Bull. Malays. Math. Sci. Soc. (2018) 41:81–89
https://doi.org/10.1007/s40840-015-0239-5

BULLETIN of the MALAYSIAN MATHEMATICAL SCIENCES SOCIETY
http://www.springer.com/mathematics/journal/40840

Complete Intersection Vanishing Ideals on Sets of Clutter Type over Finite Fields

Azucena Tochimani[1] · **Rafael H. Villarreal**[1]

Received: 1 April 2015 / Revised: 20 September 2015 / Published online: 16 October 2015

Abstract In this paper, we give a classification of complete intersection vanishing ideals on parameterized sets of clutter type over finite fields.

Keywords Complete intersection · Monomial parameterization · Vanishing ideal · Binomial ideal · Finite field

Mathematics Subject Classification Primary 14M10; Secondary 14G15 · 13P25 · 13P10 · 11T71

1 Introduction

Let $R = \mathbb{F}_q[\mathbf{y}] = \mathbb{F}_q[y_1, \ldots, y_n]$ be a polynomial ring over a finite field $\mathbb{F}_q$ and let $y^{v_1}, \ldots, y^{v_s}$ be a finite set of monomials in $\mathbb{F}_q[\mathbf{y}]$. As usual we denote the affine and projective spaces over the field $\mathbb{F}_q$ of dimensions s and $s-1$ by $\mathbb{A}^s$ and $\mathbb{P}^{s-1}$, respectively. Points of the projective space $\mathbb{P}^{s-1}$ are denoted by $[\alpha]$, where $0 \neq \alpha \in \mathbb{A}^s$.

Communicated by Anton Abdulbasah Kamil.

Azucena Tochimani was partially supported by CONACyT. Rafael H. Villarreal was partially supported by SNI.

✉ Rafael H. Villarreal
vila@math.cinvestav.mx

Azucena Tochimani
tochimani@math.cinvestav.mx

1 Departamento de Matemáticas, Centro de Investigación y de Estudios Avanzados del IPN, Apartado Postal 14–740, 07000 Mexico City, DF, Mexico

We consider a set $\mathbb{X}$, in the projective space $\mathbb{P}^{s-1}$, parameterized by $y^{v_1}, \ldots, y^{v_s}$. The set $\mathbb{X}$ consists of all points $[(x^{v_1}, \ldots, x^{v_s})]$ in $\mathbb{P}^{s-1}$ that are well defined, i.e., $x \in \mathbb{F}_q^n$ and $x^{v_i} \neq 0$ for some i. The set $\mathbb{X}$ is called of *clutter type* if $\mathrm{supp}(y^{v_i}) \not\subset \mathrm{supp}(y^{v_j})$ for $i \neq j$, where $\mathrm{supp}(y^{v_i})$ is the *support* of the monomial y^{v_i} consisting of the variables that occur in y^{v_i}. In this case, we say that the set of monomials $y^{v_1}, \ldots, y^{v_s}$ is of *clutter type*. This terminology comes from the fact that the condition $\mathrm{supp}(y^{v_i}) \not\subset \mathrm{supp}(y^{v_j})$ for $i \neq j$ means that there is a *clutter* $\mathcal{C}$, in the sense of [14], with vertex set $V(\mathcal{C}) = \{y_1, \ldots, y_n\}$ and edge set

$$E(\mathcal{C}) = \{\mathrm{supp}(y^{v_1}), \ldots, \mathrm{supp}(y^{v_s})\}.$$

A clutter is also called a *simple hypergraph*, see Definition 2.8.

Let $S = \mathbb{F}_q[t_1, \ldots, t_s] = \oplus_{d=0}^{\infty} S_d$ be a polynomial ring over the field $\mathbb{F}_q$ with the standard grading. The graded ideal $I(\mathbb{X})$ generated by the homogeneous polynomials of S that vanish at all points of $\mathbb{X}$ is called the *vanishing ideal* of $\mathbb{X}$.

