Studia Scientiarum Mathematicarum Hungarica 49 (3), 406–418 (2012)
DOI: 10.1556/SScMath.49.2012.3.1216

PARAMETERIZED AFFINE CODES

HIRAM H. LÓPEZ[1], ELISEO SARMIENTO[1], MARIA VAZ PINTO[2] and RAFAEL H. VILLARREAL[1]

[1] Departamento de Matemáticas, Centro de Investigación y de Estudios Avanzados del IPN, Apartado Postal 14–740, 07000 Mexico City, D.F.
e-mails: hlopez@math.cinvestav.mx, esarmiento@math.cinvestav.mx, vila@math.cinvestav.mx

[2] Departamento de Matemática, Instituto Superior Tecnico, Universidade Técnica de Lisboa, Avenida Rovisco Pais, 1, 1049-001 Lisboa, Portugal
e-mail: vazpinto@math.ist.utl.pt

Communicated by P. P. Pálfy

(Received May 9, 2011; accepted November 9, 2011)

Abstract

Let K be a finite field and let X^* be an affine algebraic toric set parameterized by monomials. We give an algebraic method, using Gröbner bases, to compute the length and the dimension of $C_{X^*}(d)$, the parameterized affine code of degree d on the set X^*. If Y is the projective closure of X^*, it is shown that $C_{X^*}(d)$ has the same basic parameters that $C_Y(d)$, the parameterized projective code on the set Y. If X^* is an affine torus, we compute the basic parameters of $C_{X^*}(d)$. We show how to compute the vanishing ideals of X^* and Y.

1. Introduction

Let $K = \mathbb{F}_q$ be a finite field with q elements and let $y^{v_1}, \ldots, y^{v_s}$ be a finite set of monomials. As usual if $v_i = (v_{i1}, \ldots, v_{in}) \in \mathbb{N}^n$, then we set

$$y^{v_i} = y_1^{v_{i1}} \cdots y_n^{v_{in}}, \quad i = 1, \ldots, s,$$

2000 *Mathematics Subject Classification.* Primary 13P25; Secondary 14G50, 14G15, 11T71, 94B27, 94B05.

Key words and phrases. Evaluation codes, parameterized affine codes, vanishing ideals, minimum distance, dimension, length, affine Hilbert function.

The second author was partially supported by CONACyT. The third author is a member of the Center for Mathematical Analysis, Geometry and Dynamical Systems. The fourth author was partially supported by SNI.

where $y_1, \ldots, y_n$ are the indeterminates of a ring of polynomials with coefficients in K. Consider the following set parameterized by these monomials

$$X^* := \left\{ (x_1^{v_{11}} \cdots x_n^{v_{1n}}, \ldots, x_1^{v_{s1}} \cdots x_n^{v_{sn}}) \in \mathbb{A}^s \mid x_i \in K^* \text{ for all } i \right\},$$

where $K^* = K \setminus \{0\}$ and $\mathbb{A}^s = K^s$ is an affine space over the field K. We call X^* an *affine algebraic toric set* parameterized by $y^{v_1}, \ldots, y^{v_s}$. The set X^* is a multiplicative group under componentwise multiplication.

Let $S = K[t_1, \ldots, t_s] = \oplus_{d=0}^{\infty} S_d$ be a polynomial ring over the field K with the standard grading, let $P_1, \ldots, P_m$ be the points of X^*, and let $S_{\leqq d}$ be the set of polynomials of S of degree at most d. The *evaluation map*

$$\text{ev}_d : S_{\leqq d} \longrightarrow K^{|X^*|}, \quad f \mapsto \big(f(P_1), \ldots, f(P_m)\big), \tag{1.1}$$

defines a linear map of K-vector spaces. The image of ev_d, denoted by $C_{X^*}(d)$, defines a *linear code*. We call $C_{X^*}(d)$ a *parameterized affine code* of degree d on the set X^*. As usual by a *linear code* we mean a linear subspace of $K^{|X^*|}$. Parameterized affine codes are special types of affine Reed–Muller codes in the sense of [24, p. 37]. If $s = n = 1$ and $v_1 = 1$, then $X^* = \mathbb{F}_q^*$ and we obtain the classical Reed–Solomon code of degree d [21, p. 42].

The *dimension* and the *length* of $C_{X^*}(d)$ are given by $\dim_K C_{X^*}(d)$ and $|X^*|$ respectively. The dimension and the length are two of the *basic parameters* of a linear code. A third basic parameter is the *minimum distance* which is given by

$$\delta_{X^*}(d) = \min\left\{ \|v\| : 0 \neq v \in C_{X^*}(d) \right\},$$

where $\|v\|$ is the number of non-zero entries of v.

