the monomials appearing in f. Thus we can write

$$f = \sum_{a \in P(f) \cap \mathbb{Z}^n} c_a t^a, \quad \text{where } t^a = t_1^{a_1} \cdots t_n^{a_n},\ c_a \in \mathbb{K}.$$

Given a face Q of $P(f)$ the *restriction* f^Q is the Laurent polynomial

$$f^Q = \sum_{a \in Q \cap \mathbb{Z}^n} c_a t^a.$$

Next we define evaluation codes slightly adapted to our situation (see also Hansen, 2001; Little, 2008; Tsfasman et al., 2007 for various constructions of evaluation codes). Choose a finite subset

$S = \{p_1, \dots, p_N\}$ of $(\mathbb{K}^*)^n$ and a finite-dimensional subspace $\mathcal{L}$ of $\mathbb{K}[t_1^{\pm 1}, \dots, t_n^{\pm 1}]$. Define the *evaluation map*

$$\mathrm{ev}_S : \mathcal{L} \to \mathbb{K}^N, \quad f \mapsto \big(f(p_1), \dots, f(p_N)\big).$$

The image of ev_S is a linear code, called the *evaluation code*, which we denote by $\mathcal{C}_{S,\mathcal{L}}$.

In the paper we will be dealing with evaluation codes $\mathcal{C}_{S,\mathcal{L}}$ where $\mathcal{L}$ is a space of Laurent polynomials and S is a zero-dimensional complete intersection of n hypersurfaces in a toric variety. We postpone the toric geometry definition of S until Section 2.3. Instead, we formulate this in terms of the theory of Newton polytopes. We describe S as the solution set of a Laurent polynomial system satisfying three assumptions below.

Fix a collection of n-dimensional convex lattice polytopes $P_1, \dots, P_n$ in $\mathbb{R}^n$ and let $P = P_1 + \cdots + P_n$ be their Minkowski sum. Consider n Laurent polynomials $f_1, \dots, f_n$ over $\mathbb{K}$ with Newton polytopes $P_1, \dots, P_n$ such that the system $f_1 = \cdots = f_n = 0$ satisfies the following.

Assumptions.

(1) The system is *non-degenerate* with respect to P, i.e. for every proper face $Q \subset P$ the restricted system $f_1^{Q_1} = \cdots = f_n^{Q_n} = 0$ has no solutions in $(\overline{\mathbb{K}}^*)^n$, where $Q = Q_1 + \cdots + Q_n$, for unique faces $Q_i \subset P_i$;
(2) at each $p \in S$ the collection $(f_1, \dots, f_n)$ forms a system of local parameters, i.e. the 1-forms $df_1, \dots, df_n$ are linearly independent at p;
(3) the solution set $S \subset (\overline{\mathbb{K}}^*)^n$ of the system consists of $\mathbb{K}$-rational points.

Before describing the space $\mathcal{L}$ we need to set some notation. For any set $A \subset \mathbb{R}^n$ we use $A_{\mathbb{Z}}$ to denote the set of lattice points in A, i.e. $A_{\mathbb{Z}} = A \cap \mathbb{Z}^n$. Also, we let P° denote the interior of the polytope $P = P_1 + \cdots + P_n$. Now let A be any subset of P°. Define

$$\mathcal{L}(A) = \mathrm{span}_{\mathbb{K}}\big\{t^a \;\big|\; a \in A_{\mathbb{Z}}\big\} \subset \mathbb{K}\big[t_1^{\pm 1}, \dots, t_n^{\pm 1}\big].$$

Definition 2.1. Let S be the solution set of a system $f_1 = \cdots = f_n = 0$ with n-dimensional Newton polytopes $P_1, \dots, P_n$ satisfying (1)–(3) above. Let the set A lie in the interior P° of $P = P_1 + \cdots + P_n$. The evaluation code $\mathcal{C}_{S,\mathcal{L}(A)}$ is called a *toric complete intersection code*. We will denote it simply by $\mathcal{C}_A$. Furthermore, $d(\mathcal{C}_A)$ will denote the minimum distance (the minimum weight) of $\mathcal{C}_A$.

Remark 2.2. Although the above definition makes sense for arbitrary subsets A of P°, we may just as well restrict ourselves to the case of convex polytopes A. Indeed, the construction of the code depend on $A_{\mathbb{Z}}$ rather than on A itself. Moreover, the bounds on the minimum distance of $\mathcal{C}_A$ which we prove in Section 3 will not change if one replaces A with the convex hull of $A_{\mathbb{Z}}$, whereas the dimension of $\mathcal{C}_A$ may, of course, only increase.

2.2. The Toric Euler–Jacobi theorem

Here we discuss the toric analog of the Euler–Jacobi theorem (Theorem 2.4) and its consequences. This theorem was first discovered by Khovanskii (1978) over the field of complex numbers. In Kunz (2008, Sec. 14) the first part of the theorem is proved over an arbitrary algebraically closed field. The second part of the theorem is proved over fields of positive characteristic by Joshua and Akhtar (2011) under the condition that the P_i have the same normal fan, but is currently unknown in general. Nevertheless, the proofs of our main results will only use the first part of Theorem 2.4, so we do not make any additional assumptions on the polytopes (with the exception of Theorem 4.3).

Definition 2.3. Let $f_1, \dots, f_n \in \mathbb{K}[t_1^{\pm 1}, \dots, t_n^{\pm 1}]$ be Laurent polynomials. The Laurent polynomial

$$J_f^{\mathbb{T}} = \det\left(t_j \frac{\partial f_i}{\partial t_j}\right)$$

is called the *toric Jacobian* of $f_1, \dots, f_n$.

It is easy to see that the Newton polytope $P(J_f^{\mathbb{T}})$ of the toric Jacobian lies in $P = P_1 + \cdots + P_n$, where $P_i = P(f_i)$. Also, assumption (3) in Section 2.1 implies $J_f^{\mathbb{T}}(p) \neq 0$ for every $p \in S$.

Theorem 2.4. *(See Khovanskii, 1978.) Let S be the solution set of a system $f_1 = \cdots = f_n = 0$ with n-dimensional Newton polytopes $P_1, \ldots, P_n$ satisfying* (1)–(3) *above. Let $P = P_1 + \cdots + P_n$ be the Minkowski sum. Then*

(1) *for any $h \in \mathcal{L}(P^\circ)$ we have $\sum_{p\in S} h(p)/J_f^{\mathbb{T}}(p) = 0$;*
(2) *for any function $\phi : S \to \mathbb{K}$ with $\sum_{p\in S} \phi(p) = 0$ there exists $h \in \mathcal{L}(P^\circ)$ such that $\phi(p) = h(p)/J_f^{\mathbb{T}}(p)$ for every $p \in S$.*

Here is an immediate corollary from the theorem.