There are good reasons to study vanishing ideals over finite fields. They are used in algebraic coding theory [8] and in polynomial interpolation problems [5,18]. The Reed–Muller-type codes arising from vanishing ideals on monomial parameterizations have received a lot of attention [1,3,6,8,10,13,14,16].

The vanishing ideal $I(\mathbb{X})$ is a *complete intersection* if $I(\mathbb{X})$ is generated by $s-1$ homogeneous polynomials. Notice that $s-1$ is the height of $I(\mathbb{X})$ in the sense of [12]. The interest in complete intersection vanishing ideals over finite fields comes from information and communication theory, and algebraic coding theory [4,7,9].

Let T be a projective torus in $\mathbb{P}^{s-1}$ (see Definition 2.15) and let $\mathbb{X}$ be the set in $\mathbb{P}^{s-1}$ parameterized by a clutter $\mathcal{C}$ (see Definition 2.9). Consider the set $X = \mathbb{X} \cap T$. In [14] it is shown that $I(X)$ is a complete intersection if and only if X is a projective torus in $\mathbb{P}^{s-1}$. If the clutter $\mathcal{C}$ has all its edges of the same cardinality, in [15] a classification of the complete intersection property of $I(X)$ is given using linear algebra.

The main result of this paper is a classification of the complete intersection property of $I(\mathbb{X})$ when $\mathbb{X}$ is of clutter type (Theorem 2.19). Using the techniques of [13], this classification can be used to study the *basic parameters* [11,19] of the Reed–Muller-type codes associated to $\mathbb{X}$.

For all unexplained terminology and additional information, we refer to [12] (for commutative algebra), [2] (for Gröbner bases), and [13,18,19] (for vanishing ideals and coding theory).

2 Complete Intersections

In this section, we give a full classification of the complete intersection property of vanishing ideals of sets of clutter type over finite fields. We continue to employ the notations and definitions used in Sect. 1.

Throughout this section $\mathbb{F}_q$ is a finite field, $y^{v_1}, \ldots, y^{v_s}$ are distinct monomials in the polynomial ring $R = \mathbb{F}_q[\mathbf{y}] = \mathbb{F}_q[y_1, \ldots, y_n]$, with $v_i = (v_{i1}, \ldots, v_{in})$ and $y^{v_i} = y_1^{v_{i1}} \cdots y_n^{v_{in}}$ for $i = 1, \ldots, s$, $\mathbb{X}$ is the set in $\mathbb{P}^{s-1}$ parameterized by these monomials, and $I(\mathbb{X})$ is the vanishing ideal of $\mathbb{X}$. Recall that $I(\mathbb{X})$ is the graded ideal of the polynomial ring $S = \mathbb{F}_q[t_1, \ldots, t_s]$ generated by the homogeneous polynomials of S that vanish on $\mathbb{X}$.

Definition 2.1 Given $a = (a_1, \ldots, a_n) \in \mathbb{N}^n$, we set $y^a := y_1^{a_1} \cdots y_n^{a_n}$. The *support* of y^a, denoted $\mathrm{supp}(y^a)$, is the set of all y_i such that $a_i > 0$.

Definition 2.2 The set $\mathbb{X}$ is of *clutter type* if $\mathrm{supp}(y^{v_i}) \not\subset \mathrm{supp}(y^{v_j})$ for $i \neq j$.

Definition 2.3 A *binomial* of S is an element of the form $f = t^a - t^b$, for some a, b in $\mathbb{N}^s$. An ideal generated by binomials is called a *binomial ideal*.

The set $\mathcal{S} = \mathbb{P}^{s-1} \cup \{[0]\}$ is a monoid under componentwise multiplication, that is, given $[\alpha] = [(\alpha_1, \ldots, \alpha_s)]$ and $[\beta] = [(\beta_1, \ldots, \beta_s)]$ in $\mathcal{S}$, the operation of this monoid is given by

$$[\alpha] \cdot [\beta] = [\alpha_1\beta_1, \ldots, \alpha_s\beta_s],$$

where $[\mathbf{1}] = [(1, \ldots, 1)]$ is the identity element.