The basic parameters of $C_{X^*}(d)$ are related by the *Singleton bound* for the minimum distance

$$\delta_{X^*}(d) \leqq |X^*| - \dim_K C_{X^*}(d) + 1. \tag{1.2}$$

The contents of this paper are as follows. Let $\mathbb{P}^s$ be the projective space over the field K. In Theorem 2.4, it is shown that $C_{X^*}(d)$ has the same parameters that $C_Y(d)$, the parameterized projective code of degree d on Y (see Definition 2.1), where Y is the image of X^* under the map $\mathbb{A}^s \to \mathbb{P}^s$, $x \mapsto \big[(x, 1)\big]$. It is also shown that the dimension and the length of a parameterized affine code can be expressed in terms of the Hilbert function and the degree of the vanishing ideal $I(Y)$ of Y.

As an application, if T is an affine torus we compute the basic parameters of $C_T(d)$ (see Corollaries 2.7 and 2.9). The basic parameters of other types of Reed–Muller codes (or evaluation codes) over finite fields have been computed in a number of cases. If $X = \mathbb{P}^s$, the parameters of $C_X(d)$ are described in [19, Theorem 1]. If X is the image of $\mathbb{A}^s$ under the map $\mathbb{A}^s \to \mathbb{P}^s$,

$x \mapsto \big[(x,1)\big]$, the parameters of $C_X(d)$ are described in [3, Theorem 2.6.2]. If $X \subset \mathbb{P}^s$ is a set parameterized by monomials arising from the edges of a clutter and the vanishing ideal of X is a complete intersection, the parameters of $C_X(d)$ are described in [18].

In Theorem 3.4, we show how to compute the vanishing ideal of X^*. Then, we show how to compute the vanishing ideal of Y using Gröbner bases (see Lemma 3.7). We obtain a method to compute the dimension and the length of $C_{X^*}(d)$ using the computer algebra system *Macaulay*2 [12] (see Corollary 3.8 and Procedure 3.9).

For all unexplained terminology and additional information we refer to [2, 20, 22] (for the theory of Gröbner bases, Hilbert functions, and toric ideals), [15, 21, 24] (for the theory of linear codes), and [8, 9, 10, 11, 17] for the theory of Reed–Muller codes and evaluation codes.

2. Computing the length and dimension of an affine parameterized code

We continue to use the notation and definitions used in the introduction. In this section we study parameterized affine codes and show how to express its dimension and length in terms of the Hilbert function and the degree of a certain standard graded algebra.

Let $\mathbb{P}^s$ be a projective space over the field K. Consider the algebraic toric set

$$Y := \Big\{ \big[\big(x_1^{v_{11}} \cdots x_n^{v_{1n}}, \ldots, x_1^{v_{s1}} \cdots x_n^{v_{sn}}, 1 \big) \big] \mid x_i \in K^* \text{ for all } i \Big\} \subset \mathbb{P}^s,$$

where $K^* = K \setminus \{0\}$. Notice that Y is parameterized by $y^{v_1}, \ldots, y^{v_s}, y^{v_{s+1}}$, where $v_{s+1} = 0$. Also notice that Y is the projective closure of X^* because K is a finite field (see Section 3). The sets X^* and Y have the same cardinality because the map $\rho\colon X^* \to Y$, $x \mapsto \big[(x,1)\big]$, is bijective.

The *vanishing ideal* of Y, denoted by $I(Y)$, is the ideal of $S[u]$ generated by the homogeneous polynomials that vanish on Y, where $u = t_{s+1}$ is a new variable and $S[u] = \oplus_{d \geq 0} S[u]_d$ is a polynomial ring, with the standard grading, over the field K. Let $Q_1, \ldots, Q_m$ be a set of representatives for the points of Y and let $f_0(t_1, \ldots, t_{s+1}) = t_1^d$. The evaluation map

$$\mathrm{ev}'_d\colon S[u]_d \longrightarrow K^{|Y|}, \quad f \mapsto \left(\frac{f(Q_1)}{f_0(Q_1)}, \ldots, \frac{f(Q_m)}{f_0(Q_m)} \right),$$

defines a linear map of K-vector spaces. If $Q'_1, \ldots, Q'_m$ is another set of representatives, then there are $\lambda_1, \ldots, \lambda_m$ in K^* such that $Q'_i = \lambda_i Q_i$ for all i. Thus, $f(Q'_i)/f_0(Q'_i) = f(Q_i)/f_0(Q_i)$ for $f \in S[u]_d$ and $1 \leqq i \leqq m$. This means that the map ev'_d is independent of the set of representatives that we

choose for the points of Y. In what follows we choose $(P_1, 1), \ldots, (P_m, 1)$ as a set of representatives for the points of Y.

DEFINITION 2.1. The image of ev'_d, denoted by $C_Y(d)$, defines a *linear code* that we call a *parameterized projective code* of degree d.