Corollary 2.5. *Any $h \in \mathcal{L}(P^\circ)$ which vanishes at $|S| - 1$ points of S must vanish at all points of S.*

The next result, known as the Bernstein–Kushnirenko theorem, provides the size of the solution set S for systems $f_1 = \cdots = f_n = 0$ with given Newton polytopes $P_1, \ldots, P_n$.

Theorem 2.6. *Let a Laurent polynomial system $f_1 = \cdots = f_n = 0$ with Newton polytopes $P_1, \ldots, P_n$ have isolated solution set S in $(\overline{\mathbb{K}}^*)^n$. Then $|S|$ cannot exceed the normalized mixed volume $V(P_1, \ldots, P_n)$ of the Newton polytopes. Moreover, $|S| = V(P_1, \ldots, P_n)$ if and only if the system satisfies assumptions* (1)–(2)*.*

The original proof by Bernstein (1975) uses the homotopy continuation method and is valid over the field of complex numbers. Kushnirenko (1976) gave an algebraic proof which works over any algebraically closed field regardless of the characteristic. A similar argument also appears in Tuitman (2010, Sec. 6).

Remark 2.7. Suppose we have a system $f_1 = \cdots = f_n = 0$ with Newton polytopes $P_1, \ldots, P_n$. According to Theorem 2.6, if we can exhibit $V(P_1, \ldots, P_n)$-many $\mathbb{K}$-rational solutions to the system and the solutions are isolated then the system must satisfy assumptions (1)–(3). We will use this observation when constructing toric complete intersection codes in Section 5.

Here is our first application to toric complete intersection codes.

Proposition 2.8. *If $|S| > 1$ then the minimum distance of $\mathcal{C}_{P^\circ}$ is at least 2.*

Proof. Any $h \in \mathcal{L}(P^\circ)$ which is not identically zero on S may have at most $|S| - 2$ zeroes by Corollary 2.5. Hence the weight of every non-zero codeword in $\mathcal{C}_{P^\circ}$ is at least 2. To see that such h exists one can show that if $|S| = V(P_1, \ldots, P_n) > 1$ then P° must contain at least one lattice point u, and so $\mathcal{L}(P^\circ)$ contains t^u. In fact, $V(P_1, \ldots, P_n) = 1$ is equivalent to all P_i being equal to a basis simplex Δ, in which case $P = n\Delta$ has no lattice points (Cattani et al., 2011, Prop. 2.7). □

2.3. Relation to toric varieties

Here we will show how our problem can be reformulated in the language of toric geometry. Let $X = X_\Sigma$ be a projective simplicial toric variety over $\mathbb{K}$ of dimension n, defined by a complete rational simplicial fan $\Sigma \subset \mathbb{R}^n$. Each ray $\rho \in \Sigma(1)$ is generated by a primitive lattice vector $v_\rho \in \mathbb{Z}^n$ and corresponds to a torus-invariant prime divisor D_ρ on X. A *semi-ample* divisor D on X is a torus-invariant Cartier divisor $D = \sum_{\rho\in\Sigma(1)} a_\rho D_\rho$ for which the corresponding line bundle $\mathcal{O}(D)$ is generated by global sections. This implies that the set

$$P_D = \left\{ u \in \mathbb{R}^n \;\middle|\; \langle u, v_\rho \rangle \geqslant -a_\rho,\ \rho \in \Sigma(1) \right\}$$

is a lattice polytope in $\mathbb{R}^n$ (Fulton, 1993, Sec. 3.4). Also the space of global $\mathbb{K}$-sections of $\mathcal{O}(D)$ is isomorphic to $\mathcal{L}(P_D)$ in our notation in Section 2.1.

Now fix n semi-ample divisors $D_1, \ldots, D_n$ on X and let $P_i = P_{D_i}$ be the corresponding lattice polytopes. Let $D = D_1 + \cdots + D_n$. For every $1 \leqslant i \leqslant n$ let f_i be a section of the line bundle $\mathcal{O}(D_i)$. The assumption (1) in Section 2.1 guarantees that the hypersurfaces defined by the f_i in X do not have common points on the orbits of X of codimension greater than 1, which implies that the hypersurfaces intersect in isolated points S in the dense orbit. The other two assumptions say that the intersections are transverse and consist of $\mathbb{K}$-rational points.

The following is a higher-dimensional generalization of the Ω-construction of evaluation codes on algebraic curves (Tsfasman et al., 2007, Sec. 4.1.1). Let Ω^n_X be the sheaf of Zariski n-forms on X and $\Omega^n_X(D)$ the sheaf corresponding to the divisor $D = D_1 + \cdots + D_n$. The global sections of this sheaf are n-forms whose only poles are in the support of the D_i. There is an isomorphism $\Omega^n_X(D) \cong \mathcal{O}(D - \sum_\rho D_\rho)$ (Cox et al., 2011, Sec. 8.2). We can write this explicitly in affine coordinates $(t_1, \ldots, t_n)$. A section of $\Omega^n_X(D)$ has the form

$$\omega_h = \frac{h}{f_1 \cdots f_n} \frac{dt_1}{t_1} \wedge \cdots \wedge \frac{dt_n}{t_n},$$

for some Laurent polynomial h which corresponds to a section of $\mathcal{O}(D - \sum_\rho D_\rho)$. Using the above identification, we see that the space of global sections of $\mathcal{O}(D - \sum_\rho D_\rho)$ is spanned by the lattice points of the (rational) polytope corresponding to $D - \sum_\rho D_\rho$, i.e. the interior lattice points of $P_D = P_1 + \cdots + P_n$. Hence, $h \in \mathcal{L}(P^\circ)$.