Theorem 2.4 ([17, Corollary 3.7]) *If $\mathbb{F}_q$ is a finite field and $\mathbb{Y}$ is a subset of $\mathbb{P}^{s-1}$, then $I(\mathbb{Y})$ is a binomial ideal if and only if $\mathbb{Y} \cup \{[0]\}$ is a submonoid of $\mathbb{P}^{s-1} \cup \{[0]\}$.*

Remark 2.5 Since $\mathbb{X}$ is parameterized by monomials, the set $\mathbb{X} \cup \{[0]\}$ is a monoid under componentwise multiplication. Hence, by Theorem 2.4, $I(\mathbb{X})$ is a binomial ideal.

Lemma 2.6 *Let $y^{v_1}, \ldots, y^{v_s}$ be a set of monomials such that $\mathrm{supp}(y^{v_i}) \not\subset \mathrm{supp}(y^{v_j})$ for any $i \neq j$ and let $\mathcal{G}$ be a minimal generating set of $I(\mathbb{X})$ consisting of binomials. The following hold.*

(a) If $0 \neq f = t_j^{a_j} - t^c$ for some $1 \leq j \leq s$, some positive integer a_j, and some $c \in \mathbb{N}^s$, then $f \notin I(\mathbb{X})$.
(b) For each pair $1 \leq i < j \leq s$, there is g_{ij} in $\mathcal{G}$ such that $g_{ij} = \pm(t_i^{c_{ij}} t_j - t^{b_{ij}})$, where c_{ij} is a positive integer less than or equal to q and $b_{ij} \in \mathbb{N}^s \setminus \{0\}$.
(c) For each pair $1 \leq i < j \leq s$, there is h_{ij} in $\mathcal{G}$ such that $h_{ij} = \pm(t_i t_j^{a_{ij}} - t^{e_{ij}})$, where a_{ij} is a positive integer less than or equal to q and $e_{ij} \in \mathbb{N}^s \setminus \{0\}$.
(d) If $I(\mathbb{X})$ is a complete intersection, then $s \leq 4$.

Proof (a) We proceed by contradiction. Assume that f is in $I(\mathbb{X})$. Since $I(\mathbb{X})$ is a graded binomial ideal, the binomial f is homogeneous of degree a_j, otherwise $t_j^{a_j}$ and t^c would be in $I(\mathbb{X})$ which is impossible. Thus $c \in \mathbb{N}^s \setminus \{0\}$. Hence, as $f \neq 0$, we can pick $t_i \in \mathrm{supp}(t^c)$ with $i \neq j$. By hypothesis there is $y_k \in \mathrm{supp}(y^{v_i}) \setminus \mathrm{supp}(y^{v_j})$, i.e., $v_{ik} > 0$ and $v_{jk} = 0$. Making $y_k = 0$ and $y_\ell = 1$ for $\ell \neq k$, we get that $f(y^{v_1}, \ldots, y^{v_s}) = 1$, a contradiction.

(b) The binomial $h = t_i^q t_j - t_i t_j^q$ vanishes at all points of $\mathbb{P}^{s-1}$, i.e., h is in $I(\mathbb{X})$. Thus there is g_{ij} in $\mathcal{G}$ such that $t_i^q t_j$ is a multiple of one of the two terms of the binomial g_{ij}. Hence, by part (a), the assertion follows.

(c) Since $h = t_i^q t_j - t_i t_j^q$ is in $I(\mathbb{X})$, there is h_{ij} in $\mathcal{G}$ such that $t_i t_j^q$ is a multiple of one of the two terms of the binomial h_{ij}. Hence, by part (a), the assertion follows.