DEFINITION 2.2. The *Hilbert function* of $S[u]/I(Y)$ is given by

$$H_Y(d) := \dim_K \left(S[u]_d / I(Y) \cap S[u]_d \right),$$

and the *Krull-dimension* of $S[u]/I(Y)$ is denoted by $\dim \left(S[u]/I(Y) \right)$.

The unique polynomial $h_Y(t) = \sum_{i=0}^{k-1} c_i t^i \in \mathbb{Z}[t]$ of degree

$$k - 1 = \dim \left(S[u]/I(Y) \right) - 1$$

such that $h_Y(d) = H_Y(d)$ for $d \gg 0$ is called the *Hilbert polynomial* of $S[u]/I(Y)$, see [20]. The integer $c_{k-1}(k-1)!$, denoted by $\deg \left(S[u]/I(Y) \right)$, is called the *degree* or *multiplicity* of $S[u]/I(Y)$.

PROPOSITION 2.3 ([14, Lecture 13], [7]). *$h_Y(d) = |Y|$ for $d \geqq |Y| - 1$.*

Recall that the *vanishing ideal* of X^*, denoted by $I(X^*)$, consists of all polynomials f of S that vanish on the set X^*. Given $f \in S_{\leqq d}$, we set

$$f^{\mathfrak{h}}(t_1, \ldots, t_s, u) := u^d f(t_1/u, \ldots, t_s/u).$$

The polynomial $f^{\mathfrak{h}}$ is homogeneous of degree d. The polynomial $f^{\mathfrak{h}}$ is called the *homogenization* of f with respect to u and d.

THEOREM 2.4. (a) *There is an isomorphism of K-vector spaces $\varphi : C_{X^*}(d) \to C_Y(d)$,*

$$\left(f(P_1), \ldots, f(P_m) \right) \overset{\varphi}{\longmapsto} \left(\frac{f^{\mathfrak{h}}(P_1, 1)}{f_0(P_1, 1)}, \ldots, \frac{f^{\mathfrak{h}}(P_m, 1)}{f_0(P_m, 1)} \right) = \left(\frac{f(P_1)}{f_0(P_1)}, \ldots, \frac{f(P_m)}{f_0(P_m)} \right).$$

(b) *The parameterized codes $C_{X^*}(d)$ and $C_Y(d)$ have the same parameters.*

(c) *The dimension and the length of $C_{X^*}(d)$ are*

$$H_Y(d) \quad \textit{and} \quad \deg \left(S[u]/I(Y) \right)$$

respectively.

PROOF. (a) We set $I(X^*)_{\leqq d} = I(X^*) \cap S_{\leqq d}$. The kernel of ev_d is precisely $I(X^*)_{\leqq d}$. Hence, there is an isomorphism of K-vector spaces

$$S_{\leqq d}/I(X^*)_{\leqq d} \simeq C_d(X^*) = \big\{\big(f(P_1), \ldots, f(P_m)\big) \mid f \in S_{\leqq d}\big\}. \tag{2.1}$$

The kernel of ev'_d is the homogeneous part $I(Y)_d$ of degree d of $I(Y)$. Notice that $I(Y)_d$ is equal to $I(Y) \cap S[u]_d$. Therefore, there is an isomorphism of K-vector spaces

$$S[u]_d/I(Y)_d \simeq C_Y(d). \tag{2.2}$$

The homogenization map $\psi : S_{\leqq d} \to S[u]_d$, $f \mapsto f^{\mathfrak{h}}$, is an isomorphism of K-vector spaces (see [13, p. 330]) such that $\psi\big(I(X^*)_{\leqq d}\big) = I(Y)_d$. Hence, the induced map

$$\Phi : S_{\leqq d} \to S[u]_d/I(Y)_d, \qquad f \longmapsto f^{\mathfrak{h}} + I(Y)_d, \tag{2.3}$$

is a surjection. Thus, by Eqs. (2.1) and (2.2), it suffices to observe that $\ker(\Phi) = I(X^*)_{\leqq d}$.

(b) From part (a) it is clear that $C_{X^*}(d)$ and $C_Y(d)$ have the same dimension and length. To show that they have the same minimum distance it suffices to notice that the isomorphism φ between $C_{X^*}(d)$ and $C_Y(d)$ preserves the norm, i.e., $\|v\| = \big\|\varphi(v)\big\|$ for $v \in C_{X^*}(d)$.

(c) The ring $S[u]/I(Y)$ has Krull-dimension 1 (see [16, Theorem 2.1(c), p. 85]), thus its Hilbert polynomial $h_Y(t) = c_0$ is a non-zero constant and its degree is equal to c_0. Then, by Proposition 2.3, we get

$$|Y| = h_Y(d) = c_0 = \deg\big(S[u]/I(Y)\big)$$

for $d \geqq |Y| - 1$. Thus, $|Y|$ is the degree of $S[u]/I(Y)$. Hence, from part (b), we get that the length of $C_{X^*}(d)$ is equal to the degree of $S[u]/I(Y)$ and the dimension of $C_{X^*}(d)$ is equal to $H_Y(d)$. □

From this result it follows at once that the codes $C_{X^*}(d)$ and $C_Y(d)$ are equivalent in the sense of [21, p. 48].