Now let $S = \{p_1, \ldots, p_N\}$ be the intersection of the hypersurfaces defined by the f_i as above. Then at every $p \in S$ the local (Grothendieck) residue $\operatorname{res}_p(\omega_h)$ is defined (Gelfond and Khovanskii, 2002). Choose a subspace $\mathcal{L}$ of global sections of $\Omega^n_X(D)$. This results in the *residue map*

$$\operatorname{res}_S : \mathcal{L} \to \mathbb{K}^N, \quad \omega_h \mapsto \big(\operatorname{res}_{p_1}(\omega_h), \ldots, \operatorname{res}_{p_N}(\omega_h)\big),$$

whose image is a linear code. In the case of transverse intersections at p we have $\operatorname{res}_p(\omega_h) = h(p)/J^{\mathbb{T}}_f(p)$ and the reside map becomes:

$$\operatorname{res}_S : \mathcal{L} \to \mathbb{K}^N, \quad \omega_h \mapsto \left(\frac{h(p_1)}{J^{\mathbb{T}}_f(p_1)}, \ldots, \frac{h(p_N)}{J^{\mathbb{T}}_f(p_N)}\right).$$

The linear code it defines is equivalent to the toric complete intersection code from Definition 2.1. A similar construction of *toric residue codes* appears in Joshua and Akhtar (2011) in relation to quantum stabilizer codes.

The sum of the local residues over $p \in S$ is the *global residue* $\operatorname{Res}_f(h)$ of h with respect to $f = (f_1, \ldots, f_n)$. In these terms the first statement of Theorem 2.4 says that the global residue of any $h \in \mathcal{L}(P^\circ)$ equals zero. The global residue is closely related to the toric residue (Cox, 1996) and was studied by Cattani et al. (1997); Cattani and Dickenstein (1997); Soprunov (2007).

3. Bounds for the minimum distance

Recall that the evaluation code $\mathcal{C}_A$ is constructed by choosing a subset A of P°. Note that lattice translations of A, i.e. translations by lattice vectors, result in equivalent codes, so the minimum distance $d(\mathcal{C}_A)$ is independent of such translations. Consider a "complementary" set B, for which $A + B \subseteq P^\circ$. It turns out that $d(\mathcal{C}_A)$ is related to properties of the space $\mathcal{L}(B)$ as Theorem 3.2 below shows. The following definition from classical algebraic geometry will be used throughout the paper.

Definition 3.1. We say that a finite set of points $T \subset (\mathbb{K}^*)^n$ *imposes independent conditions* on a space of Laurent polynomials $\mathcal{L}$ if the evaluation map $\operatorname{ev}_T : \mathcal{L} \to \mathbb{K}^{|T|}$ is surjective.

Theorem 3.2. *Let S be the solution set of a system $f_1 = \cdots = f_n = 0$ satisfying assumptions (1)–(3) above. Let A and B be two subsets of $\mathbb{R}^n$ such that $A + B \subseteq P^\circ$. If any $T \subseteq S$ of size m imposes independent conditions on the space $\mathcal{L}(B)$ then $d(\mathcal{C}_A) \geqslant m + 1$.*

Proof. We need to show that any $h \in \mathcal{L}(A)$, not identically zero on S, vanishes at no more than $|S| - m - 1$ points of S. Assume there exist $h \in \mathcal{L}(A)$ and a subset $Z \subset S$ of size $|S| - m$ such that h vanishes on Z, but $h(p) \neq 0$ for some $p \in S$. By our assumption $S \setminus Z$ imposes independent conditions on $\mathcal{L}(B)$, so there exists $g \in \mathcal{L}(B)$ such that g vanishes at every point of $S \setminus (Z \cup \{p\})$, but not at p. Now the polynomial hg belongs to $\mathcal{L}(A + B) \subseteq \mathcal{L}(P^\circ)$ and vanishes at every point of S but not at p, which contradicts Corollary 2.5. □

Remark 3.3. Consider a special case: $X = \mathbb{P}^n$, $f_1, \ldots, f_n$ are homogeneous polynomials of degrees $d_1, \ldots, d_n$; and $\mathcal{L}(A)$ and $\mathcal{L}(B)$ are subspaces of homogeneous polynomials of degrees a and $s - a$, respectively, where $s = \sum_{i=1}^{n} d_i - (n+1)$. In this case Theorem 3.2 follows from the Cayley–Bacharach theorem (Eisenbud et al., 1996) and serves as the main tool in the proofs of the results of Gold et al. (2005) and Ballico and Fontanari (2006). We would like to point out that no toric analog of the Cayley–Bacharach theorem is currently known, however, the Toric Euler–Jacobi theorem is sufficient for our application to toric complete intersection codes.

Our next goal is to understand what sets B satisfy the condition of the above theorem for some value of m. Here is our first example.

Lemma 3.4. *Let $B = B_1 + \cdots + B_m$ where the lattice set $B_i \cap \mathbb{Z}^n$ affinely generates $\mathbb{Z}^n$ for every $1 \leqslant i \leqslant m$. Then any $m + 1$ points in $(\mathbb{K}^*)^n$ impose independent conditions on the space $\mathcal{L}(B)$.*

Proof. Suppose $m = 1$ and let $T = \{p_0, p_1\}$ be any subset in $(\mathbb{K}^*)^n$. It is enough to show that there is a polynomial $g \in \mathcal{L}(B)$ such that $g(p_1) = 0$ and $g(p_0) \neq 0$. We may assume that B contains the origin. Let $\{v_1, \ldots, v_n\} \subseteq B$ be a basis for $\mathbb{Z}^n$ and let $s = t^M = (t^{v_1}, \ldots, t^{v_n})$ be the corresponding automorphism of $(\mathbb{K}^*)^n$. Choose a linear function $l(s)$ such that $l(p_1^M) = 0$ and $l(p_0^M) \neq 0$. Then the polynomial $g(t) = l(t^M)$ lies in $\mathcal{L}(B)$ and satisfies the required property.

In general, let $T = \{p_0, \ldots, p_m\}$ be any subset of $m + 1$ points in $(\mathbb{K}^*)^n$. By the previous case for every $1 \leqslant i \leqslant m$ there exists $g_i \in \mathcal{L}(B_i)$ such that $g_i(p_i) = 0$ and $g_i(p_0) \neq 0$. Then the polynomial $g = \prod_{i=1}^{m} g_i$ lies in $\mathcal{L}(B)$, vanishes on $T \setminus \{p_0\}$, and is not zero at p_0. This implies that T imposes independent conditions on $\mathcal{L}(B)$. □

In our first application of Theorem 3.2 we estimate $d(\mathcal{C}_A)$ using the number of "primitive" simplices Δ_i one can add to A and still stay in P°, after a possible lattice translation. We say that a simplex Δ is *primitive* if $\Delta = \text{conv.hull}\{0, v_1, \ldots, v_n\}$, where $\{v_1, \ldots, v_n\}$ is a basis for $\mathbb{Z}^n$.