(d) Since $I(\mathbb{X})$ is a complete intersection, there is a set of binomials $\mathcal{G} = \{g_1, \ldots, g_{s-1}\}$ that generate $I(\mathbb{X})$. The number of monomials that occur in $g_1, \ldots, g_{s-1}$ is at most $2(s-1)$. Thanks to part (b) for each pair $1 \leq i < j \leq s$, there is a monomial $t_i^{c_{ij}} t_j$, with $c_{ij} \in \mathbb{N}_+$, and a binomial g_{ij} in $\mathcal{G}$ such that the monomial $t_i^{c_{ij}} t_j$ occurs in g_{ij}. As there are at least $s(s-1)/2$ of these monomials, we get $s(s-1)/2 \leq 2(s-1)$. Thus $s \leq 4$. □

Lemma 2.7 *Let K be a field and let I be the ideal of $S = K[t_1, t_2, t_3, t_4]$ generated by the binomials $g_1 = t_1t_2 - t_3t_4$, $g_2 = t_1t_3 - t_2t_4$, $g_3 = t_2t_3 - t_1t_4$. The following hold.*

(i) $\mathcal{G} = \{t_2t_3 - t_1t_4, t_1t_3 - t_2t_4, t_1t_2 - t_3t_4, t_2^2t_4 - t_3^2t_4, t_1^2t_4 - t_3^2t_4, t_3^3t_4 - t_3t_4^3\}$ *is a Gröbner basis of I with respect to the GRevLex order $\prec$ on S.*
(ii) If $\mathrm{char}(K) = 2$, *then* $\mathrm{rad}(I) \neq I$.
(iii) If $\mathrm{char}(K) \neq 2$ *and e_i is the i-th unit vector, then $I = I(\mathbb{X})$, where*

$$\mathbb{X} = \{[e_1], [e_2], [e_3], [e_4], [(1, -1, -1, 1)], [(1, 1, 1, 1)], [(-1, -1, 1, 1)], [(-1, 1, -1, 1)]\}.$$

Proof (i) Using Buchberger's criterion [2, p. 84], it is seen that $\mathcal{G}$ is a Gröbner basis of I.

(ii) Setting $h = t_1t_2 - t_1t_3$, we get $h^2 = (t_1t_2)^2 - (t_1t_3)^2 = t_1t_2g_1 + t_1t_3g_2$, where $g_1 = t_1t_2 - t_3t_4$ and $g_2 = t_1t_3 - t_2t_4$. Thus $h \in \mathrm{rad}(I)$. Using part (i) it is seen that $h \notin I$.

(iii) As g_i vanishes at all points of $\mathbb{X}$ for $i = 1, 2, 3$, we get the inclusion $I \subset I(\mathbb{X})$. Since $\mathbb{X} \cup \{0\}$ is a monoid under componentwise multiplication, by Theorem 2.4, $I(\mathbb{X})$ is a binomial ideal. Take a homogeneous binomial f in S that vanishes at all points of $\mathbb{X}$. Let $h = t^a - t^b$, $a = (a_i)$, $b = (b_i)$, be the residue obtained by dividing f by $\mathcal{G}$. Hence we can write $f = g + h$, where $g \in I$ and the terms t^a and t^b are not divisible by any of the leading terms of $\mathcal{G}$. It suffices to show that $h = 0$. Assume that $h \neq 0$. As $h \in I(\mathbb{X})$ and $[e_i]$ is in $\mathbb{X}$ for all i, we get that $|\mathrm{supp}(t^a)| \geq 2$ and $|\mathrm{supp}(t^b)| \geq 2$. It follows that h has one of the following forms:

$$h = t_1t_4^i - t_2t_4^i, \qquad h = t_1t_4^i - t_3t_4^i, \qquad h = t_2t_4^i - t_3t_4^i,$$
$$h = t_3^2t_4^{i-1} - t_3t_4^i, \qquad h = t_3^2t_4^{i-1} - t_2t_4^i, \qquad h = t_3^2t_4^{i-1} - t_1t_4^i,$$

where $i \geq 1$, a contradiction because none of these binomials vanishes at all points of $\mathbb{X}$. □

Definition 2.8 A *hypergraph* $\mathcal{H}$ is a pair $(V(\mathcal{H}), E(\mathcal{H}))$ such that $V(\mathcal{H})$ is a finite set and $E(\mathcal{H})$ is a subset of the set of all subsets of $V(\mathcal{H})$. The elements of $E(\mathcal{H})$ and $V(\mathcal{H})$ are called *edges* and *vertices*, respectively. A hypergraph is *simple* if $f_1 \not\subset f_2$ for any two edges f_1, f_2. A simple hypergraph is called a *clutter* and will be denoted by $\mathcal{C}$ instead of $\mathcal{H}$.