REMARK 2.5. If $H_{X^*}(d)$ is the *affine Hilbert function* of the affine K-algebra $S/I(X^*)$, given by

$$H_{X^*}(d) := \dim_K S_{\leqq d}/I(X^*)_{\leqq d},$$

then, by Eq. (2.3), $H_Y(d) = H_{X^*}(d)$ for $d \geqq 1$ (see [13, Remark 5.3.16]).

COROLLARY 2.6. (a) *The dimension of $C_{X^*}(d)$ is increasing, as a function of d, until it reaches a constant value equal to $|X^*|$.*

(b) *The minimum distance of $C_{X^*}(d)$ is decreasing, as a function of d, until it reaches a constant value equal to* 1.

PROOF. The dimension of $C_Y(d)$ is increasing, as a function of d, until it reaches a constant value equal to $|Y|$ (see [7, Remark 1.1, p. 166] or [4, p. 456]). The minimum distance of $C_Y(d)$ is decreasing, as a function of d, until it reaches a constant value equal to 1. This was shown in [16, Proposition 5.1, p. 99] and [23, Proposition 2.1]. Therefore the result follows from Theorem 2.4. □

Next, we give an application by computing the basic parameters of a certain family of parameterized affine codes. Let X^* be an affine algebraic toric set parameterized by $y_1, \ldots, y_s$. In this case we denote X^* by T and Y by $\mathbb{T}$. We call T (resp. $\mathbb{T}$) an *affine* (resp. *projective*) *torus.* Recall that T and $\mathbb{T}$ are given by

$$T = \left\{ (x_1, \ldots, x_s) \mid x_i \in K^* \right\} \subset \mathbb{A}^s \quad \text{and}$$

$$\mathbb{T} = \left\{ \left[(x_1, \ldots, x_s, 1) \right] \mid x_i \in K^* \right\} \subset \mathbb{P}^s,$$

respectively.

COROLLARY 2.7. *The minimum distance of $C_T(d)$ is given by*

$$\delta_T(d) = \begin{cases} (q-1)^{s-k-1}(q-1-\ell) & \text{if } \ d \leqq (q-2)s-1, \\ 1 & \text{if } \ d \geqq (q-2)s, \end{cases}$$

where k and ℓ are the unique integers such that $k \geqq 0$, $1 \leqq \ell \leqq q-2$ and $d = k(q-2)+\ell$.

PROOF. It was shown in [18] that the minimum distance of $C_{\mathbb{T}}(d)$ is given by the formula above. Thus, by Theorem 2.4, the result follows. □

A linear code is called *maximum distance separable* (MDS for short) if equality holds in the Singleton bound (see Eq. (1.2)). As a consequence of this result we obtain the well-known formula for the minimum distance of a Reed–Solomon code [21, p. 42].

COROLLARY 2.8 (Reed–Solomon codes). *Let T be an affine torus in $\mathbb{A}^1$. Then the minimum distance $\delta_T(d)$ of $C_T(d)$ is given by*

$$\delta_T(d) = \begin{cases} q-1-d & \text{if } \ 1 \leqq d \leqq q-3, \\ 1 & \text{if } \ d \geqq q-2, \end{cases}$$

and $C_T(d)$ is an MDS code.

PROOF. In this situation $s = 1$. If $d \leqq q-3$, we can write $d = k(q-2)+\ell$, where $k = 0$ and $\ell = d$. Then, by Corollary 2.7, we get $\delta_T(d) = q-1-d$ for $d \leqq q-3$ and $\delta_T(d) = 1$ for $d \geqq q-2$. □

COROLLARY 2.9. *The length of $C_T(d)$ is $(q-1)^s$ and its dimension is*

$$\dim_K C_T(d) = \sum_{j=0}^{\lfloor \frac{d}{q-1} \rfloor} (-1)^j \binom{s}{j} \binom{s+d-j(q-1)}{s}.$$

PROOF. The length of $C_T(d)$ is clearly equal to $(q-1)^s$ because $T = (K^*)^s$. It was shown in [4] that the dimension of $C_{\mathbb{T}}(d)$ is given by the formula above. Thus, by Theorem 2.4, the result follows. □

EXAMPLE 2.10. Let T be an affine torus in $\mathbb{A}^2$ and let $C_T(d)$ be its parameterized affine code of degree d over the field $K = \mathbb{F}_{11}$. Using Corollaries 2.7 and 2.9, we obtain:

d	1	2	3	4	5	6	7	8	9	10	11	12	13
$\lvert T\rvert$	100	100	100	100	100	100	100	100	100	100	100	100	100
$\dim C_T(d)$	3	6	10	15	21	28	36	45	55	64	72	79	85
$\delta_T(d)$	90	80	70	60	50	40	30	20	10	9	8	7	6

3. Computing the dimension and length of $C_{X^*}(d)$

We continue to use the notation and definitions used in Sections 1 and 2. In this section we give expressions for $I(X^*)$ and $I(Y)$ – valid over any finite field K with q elements – that allow to compute some of the basic parameters of a parameterized affine code using Gröbner bases.