Theorem 3.5. *Let S be the solution set of a system $f_1 = \cdots = f_n = 0$ satisfying assumptions (1)–(3) above. Let A be any set such that $A + \Delta_1 + \cdots + \Delta_m \subseteq P^\circ$ up to a lattice translation, where each Δ_i is a primitive simplex. Then $d(\mathcal{C}_A) \geqslant m + 2$.*

Proof. This follows from Theorem 3.2 and Lemma 3.4. □

In our next application we will consider solution sets $S \subset (\mathbb{K}^*)^n$ satisfying one additional assumption.

Assumption.

(4) There exists an n-polytope Q such that any $|Q_\mathbb{Z}|$ points of S impose independent conditions on $\mathcal{L}(Q)$. In other words, for any subset $T \subset S$ of size $|Q_\mathbb{Z}|$ the evaluation map $\text{ev}_T : \mathcal{L}(Q) \to \mathbb{K}^{|Q_\mathbb{Z}|}$ is an isomorphism.

Example 3.6. Suppose $X = \mathbb{P}^n$ and $Q = \Delta$ is the standard n-simplex, i.e. the convex hull of the origin and the n standard basis vectors. Then (4) is equivalent to saying that no $n + 1$ points of S lie on a

hyperplane. Complete intersections in $\mathbb{P}^n$ with this "generality" assumption were considered by Ballico and Fontanari (2006).

The assumption (4) allows us to obtain better bounds on the minimum distance of the codes $\mathcal{C}_A$, as was suggested by Ballico and Fontanari (2006) in the case of the projective space. In fact, their approach generalizes to arbitrary toric varieties. We will begin with a toric analog of their Horace Lemma.

Proposition 3.7. *Let $T \subset (\mathbb{K}^*)^n$ be a finite subset and A a bounded subset of $\mathbb{R}^n$. Consider a hypersurface H in $(\mathbb{K}^*)^n$ defined by $h \in \mathcal{L}(Q)$. If $T \cap H$ imposes independent conditions on $\mathcal{L}(A+Q)$ and $T \setminus (T \cap H)$ imposes independent conditions on $\mathcal{L}(A)$ then T imposes independent conditions on $\mathcal{L}(A+Q)$.*

Proof. Take any point $p \in T$. If $p \notin H$ then there exists $g \in \mathcal{L}(A)$ which does not vanish at p, but vanishes at all the other points of $T \setminus (T \cap H)$. Then the polynomial $f = gh \in \mathcal{L}(A+Q)$ vanishes at all points of $T \setminus \{p\}$. Also $f(p) = g(p)h(p) \neq 0$ since $p \notin H$.

Now if $p \in H$ then there exists $f_1 \in \mathcal{L}(A+Q)$ which does not vanish at p, but vanishes at all the other points of $T \cap H$. Consider the function $\phi : T \setminus (T \cap H) \to \mathbb{K}$ given by $q \mapsto f_1(q)/h(q)$. We know that there exists $g \in \mathcal{L}(A)$ such that $g(q) = \phi(q)$ for any $q \in T \setminus (T \cap H)$. Put $f = f_1 - gh$. Clearly $f \in \mathcal{L}(A+Q)$ and f vanishes at every point of T except at p. □

Proposition 3.8. *Let S be any subset of $(\mathbb{K}^*)^n$ satisfying assumption (4). Then, for any $k \geqslant 0$, any subset $T \subseteq S$ of size $|T| = (|Q_{\mathbb{Z}}| - 1)k + 1$ imposes independent conditions on $\mathcal{L}(kQ)$.*

Proof. The proof is by induction on k. For $k = 0$ we have $T = \{p\}$ which imposes independent conditions on the space $\mathcal{L}(kQ) \cong \mathbb{K}$.

For $k > 0$ choose $T' \subset T$ of size $m = |Q_{\mathbb{Z}}| - 1$. Since $m < |Q_{\mathbb{Z}}| = \dim \mathcal{L}(Q)$ there exists a non-zero polynomial $h \in \mathcal{L}(Q)$ which vanishes on T'. Moreover, $T' = S \cap H$, where H is the hypersurface defined by h. Indeed, if $S \cap H$ contains a point p not in T' then the evaluation map $\mathrm{ev}_{T' \cup \{p\}} : \mathcal{L}(Q) \to \mathbb{K}^{m+1}$ is degenerate which contradicts the assumption (4). Clearly, since $T' \subset T \subset S$ we have $T' = S \cap H = T \cap H$.

Now $T \setminus T'$ has size $m(k-1)+1$ and by induction imposes independent conditions on $\mathcal{L}((k-1)Q)$. Also by (4) the set T' imposes independent conditions on $\mathcal{L}(Q)$ and hence on $\mathcal{L}(kQ)$ as $Q \subset kQ$ up to a lattice translation. It remains to apply Proposition 3.7. □

Theorem 3.9. *Let S be the solution set of a system $f_1 = \cdots = f_n = 0$ satisfying assumptions (1)–(4). Let A be any set such that $A + kQ \subset P^\circ$ up to a lattice translation, for some $k \geqslant 0$. Then*

$$d(\mathcal{C}_A) \geqslant \big(|Q_{\mathbb{Z}}| - 1\big)k + 2.$$

Proof. The theorem follows from Proposition 3.8 and Theorem 3.2 where we put $m = (|Q_{\mathbb{Z}}| - 1)k + 1$. □

4. Constructing toric complete intersection codes

In this section we give geometric conditions on the polytopes $P_1, \ldots, P_n$ and Q that produce systems satisfying assumption (4) if the coefficients are generic elements of $\overline{\mathbb{K}}$. We use these conditions when constructing examples of toric complete intersection codes in Section 5.

Theorem 4.1. *Let Q be an n-dimensional lattice polytope such that $Q_{\mathbb{Z}}$ generates $\mathbb{Z}^n$. Suppose*

1. $V(P_1, \ldots, P_{n-1}, Q) \geqslant |Q_{\mathbb{Z}}|$,
2. $(|Q_{\mathbb{Z}}| - 1)Q \subset P_n$.

Then the solution set of any system $f_1 = \cdots = f_n = 0$ with Newton polytopes $P_1, \dots, P_n$ and generic coefficients satisfies assumption (4).