One example of a clutter is a graph with the vertices and edges defined in the usual way.

Definition 2.9 Let $\mathcal{C}$ be a *clutter* with vertex set $V(\mathcal{C}) = \{y_1, \ldots, y_n\}$, let $f_1, \ldots, f_s$ be the edges of $\mathcal{C}$ and let $v_k = \sum_{x_i \in f_k} e_i$ be the *characteristic vector* of f_k for $1 \leq k \leq s$, where e_i is the i-th unit vector. The set in the projective space $\mathbb{P}^{s-1}$ parameterized by $y^{v_1}, \ldots, y^{v_s}$, denoted by $\mathbb{X}_{\mathcal{C}}$, is called the *projective set parameterized* by $\mathcal{C}$.

Lemma 2.10 *Let $\mathbb{F}_q$ be a finite field with $q \neq 2$ elements, let $\mathcal{C}$ be a clutter with vertices $y_1, \ldots, y_n$, let $v_1, \ldots, v_s$ be the characteristic vectors of the edges of $\mathcal{C}$ and let $\mathbb{X}_{\mathcal{C}}$ be the projective set parameterized by $\mathcal{C}$. If $f = t_i t_j - t_k t_\ell \in I(\mathbb{X}_{\mathcal{C}})$, with i, j, k, l distinct, then $y^{v_i} y^{v_j} = y^{v_k} y^{v_\ell}$.*

Proof For simplicity assume that $f = t_1 t_2 - t_3 t_4$. Setting $A_1 = \text{supp}(y^{v_1} y^{v_2})$, $A_2 = \text{supp}(y^{v_3} y^{v_4})$, $S_1 = \text{supp}(y^{v_1}) \cap \text{supp}(y^{v_2})$, and $S_2 = \text{supp}(y^{v_3}) \cap \text{supp}(y^{v_4})$, it suffices to show the equalities $A_1 = A_2$ and $S_1 = S_2$. If $A_1 \not\subset A_2$, pick $y_k \in A_1 \setminus A_2$. Making $y_k = 0$ and $y_\ell = 1$ for $\ell \neq k$, and using that f vanishes on $\mathbb{X}_{\mathcal{C}}$, we get that $f(y^{v_1}, \ldots, y^{v_4}) = -1 = 0$, a contradiction. Thus $A_1 \subset A_2$. The other inclusion follows by a similar reasoning. Next we show the equality $S_1 = S_2$. If $S_1 \not\subset S_2$, pick a variable $y_k \in S_1 \setminus S_2$. Let β be a generator of the cyclic group $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. Making $y_k = \beta$, $y_\ell = 1$ for $\ell \neq k$, and using that f vanishes on $\mathbb{X}_{\mathcal{C}}$ and the equality $A_1 = A_2$, we get that $f(y^{v_1}, \ldots, y^{v_4}) = \beta^2 - \beta = 0$. Hence $\beta^2 = \beta$ and $\beta = 1$, a contradiction because $q \neq 2$. Thus $S_1 \subset S_2$. The other inclusion follows by a similar argument. □

Remark 2.11 Let $\mathbb{F}_q$ be a finite field with q odd and let $\mathbb{X}$ be the set of clutter type in $\mathbb{P}^3$ parameterized by the following monomials:

$$\begin{aligned}
y^{v_1} &= y_1^{q-1} y_2^r y_3^r y_4^{q-1} y_5^{q-1} y_6^{q-1} y_7^{q-1},\\
y^{v_2} &= y_1^r y_2^r y_3^{q-1} y_4^{q-1} y_5^{q-1} y_6^{q-1} y_8^{q-1},\\
y^{v_3} &= y_1^r y_2^{q-1} y_3^r y_4^{q-1} y_5^{q-1} y_7^{q-1} y_8^{q-1},\\
y^{v_4} &= y_1^{q-1} y_2^{q-1} y_3^{q-1} y_4^{q-1} y_6^{q-1} y_7^{q-1} y_8^{q-1},
\end{aligned}$$

where $r = (q-1)/2$. Then

$$\begin{aligned}
\mathbb{X} = \{&[e_1], [e_2], [e_3], [e_4], [(1, -1, -1, 1)],\\
&[(1, 1, 1, 1)], [(-1, -1, 1, 1)], [(-1, 1, -1, 1)]\},
\end{aligned}$$