THEOREM 3.1 (Combinatorial Nullstellensatz [1, Theorem 1.2]). *Let $R = K[y_1, \ldots, y_n]$ be a polynomial ring over a field K, let $f \in R$, and let $a = (a_i) \in \mathbb{N}^n$. Suppose that the coefficient of y^a in f is non-zero and $\deg(f) = a_1 + \cdots + a_n$. If $S_1, \ldots, S_n$ are subsets of K, with $|S_i| > a_i$ for all i, then there are $s_1 \in S_1, \ldots, s_n \in S_n$ such that $f(s_1, \ldots, s_n) \neq 0$.*

LEMMA 3.2. *Let $K = \mathbb{F}_q$ and let G be a polynomial in $K[y_1, \ldots, y_n]$. If G vanishes on $(K^*)^n$ and $\deg_{y_i}(G) < q-1$ for $i = 1, \ldots, n$, then $G = 0$.*

PROOF. We proceed by contradiction. Assume that G is non-zero. Then, there is a monomial y^a that occurs in G with $\deg(G) = a_1 + \cdots + a_n$, where $a = (a_1, \ldots, a_n)$ and $a_i > 0$ for some i. We set $S_i = K^*$ for all i. As $\deg_{y_i}(G) < q-1$ for all i, then $a_i < |S_i| = q-1$ for all i. Thus, by Lemma 3.1,

there are $x_1, \ldots, x_n \in K^*$ so that $G(x_1, \ldots, x_n) \neq 0$, a contradiction to the fact that G vanishes on $(K^*)^n$. □

A polynomial of the form $t^a - t^b$, with $a, b \in \mathbb{N}^s$, is called a *binomial* of S. An ideal generated by binomials is called a *binomial ideal.*

LEMMA 3.3. *Let $B = K[t_1, \ldots, t_s, y_1, \ldots, y_n]$ be a polynomial ring over an arbitrary field K. If I' is a binomial ideal of B, then $I' \cap K[t_1, \ldots, t_s]$ is a binomial ideal.*

PROOF. Let $S = K[t_1, \ldots, t_s]$ and let $\mathcal{G}$ be a Gröbner basis of I' with respect to the lexicographic order $y_1 \succ \cdots \succ y_n \succ t_1 \succ \cdots \succ t_s$. By Buchberger algorithm [2, Theorem 2, p. 89] the set $\mathcal{G}$ consists of binomials and by elimination theory [2, Theorem 2, p. 114] the set $\mathcal{G} \cap S$ is a Gröbner basis of $I' \cap S$. Hence $I' \cap S$ is a binomial ideal. See the proof of [22, Corollary 4.4, p. 32] for additional details. □

THEOREM 3.4. *Let $B = K[t_1, \ldots, t_s, y_1, \ldots, y_n]$ be a polynomial ring over a finite field K with q elements. Then*

$$I(X^*) = \left(t_1 - y^{v_1}, \ldots, t_s - y^{v_s}, y_1^{q-1} - 1, \ldots, y_n^{q-1} - 1\right) \cap S$$

and $I(X^*)$ is a binomial ideal.

PROOF. We set $I' = \left(t_1 - y^{v_1}, \ldots, t_s - y^{v_s}, y_1^{q-1} - 1, \ldots, y_n^{q-1} - 1\right) \subset B$. First we show the inclusion $I(X^*) \subset I' \cap S$. Take a polynomial $F = F(t_1, \ldots, t_s)$ that vanishes on X^*. We can write

$$F = \lambda_1 t^{m_1} + \cdots + \lambda_r t^{m_r} \quad (\lambda_i \in K^*;\ m_i \in \mathbb{N}^s). \tag{3.1}$$

Write $m_i = (m_{i1}, \ldots, m_{is})$ for $1 \leqq i \leqq r$. Applying the binomial theorem to expand the right hand side of the equality

$$t_j^{m_{ij}} = \left[\left(t_j - y^{v_j}\right) + y^{v_j}\right]^{m_{ij}}, \quad 1 \leqq i \leqq r,\ 1 \leqq j \leqq s,$$

we get the equality

$$t_j^{m_{ij}} = \left(\sum_{k=0}^{m_{ij}-1} \binom{m_{ij}}{k} \left(\left(t_j - y^{v_j}\right)^{m_{ij}-k} \left(y^{v_j}\right)^k\right)\right) + \left(y^{v_j}\right)^{m_{ij}}.$$