Proof. Let $m = |Q_{\mathbb{Z}}| - 1$. Let Γ_i be the hypersurface in $(\overline{\mathbb{K}}^*)^n$ defined by f_i. Consider the curve $C = \Gamma_1 \cap \cdots \cap \Gamma_{n-1}$ in $(\overline{\mathbb{K}}^*)^n$. Let V consist of all ordered collections $(p_0, \dots, p_m)$ of regular points in C such that $\{p_0, \dots, p_m\}$ do not impose independent conditions on $\mathcal{L}(Q)$. In other words,

$$V = \left\{ T = (p_0, \dots, p_m) \in C_{\text{reg}}^{m+1} \;\middle|\; \text{ev}_T : \mathcal{L}(Q) \to \left(\overline{\mathbb{K}}^*\right)^{m+1} \text{ is not surjective} \right\},$$

where by abuse of notation we denote by T both the ordered collection $(p_0, \dots, p_m)$ and the set $\{p_0, \dots, p_m\}$. The set V is algebraic with a dense open subset $V_0 \subset V$ consisting of points of V for which the map ev_T has one-dimensional kernel.

First we will show that $\dim V = m$. Indeed, every $T \in V_0$ defines a unique hypersurface H, defined by a polynomial in $\mathcal{L}(Q)$, such that the corresponding set T lies in $C \cap H$. We obtain a map $\pi : V_0 \to \mathbb{P}\mathcal{L}(Q)$. On the other hand, by the Bernstein–Kushnirenko theorem (see Theorem 2.6) any generic hypersurface H with Newton polytope Q satisfies $|C \cap H| = V(P_1, \dots, P_{n-1}, Q) \geqslant m + 1$, so the image of π is dense in $\mathbb{P}\mathcal{L}(Q)$. Clearly, the fibers $\pi^{-1}(H)$ are finite, so we get $\dim(V) = \dim(V_0) = \dim(\pi(V_0)) = \dim(\mathbb{P}\mathcal{L}(Q)) = m$.

Now we will show that choosing a generic f_n with Newton polytope P_n produces $S = C \cap \Gamma_n$ which satisfies assumption (4). For this consider the set

$$W = \bigcup_{T \in V} W_T, \quad \text{where } W_T = \left\{ f \in \mathcal{L}(P_n) \;\middle|\; f \text{ vanishes on } T \right\}.$$

Clearly, every f_n in the complement of W produces such S (we also must avoid those f_n which have zero coefficients corresponding to the vertices of P_n), so we need to show that W has positive codimension in $\mathcal{L}(P_n)$. Indeed, according to our assumption $mQ \subset P_n$, so every set of $m + 1$ points in S imposes independent conditions on $\mathcal{L}(mQ)$ (by Lemma 3.4) and hence on $\mathcal{L}(P_n)$. Therefore the codimension of every subspace W_T equals $m + 1$. Thus W is a vector bundle with m-dimensional base and codimension $m + 1$ fiber, so W has codimension one. □

In the next theorem we show that in some situations the condition $(|Q_{\mathbb{Z}}| - 1)Q \subset P_n$ can be replaced with $P_1 + \cdots + P_{n-1} + Q \subset P_n$. When $|Q_{\mathbb{Z}}|$ grows fast as a function of n, the latter condition is preferable if one wants to avoid dealing with unnecessarily large P_n.

We will need the following consequence of the Toric Euler–Jacobi theorem.

Proposition 4.2. *Let $P_1, \dots, P_n$ be n-dimensional lattice polytopes with the same normal fan, such that* $\operatorname{char} \mathbb{K}$ *does not divide the normalized mixed volume $V(P_1, \dots, P_n)$. Let S be the solution set for a system $f_1 = \cdots = f_n = 0$ with Newton polytopes $P_1, \dots, P_n$, satisfying assumptions* (1)–(3)*. Then S imposes independent conditions on the space $\mathcal{L}(P)$.*

Proof. We need to show that for any function $\psi : S \to \mathbb{K}$ there exists $g \in \mathcal{L}(P)$ with $g(p) = \psi(p)$ for all $p \in S$. Define $\phi : S \to \mathbb{K}$ by setting $\phi(p) = \frac{\psi(p)}{J_f^{\mathbb{T}}(p)} - c$, where $c = \frac{1}{|S|} \sum_{p \in S} \frac{\psi(p)}{J_f^{\mathbb{T}}(p)}$. Then $\sum_{p \in S} \phi(p) = 0$, so by Theorem 2.4 there exists $h \in \mathcal{L}(P^\circ)$ such that $h(p) = J_f^{\mathbb{T}}(p)\phi(p)$ for all $p \in S$. Now we can put $g = h + cJ_f^{\mathbb{T}} \in \mathcal{L}(P)$, as $g(p) = h(p) + cJ_f^{\mathbb{T}}(p) = \psi(p)$ for all $p \in S$, as required. □

This can be slightly refined. As we have seen in the above proof, Proposition 4.2 still holds if we replace $\mathcal{L}(P)$ with $\operatorname{span}_{\mathbb{K}}\{\mathcal{L}(P^\circ), J_f^{\mathbb{T}}\}$.

Theorem 4.3. *Let $P_1, \dots, P_n$ and Q be n-dimensional lattice polytopes with the same normal fan and such that $Q_{\mathbb{Z}}$ generates $\mathbb{Z}^n$. Suppose*

1. $V(P_1, \dots, P_{n-1}, Q) \geqslant |Q_{\mathbb{Z}}|$,
2. $P_1 + \cdots + P_{n-1} + Q \subset P_n$.

Then the solution set of any system $f_1 = \cdots = f_n = 0$ with Newton polytopes $P_1, \ldots, P_n$ and generic coefficients satisfies assumption (4).

Proof. The proof is the same as for Theorem 4.1, except for the last two sentences. Instead we need the following observation. Let $T \in V$. By the definition of V there exists a hypersurface H defined by a polynomial in $\mathcal{L}(Q)$ such that $T \subseteq C \cap H$. By Proposition 4.2, $C \cap H$ imposes independent conditions on the space $\mathcal{L}(P_1 + \cdots + P_{n-1} + Q)$. Therefore T imposes independent conditions on $\mathcal{L}(P_n)$ and hence the codimension of the subspace W_T equals $m+1$. The rest is as in the proof of Theorem 4.1. □

5. Examples

In this section we put several applications of the results of the previous section as well as provide specific examples of toric complete intersection codes over finite fields.

We start by showing how Theorem 3.5 and Theorem 3.9 recover the results of Gold et al. (2005) and Ballico and Fontanari (2006).

Example 5.1. Let S be a zero-dimensional smooth complete intersection in $\mathbb{P}^n$ given by n homogeneous polynomials $F_1, \ldots, F_n$ over $\mathbb{K}$. Suppose S lies in $\mathbb{P}^n(\mathbb{K})$. Up to a projective change of coordinates we may assume that S lies in the algebraic torus $(\mathbb{K}^*)^n$. Rewriting F_i in the affine coordinates for $(\mathbb{K}^*)^n$ we obtain a polynomial f_i with Newton polytope $P_i = d_i\Delta$ where Δ is the standard n-simplex and $d_i = \deg(F_i)$. It is easy to see that S satisfies the assumptions (1)–(3) in Section 2.1.