As a result, we obtain that t^{m_i} can be written as:

$$t^{m_i} = t_1^{m_{i1}} \cdots t_s^{m_{is}} = p_i + (y^{v_1})^{m_{i1}} \cdots \left(y^{v_s}\right)^{m_{is}},$$

where p_i is a polynomial in the ideal $\big(t_1 - y^{v_1}, \ldots, t_s - y^{v_s}\big)$. Thus, substituting $t^{m_1}, \ldots, t^{m_r}$ in Eq. (3.1), we obtain that F can be written as:

$$F = \sum_{i=1}^{s} g_i\big(t_i - y^{v_i}\big) + F\big(y^{v_1}, \ldots, y^{v_s}\big) \tag{3.2}$$

for some $g_1, \ldots, g_s$ in B. By the division algorithm in $K[y_1, \ldots, y_n]$ (see [2, Theorem 3, p. 63]) we can write

$$F\big(y^{v_1}, \ldots, y^{v_s}\big) = \sum_{i=1}^{n} h_i\big(y_i^{q-1} - 1\big) + G(y_1, \ldots, y_n) \tag{3.3}$$

for some $h_1, \ldots, h_n$ in $K[y_1, \ldots, y_n]$, where the monomials that occur in $G = G(y_1, \ldots, y_n)$ are not divisible by any of the monomials $y_1^{q-1}, \ldots, y_n^{q-1}$, i.e., $\deg_{y_i}(G) < q - 1$ for $i = 1, \ldots, n$. Therefore, using Eqs. (3.2) and (3.3), we obtain the equality

$$F = \sum_{i=1}^{s} g_i\big(t_i - y^{v_i}\big) + \sum_{i=1}^{n} h_i\big(y_i^{q-1} - 1\big) + G(y_1, \ldots, y_n). \tag{3.4}$$

Thus to show that $F \in I' \cap S$ we need only show that $G = 0$. We claim that G vanishes on $(K^*)^n$. Take an arbitrary sequence $x_1, \ldots, x_n$ of elements of K^*. Making $t_i = x^{v_i}$ for all i in Eq. (3.4) and using that F vanishes on X^*, we obtain

$$\begin{aligned} 0 &= F\big(x^{v_1}, \ldots, x^{v_s}\big) \\ &= \sum_{i=1}^{s} g_i'\big(x^{v_i} - y^{v_i}\big) + \sum_{i=1}^{n} h_i\big(y_i^{q-1} - 1\big) + G(y_1, \ldots, y_n), \end{aligned} \tag{3.5}$$

where $g_i' = g_i(x^{v_1}, \ldots, x^{v_s}, y_1, \ldots, y_n)$. Since $(K^*, \cdot\,)$ is a group of order $q - 1$, we can then make $y_i = x_i$ for all i in Eq. (3.5) to get that G vanishes on $(x_1, \ldots, x_n)$. This completes the proof of the claim. Therefore G vanishes on $(K^*)^n$ and $\deg_{y_i}(G) < q - 1$ for all i. Hence $G = 0$ by Lemma 3.2.

Next we show the inclusion $I(X^*) \supset I' \cap S$. Take a polynomial f in $I' \cap S$. Then we can write

$$f = \sum_{i=1}^{s} g_i\big(t_i - y^{v_i}\big) + \sum_{i=1}^{n} h_i\big(y_i^{q-1} - 1\big) \tag{3.6}$$

for some polynomials $g_1, \ldots, g_s, h_1, \ldots, h_n$ in B. Take a point $P = \big(x^{v_1}, \ldots, x^{v_s}\big)$ in X^*. Making $t_i = x^{v_i}$ in Eq. (3.6), we get

$$f\big(x^{v_1}, \ldots, x^{v_s}\big) = \sum_{i=1}^{s} g_i'\big(x^{v_i} - y^{v_i}\big) + \sum_{i=1}^{n} h_i'\big(y_i^{q-1} - 1\big),$$

where $g_i' = g_i\big(x^{v_1}, \ldots, x^{v_s}, y_1, \ldots, y_n\big)$ and $h_i' = h_i\big(x^{v_1}, \ldots, x^{v_s}, y_1, \ldots, y_n\big)$. Hence making $y_i = x_i$ for all i, we get that $f(P) = 0$. Thus f vanishes on X^*. □

In this paper we are always working over a finite field K. If $K = \mathbb{C}$ is the field of complex numbers and X is an affine toric variety, i.e.,

$$X = V(\mathfrak{p}) = \big\{ P \in K^n \mid f(P) = 0 \text{ for all } f \in \mathfrak{p} \big\}$$

is the *zero set* of a toric ideal $\mathfrak{p}$, then by the Nullstellensatz [5, Theorem 1.6] we have that $I(X) = \mathfrak{p}$. This means that $I(X)$ is a binomial ideal. For infinite fields, we can use the Combinatorial Nullstellensatz (see Theorem 3.1) to show the following description of $I(X^*)$. We refer to [22] for the theory of toric ideals.