Now let $s = \sum_{i=1}^n d_i - (n+1)$ and let $A = a\Delta$ for some $1 \leqslant a \leqslant s$. Notice that $\mathcal{L}(A)$ is the space of polynomials of total degree at most a. We are going to apply Theorem 3.5 with $l = s - a$ and all the Δ_i being simply Δ. Clearly, $A + \Delta_1 + \cdots + \Delta_n$, which equals $s\Delta$, lies in the interior of $P = (\sum_{i=1}^n d_i)\Delta$. Therefore, by Theorem 3.5, $d(\mathcal{C}_A) \geqslant s - a + 2$. This is the result of Gold et al. (2005).

Next suppose S satisfies assumption (4) with $Q = \Delta$. As pointed out before this means that no $n+1$ points of S lie in a hyperplane in $\mathbb{P}^n$. Applying Theorem 3.9 with $k = s - a$ we obtain $d(\mathcal{C}_A) \geqslant n(s-a) + 2$, which is the result of Ballico and Fontanari (2006).

In the next example we consider systems defined by multi-homogeneous polynomials. This is the case of toric variety $X = \mathbb{P}^1 \times \cdots \times \mathbb{P}^1$.

Example 5.2. For $1 \leqslant i \leqslant n$ let P_i be the lattice box with dimensions $(d_{i1}, \ldots, d_{in})$, each $d_{ij} \geqslant 1$. Let S be the solution set of a system $f_1 = \cdots = f_n = 0$ with Newton polytopes $P_1, \ldots, P_n$ satisfying assumptions (1)–(3). By the Bernstein–Kushnirenko theorem $|S| = V(P_1, \ldots, P_n)$ which equals $\mathrm{Perm}(D)$, the permanent of the matrix $D = (d_{ij})$. Indeed, since each P_i is the Minkowski sum of segments $P_i = \sum_{j=1}^n I_{ij}$, where $I_{ij} = [0, d_{ij}e_j]$, by the multi-linearity of the mixed volume we obtain

$$V(P_1, \ldots, P_n) = V\left(\sum_{j=1}^n I_{1j}, \ldots, \sum_{j=1}^n I_{nj}\right) = \sum_{\sigma \in S_n} V(I_{1\sigma(1)}, \ldots, I_{n\sigma(n)})$$
$$= \sum_{\sigma \in S_n} d_{1\sigma(1)} \cdots d_{n\sigma(n)} = \mathrm{Perm}(D).$$

Now let A be a lattice box with dimensions $(a_1, \ldots, a_n)$. Note that P is a lattice box with dimensions $(d_1, \ldots, d_n)$, where $d_j = \sum_i d_{ij}$. Hence A lies in P° whenever $1 \leqslant a_j \leqslant d_j - 2$. Next, suppose S satisfies the assumption (4) with $Q = \square$, the unit n-cube. Then for $k = \min_j(d_j - 2 - a_j)$ we have $A + k\square \subset P^\circ$. Applying Theorem 3.9 we get

$$d(\mathcal{C}_A) \geqslant \left(2^n - 1\right) \min_{1 \leqslant j \leqslant n} (d_j - 2 - a_j) + 2.$$

Let us now see under which condition on the polytopes P_i the assumption (4) is generically satisfied. According to Theorem 4.1 and Theorem 4.3 it is enough to require $V(P_1, \ldots, P_{n-1}, \square) \geqslant 2^n$

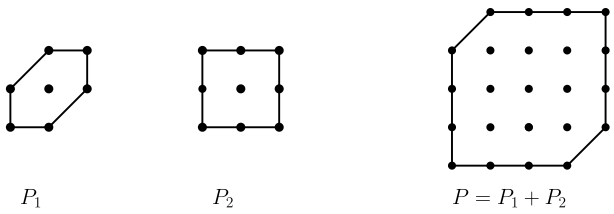

Fig. 5.1. The Newton polygons and their Minkowski sum.

and either $(2^n - 1)\square \subseteq P_n$ or $P_1 + \cdots + P_{n-1} + \square \subseteq P_n$. The latter occurs when $d_{nj} \geqslant \min(2^n - 1, \sum_{i=1}^{n-1} d_{ij} + 1)$ for $1 \leqslant j \leqslant n$. For the former note that $\square \subset P_i$, so by monotonicity of the mixed volume

$$V(P_1, \ldots, P_{n-1}, \square) \geqslant V(\square, \ldots, \square) = n! \geqslant 2^n,$$

for $n \geqslant 4$. For $n = 2$ we require $V(P_1, \square) = d_{11} + d_{12} \geqslant 4$. For $n = 3$ we require that at least one edge of either P_1 or P_2 has length 2, since in this case

$$V(P_1, P_2, \square) = d_{11}d_{22} + d_{12}d_{23} + d_{13}d_{21} + d_{13}d_{22} + d_{12}d_{21} + d_{11}d_{23} \geqslant 8.$$

In the next two examples we present two explicit toric complete intersection codes over $\mathbb{F}_{16}$ and $\mathbb{F}_{128}$, respectively. In both cases the toric variety is a del Pezzo surface. We use MAGMA (Bosma et al., 1997) for constructing these examples.

Example 5.3. Let ξ be a generator of the cyclic group $\mathbb{F}_{16}^*$. Let P_1 and P_2 be as in Fig. 5.1. Consider the following system.

$$\begin{cases} f_1 = x^2y^2 + \xi^7x^2y + \xi^{11}xy^2 + \xi^4xy + x + \xi^7y^2 + \xi^{13} = 0, \\ f_2 = x^2y^2 + \xi^7x^2y + \xi^6x^2 + \xi^{14}xy^2 + \xi^{12}xy + \xi^3x + y^2 + \xi^5y + \xi^4 = 0. \end{cases}$$

The system has $8 = V(P_1, P_2)$ simple solutions in $(\mathbb{F}_{16}^*)^2$:

$$S = \left\{ \left(\xi, \xi^6\right), \left(\xi^4, \xi^3\right), \left(\xi^{11}, 1\right), \left(\xi^{11}, \xi^{12}\right), \left(\xi^{12}, \xi^7\right), \left(\xi^{13}, \xi^9\right), \left(\xi^{14}, \xi^4\right), \left(\xi^{14}, \xi^{13}\right) \right\}.$$

Let $Q = \square$, the unit square. One can check that any 4 points of S impose independent conditions on the space $\mathcal{L}(\square)$. Now choose $A = \square$ as well. We have $A + \square \subset P^\circ$, so

$$d(\mathcal{C}_A) \geqslant (4 - 1) + 2 = 5.$$

Furthermore $\dim \mathcal{C}_A = |A_{\mathbb{Z}}| = 4$, so we get an MDS $[8, 4, 5]$-code over $\mathbb{F}_{16}$.