PROPOSITION 3.5. *Let $B = K[t_1, \ldots, t_s, y_1, \ldots, y_n]$ be a polynomial ring over an infinite field K. Then*

$$I(X^*) = \big(t_1 - y^{v_1}, \ldots, t_s - y^{v_s}\big) \cap S$$

and $I(X^*)$ is the toric ideal of $K\big[y^{v_1}, \ldots, y^{v_s}\big]$.

Our next aim is to show how to compute $I(Y)$. For $f \in S$ of degree e define

$$f^h = u^e f(t_1/u, \ldots, t_s/u),$$

that is, f^h is the *homogenization* of the polynomial f with respect to u. The *homogenization* of $I(X^*) \subset S$ is the ideal $I(X^*)^h$ of $S[u]$ given by

$$I(X^*)^h = \big(\big\{ f^h \mid f \in I(X^*) \big\}\big).$$

Let $\succ$ be the *elimination order* on the monomials of $S[u]$ with respect to $t_1, \ldots, t_s, t_{s+1}$, where $u = t_{s+1}$. Recall that this order is defined as $t^b \succ t^a$ if and only if the total degree of t^b in the variables $t_1, \ldots, t_{s+1}$ is greater than that of t^a, or both degrees are equal, and the last nonzero component of $b - a$ is negative.

DEFINITION 3.6. The *projective closure* of X^*, denoted by $\overline{X^*}$, is given by $\overline{X^*} := \overline{Y}$, where $\overline{Y}$ is the closure of Y in the Zariski topology of $\mathbb{P}^s$.

LEMMA 3.7. *If $f_1, \ldots, f_r$ is a Gröbner basis of $I(X^*)$, then $f_1^h, \ldots, f_r^h$ form a Gröbner basis and the following equalities hold:*

$$I(Y) = I(X^*)^h = \left(f_1^h, \ldots, f_r^h\right).$$

PROOF. In our situation $\overline{X^*} = \overline{Y} = Y$ because K is a finite field. Thus, the result follows readily from [25, Propositions 2.4.26 and 2.4.30]. □

COROLLARY 3.8. *The dimension and the length of $C_{X^*}(d)$ can be computed using Gröbner basis.*

PROOF. By Lemma 3.7 we can find a generating set of $I(Y)$ using Gröbner basis. Thus, using the computer algebra system *Macaulay*2 [6, 12], we can compute the Hilbert function and the degree of $S[u]/I(Y)$, i.e., we can compute the dimension and the length of $C_Y(d)$. Consequently, Theorem 2.4 allows to compute the dimension and the length of $C_{X^*}(d)$ using Gröbner basis. □

Putting the results of this section together we obtain the following procedure.

PROCEDURE 3.9. The following simple procedure for *Macaulay*2 computes the dimension and the length of a parameterized affine code $C_{X^*}(d)$ of degree d.

```
R=GF(q)[y1,...,yn,t1,...,ts,u,MonomialOrder=>Eliminate n]
I'=ideal(t1-y1^{v_1},...,t_s-y^{s},y1^{q-1}-1,...,yn^{q-1}-1)
I(X^*)=ideal selectInSubring(1,gens gb I')
I(Y)'=homogenize(I(X^*),u)
S=GF(q)[t1,...,ts,u]
I(Y)=substitute(I(Y)',S)
degree I(Y)
hilbertFunction(d,I(Y))
```

EXAMPLE 3.10. Let X^* be the affine algebraic toric set parameterized by y_1y_2, y_2y_3, y_1y_3 and let $C_{X^*}(d)$ be its parameterized affine code of order d over the field $K = \mathbb{F}_5$. Using *Macaulay*2, together with Procedure 3.9, we obtain:

$$I(X^*) = \left(t_3^4 - 1, t_2^2t_3^2 - t_1^2, t_1^2t_3^2 - t_2^2, t_2^4 - 1, t_1^2t_2^2 - t_3^2, t_1^4 - 1\right),$$

$$I(Y) = \left(t_3^4 - t_4^4, t_2^2t_3^2 - t_1^2t_4^2, t_1^2t_3^2 - t_2^2t_4^2, t_2^4 - t_4^4, t_1^2t_2^2 - t_3^2t_4^2, t_1^4 - t_4^4\right),$$

d	1	2	3	4	5
$\lvert X^*\rvert$	32	32	32	32	32
$\dim C_{X^*}(d)$	4	10	20	29	32
$\delta_{X^*}(d)$	23	8			1

The minimum distance was also computed with *Macaulay*2.

Acknowledgment. We thank the referee for the careful reading of the paper and for the improvements that he/she suggested.

REFERENCES

[1] Alon, N., Combinatorial Nullstellensatz, Recent trends in combinatorics (Mátraháza, 1995), *Combin. Probab. Comput.,* **8** (1999), no. 1–2, 7–29.

[2] Cox, D. Little, J. and O'Shea, D., *Ideals, Varieties, and Algorithms,* Springer-Verlag, 1992.

[3] Delsarte, P., Goethals, J. M. and F. J. MacWilliams, On generalized Reed-Muller codes and their relatives, *Information and Control,* **16** (1970), 403–442.

[4] Duursma, I. M., Rentería, C. and Tapia-Recillas, H., Reed–Muller codes on complete intersections, *Appl. Algebra Engrg. Comm. Comput.,* **11** (2001), no. 6, 455–462.

[5] Eisenbud, D., *Commutative Algebra with a view toward Algebraic Geometry,* Graduate Texts in Mathematics **150**, Springer-Verlag, 1995.

[6] Eisenbud, D., Grayson, D. R. and Stillman, M., eds., *Computations in algebraic geometry with Macaulay 2,* Algorithms and Computation in Mathematics **8**, Springer-Verlag, Berlin, 2002.

[7] Geramita, A. V., Kreuzer, M. and Robbiano, L., Cayley–Bacharach schemes and their canonical modules, *Trans. Amer. Math. Soc.,* **339** (1993), no. 1, 163–189.

[8] Gold, L., Little, J. and Schenck, H., Cayley–Bacharach and evaluation codes on complete intersections, *J. Pure Appl. Algebra,* **196** (2005), no. 1, 91–99.

[9] González-Sarabia, M. and Rentería, C., Evaluation codes associated to complete bipartite graphs, *Int. J. Algebra,* **2** (2008), no. 1–4, 163–170.

[10] González-Sarabia, M., Rentería, C. and Hernández de la Torre, M., Minimum distance and second generalized Hamming weight of two particular linear codes, *Congr. Numer.,* **161** (2003), 105–116.

[11] González-Sarabia, M., Rentería, C. and Tapia-Recillas, H., Reed–Muller-type codes over the Segre variety, *Finite Fields Appl.,* **8** (2002), no. 4, 511–518.

[12] Grayson, D. and Stillman, M., *Macaulay*2, 1996. Available via anonymous ftp from `math.uiuc.edu`.

[13] Greuel, G. M. and Pfister, G., *A Singular Introduction to Commutative Algebra,* 2nd extended edition, Springer, Berlin, 2008.

[14] Harris, J., *Algebraic Geometry. A first course,* Graduate Texts in Mathematics, **133**, Springer-Verlag, New York, 1992.

[15] MacWilliams, F. J. and Sloane, N. J. A., The Theory of Error-correcting Codes, North-Holland, 1977.

[16] Rentería, C., Simis, A. and Villarreal, R. H., Algebraic methods for parameterized codes and invariants of vanishing ideals over finite fields, *Finite Fields Appl.,* **17** (2011), no. 1, 81–104.

[17] Rentería, C. and Tapia-Recillas, H., Reed–Muller codes: an ideal theory approach, *Comm. Algebra,* **25** (1997), no. 2, 401–413.

[18] Sarmiento, E., Vaz Pinto, M. and Villarreal, R. H., The minimum distance of parameterized codes on projective tori, *Appl. Algebra Engrg. Comm. Comput.,* **22** (2011), no. 4, 249–264.

[19] Sørensen, A., Projective Reed–Muller codes, *IEEE Trans. Inform. Theory,* **37** (1991), no. 6, 1567–1576.

[20] Stanley, R., Hilbert functions of graded algebras, *Adv. Math.,* **28** (1978), 57–83.

[21] Stichtenoth, H., *Algebraic function fields and codes,* Universitext, Springer-Verlag, Berlin, 1993.

[22] Sturmfels, B., *Gröbner Bases and Convex Polytopes,* University Lecture Series **8**, American Mathematical Society, Rhode Island, 1996.

[23] Tohăneanu, S., Lower bounds on minimal distance of evaluation codes, *Appl. Algebra Engrg. Comm. Comput.,* **20** (2009), no. 5–6, 351–360.

[24] Tsfasman, M., Vladut, S. and Nogin, D., *Algebraic geometric codes: basic notions,* Mathematical Surveys and Monographs **139**, American Mathematical Society, Providence, RI, 2007.

[25] Villarreal, R. H., *Monomial Algebras,* Monographs and Textbooks in Pure and Applied Mathematics, **238**, Marcel Dekker, New York, 2001.