To construct a bigger example we start with polygons P_1, P_2 satisfying the conditions of Theorem 4.1. Then we choose a random polynomial f_1 with Newton polytope P_1. If the size of the field is big enough we can choose $V(P_1, P_2)$ rational points on the curve $f_1 = 0$ which satisfy assumption (4).

Example 5.4. The polygons P_1 and P_2 and their Minkowski sum P are depicted in Fig. 5.2. Consider a system $f_1 = f_2 = 0$ over $\mathbb{F}_q$ with Newton polytopes P_1, P_2 satisfying assumptions (1)–(3), and let S be the solution set of the system. We have $|S| = V(P_1, P_2) = 14$. On the other hand, a simple application of the Serre bound shows that for $q \leqslant 8$ the curve $f_1 = 0$ has less than 14 rational points. Therefore we must have $q > 8$.

First we consider an application of Theorem 3.5. Take A to be a 2×2 lattice square, Δ_1 the convex hull of $\{(0, 0), (1, 0), (1, 1)\}$, and Δ_2 the convex hull of $\{(0, 0), (0, 1), (1, 1)\}$. Then $A + \Delta_1 + \Delta_2 \subset P^\circ$. Therefore, by Theorem 3.5, we have $d(\mathcal{C}_A) \geqslant 2 + 2 = 4$. The evaluation map $\mathrm{ev}_S : \mathcal{L}(A) \to {\mathbb{F}_q}^{14}$ has one-dimensional kernel spanned by f_1. Therefore, $\dim \mathcal{C}_A = |A_{\mathbb{Z}}| - 1 = 8$ and we obtain a $[14, 8, \geqslant 4]$-code over $\mathbb{F}_q$ with $q \geqslant 9$.

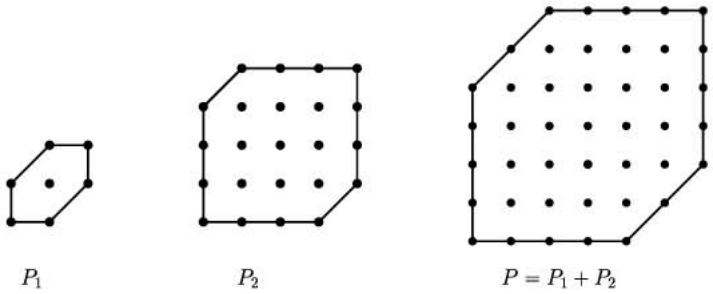

Fig. 5.2. The Newton polygons and their Minkowski sum.

Next we consider a set S satisfying the additional assumption (4). We set $Q = \square$, the unit square. Since $V(P_1, \square) = 5 \geqslant 4$ and $3\square \subset P_2$, both conditions of Theorem 4.1 are satisfied.

We will work over $\mathbb{F}_{128}$; as before ξ will denote a generator of $\mathbb{F}_{128}^*$. Here is a random polynomial over $\mathbb{F}_{128}$ with Newton polytope P_1:

$$f_1 = x^2y^2 + \xi x^2 y + \xi^{32} xy^2 + \xi^4 xy + \xi^{78} x + \xi^{110} y + \xi^{31}.$$

The curve $f_1 = 0$ has 146 rational points in the torus. We choose 14 of these rational points which impose independent conditions on $\mathcal{L}(\square)$. Here is one such subset:

$$S = \{(\xi^5, \xi^{91}), (\xi^{43}, \xi^{59}), (\xi^{44}, \xi^{100}), (\xi^{47}, \xi^{125}), (\xi^{51}, \xi^{33}), (\xi^{58}, \xi^{90}), (\xi^{68}, \xi^{42}), (\xi^{78}, \xi^{11}), (\xi^{78}, \xi^{12}), (\xi^{85}, \xi^{79}), (\xi^{96}, \xi^{11}), (\xi^{105}, \xi^{41}), (\xi^{116}, \xi^{106}), (\xi^{124}, \xi^{65})\}.$$

Since $|P_2 \cap \mathbb{Z}^2| > |S| = 14$ there exist polynomials f_2 with Newton polytope P_2 which vanish at S. We choose such f_2 that has no common factors with f_1. For example, we can take

$$f_2 = x^4y^4 + \xi^{59}x^4y + \xi^{10}x^3y + \xi^{66}x^3 + \xi^{26}x^2y + \xi^{104}x^2 + xy^4 + \xi^{44}xy^3 + \xi^{50}xy^2 + \xi^{78}xy + \xi^{56}x + \xi^{118}y^3 + \xi^{38}y^2 + \xi^{36}y + \xi^{108}.$$

By Remark 2.7, S is the solution set of $f_1 = f_2 = 0$ and satisfies assumptions (1)–(4). Next we look at different choices of the set A.

(a) Let $A = P_1$. Then $A + 2\square \subset P^\circ$, so by Theorem 3.9 we get $d(\mathcal{C}_A) \geqslant (4-1)\cdot 2 + 2 = 8$. It is easy to see that $\dim \mathcal{C}_A = |A_{\mathbb{Z}}| - 1 = 6$ and we obtain a $[14, 6, \geqslant 8]$-code over $\mathbb{F}_{128}$. In fact, the minimum distance is exactly 8 in this case.

(b) Let A be the segment joining $(0,0)$ and $(1,1)$. Then $A + 3\square \subset P^\circ$, so by Theorem 3.9 we get $d(\mathcal{C}_A) \geqslant (4-1)\cdot 3 + 2 = 11$. Since $\dim \mathcal{C}_A = |A_{\mathbb{Z}}| = 2$ we get a $[14, 2, \geqslant 11]$-code over $\mathbb{F}_{128}$, which is in fact a $[14, 2, 13]$-code.

(c) Let $A = P_1 + \square$. Then $A + \square \subset P^\circ$ so by Theorem 3.9 we get $d(\mathcal{C}_A) \geqslant (4-1) + 2 = 5$. To compute the dimension of $\mathcal{C}_A$ note that $\mathrm{ev}_S : \mathcal{L}(A) \to \mathbb{F}_{128}{}^{14}$ has 4-dimensional kernel. In fact, $\mathcal{L}(A) \cap I = \mathrm{span}\{f_1, xf_1, yf_1, xyf_1\}$, where I is the ideal generated by f_1, f_2. Therefore $\dim \mathcal{C}_A = |A_{\mathbb{Z}}| - 4 = 10$. This shows that $\mathcal{C}_A$ is an MDS code over $\mathbb{F}_{128}$ with parameters $[14, 10, 5]$.

6. Conclusion and further work

Given a system of Laurent polynomial equations $f_1 = \cdots = f_n = 0$ with n-dimensional Newton polytopes $P_1, \ldots, P_n$ satisfying assumptions (1)–(3) or (1)–(4) and a set $A \subset P^\circ$ we defined a class of evaluation codes $\mathcal{C}_{S,\mathcal{L}(A)}$, called toric complete intersection codes, and found general lower bounds for their minimum distance.

We then gave conditions on the polytopes $P_1, \ldots, P_n$ and Q which guarantee that generic systems with such Newton polytopes satisfy assumption (4). One would like to obtain some general results

about the size of the field for which toric complete intersections with given polytopes exist and with what probability they occur. This would allow a more systematic way of constructing them and studying their parameters.

Computing the dimension of $\mathcal{C}_{S,\mathcal{L}(A)}$ is not obvious since the evaluation map will have a non-trivial kernel, in general. It requires computing the codimension of the ideal generated by the f_i in the space $\mathcal{L}(A)$. Although this can be done in concrete examples one would like to have a general way of doing so.

Acknowledgements

I thank Ştefan Tohaneanu for several fruitful discussions about evaluation codes on complete intersections and explaining his work in Tohaneanu (2009, 2011); and Jan Tuitman for answering questions about the Bernstein–Kushnirenko theorem in positive characteristic. I am grateful to two anonymous referees whose comments helped to improve the exposition.

References

Ballico, E., Fontanari, C., 2006. The Horace method for error-correcting codes. Appl. Algebra Engrg. Comm. Comput. 17 (2), 135–139.

Bernstein, D.N., 1975. The number of roots of a system of equations. Funct. Anal. Appl. 9 (2), 183–185.

Bosma, Wieb, Cannon, John, Playoust, Catherine, 1997. The Magma algebra system. I. The user language. J. Symbolic Comput. 24, 235–265.

Cattani, E., Cox, D.A., Dickenstein, A., 1997. Residues in toric varieties. Compos. Math. 108 (1), 35–76.

Cattani, E., Cueto, M.A., Dickenstein, A., Di Rocco, S., Sturmfels, B., 2011. Mixed discriminants. arXiv:1112.1012v1 [math.AG].

Cattani, E., Dickenstein, A., 1997. A global view of residues in the torus. J. Pure Appl. Algebra 117/118, 119–144.

Cox, D.A., 1996. Toric residues. Ark. Mat. 34, 73–96.

Cox, D.A., Little, J., Schenck, H., 2011. Toric Varieties. Grad. Stud. Math., vol. 124. AMS, Providence, RI.

Duursma, I., Rentería, C., Tapia-Recillas, H., 2001. Reed–Muller codes on complete intersections. Appl. Algebra Engrg. Comm. Comput. 11, 455–462.

Eisenbud, D., Green, M., Harris, J., 1996. Cayley–Bacharach theorems and conjectures. Bull. Amer. Math. Soc. 33 (3), 295–324.

Fulton, W., 1993. Introduction to Toric Varieties. Princeton Univ. Press, Princeton.

Gelfond, O.A., Khovanskii, A.G., 2002. Toric geometry and Grothendieck residues. Mosc. Math. J. 2 (1), 99–112.

Gold, L., Little, J., Schenck, H., 2005. Cayley–Bacharach and evaluation codes on complete intersections. J. Pure Appl. Algebra 196 (1), 91–99.

Hansen, J., 2000. Toric surfaces and error-correcting codes. In: Buchmann, J., et al. (Eds.), Coding Theory, Cryptography, and Related Areas. Springer, pp. 132–142.

Hansen, J., 2001. Error-correcting codes from higher-dimensional varieties. Finite Fields Appl. 7 (4), 530–552.

Hansen, J., 2003. Linkage and codes on complete intersections. Appl. Algebra Engrg. Comm. Comput. 14, 175–185.

Joshua, R., Akhtar, R., 2011. Toric residue codes: I. Finite Fields Appl. 17 (1), 15–50.

Joyner, D., 2004. Toric codes over finite fields. Appl. Algebra Engrg. Comm. Comput. 15, 63–79.

Khovanskii, A.G., 1978. Newton polyhedra and the Euler–Jacobi formula. Russian Math. Surveys 33 (6), 237–238.

Kunz, E., 2008. Residues and Duality for Projective Algebraic Varieties. Univ. Lecture Ser., vol. 47. AMS, Providence, RI.

Kushnirenko, A.G., 1976. Newton polyhedra and Bezout's theorem. Funktsional. Anal. i Prilozhen. 10 (3), 82–83 (in Russian).

Little, J., 2008. Algebraic geometry codes from higher dimensional varieties. In: Martinez-Moro, E., et al. (Eds.), Advances in Algebraic Geometry Codes. In: Ser. Coding Theory Cryptol., vol. 5. World Sci. Publ., Hackensack, NJ, pp. 257–293.

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

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

Ruano, Diego, 2007. On the parameters of r-dimensional toric codes. Finite Fields Appl. 13, 962–976.

Soprunov, I., 2007. Global residues for sparse polynomial systems. J. Pure Appl. Algebra 209 (2), 383–392.

Soprunov, I., Soprunova, J., 2009. Toric surface codes and Minkowski length of polygons. SIAM J. Discrete Math. 23 (1), 384–400.

Soprunov, I., Soprunova, J., 2010. Bringing toric codes to the next dimension. SIAM J. Discrete Math. 24 (2), 655–665.

Tohaneanu, Ştefan O., 2009. Lower bounds on minimal distance of evaluation codes. Appl. Algebra Engrg. Comm. Comput. 20 (5–6), 351–360.

Tohaneanu, Ştefan O., 2011. The minimum distance of sets of points and the minimum socle degree. J. Pure Appl. Algebra 215 (11), 2645–2651.

Tsfasman, M., Vlăduţ, S., Nogin, D., 2007. Algebraic Geometric Codes: Basic Notions. Math. Surveys Monogr., vol. 139. AMS, Providence, RI.

Tuitman, J., 2010. Counting points in families of nondegenerate curves. PhD thesis.