$|\mathbb{X}| = 8$ and $I(\mathbb{X}) = (t_1 t_2 - t_3 t_4, t_1 t_3 - t_2 t_4, t_2 t_3 - t_1 t_4)$.

Below we show that the set $\mathbb{X}$ of Remark 2.11 cannot be parameterized by a clutter.

Remark 2.12 Let $\mathbb{F}_q$ be a finite field with $q \neq 2$ elements. Then the ideal

$$I = (t_1 t_2 - t_3 t_4, t_1 t_3 - t_2 t_4, t_2 t_3 - t_1 t_4)$$

cannot be the vanishing ideal of a set in $\mathbb{P}^3$ parameterized by a clutter. Indeed assume that there is a clutter $\mathcal{C}$ such that $I = I(\mathbb{X}_{\mathcal{C}})$ and $\mathbb{X}_{\mathcal{C}} \subset \mathbb{P}^3$. If $v_1, \ldots, v_4$ are the characteristic vectors of the edges of $\mathcal{C}$. Then, by Lemma 2.10, we get $v_1 + v_2 = v_3 + v_4$, $v_1 + v_3 = v_2 + v_4$ and $v_2 + v_3 = v_1 + v_4$. It follows that $v_1 = v_2 = v_3 = v_4$, a contradiction.

Lemma 2.13 *Let K be a field and let I be the ideal of $S = K[t_1, t_2, t_3]$ generated by the binomials $g_1 = t_1t_2 - t_2t_3$, $g_2 = t_1t_3 - t_2t_3$. The following hold.*

(i) $\mathcal{G} = \{t_1t_3 - t_2t_3,\ t_1t_2 - t_2t_3,\ t_2^2t_3 - t_2t_3^2\}$ is a Gröbner basis of I with respect to the GRevLex order $\prec$ on S.

(ii) $I = I(\mathbb{X})$, where $\mathbb{X} = \{[e_1],\ [e_2],\ [e_3],\ [(1, 1, 1)]\}$.

Proof It follows using the arguments given in Lemma 2.7. □

Remark 2.14 Let $\mathbb{F}_q$ be a finite field with q elements and let $\mathbb{X}$ be the projective set in $\mathbb{P}^2$ parameterized by the following monomials:

$$y^{v_1} = y_1^{q-1}y_2^{q-1},\ y^{v_2} = y_2^{q-1}y_3^{q-1},\ y^{v_3} = y_1^{q-1}y_3^{q-1}.$$

Then $\mathbb{X} = \{[e_1],\ [e_2],\ [e_3],\ [(1, 1, 1)]\}$ and $I(\mathbb{X}) = (t_1t_2 - t_2t_3,\ t_1t_3 - t_2t_3)$.

Definition 2.15 The set $T = \{[(x_1, \dots, x_s)] \in \mathbb{P}^{s-1} | x_i \in \mathbb{F}_q^* \text{ for all } i\}$ is called a *projective torus* in $\mathbb{P}^{s-1}$.

Lemma 2.16 *Let β be a generator of $\mathbb{F}_q^*$ and $0 \neq r \in \mathbb{N}$. Suppose $s = 2$. If $I = (t_1^{r+1}t_2 - t_1t_2^{r+1})$ and r divides $q - 1$, then $I = I(\mathbb{X})$, where $\mathbb{X}$ is the set of clutter type in $\mathbb{P}^1$ parameterized by y_1^{q-1}, $y_2^{q-1}y_3^k$ and $r = \mathrm{o}(\beta^k)$.*

Proof We set $f = t_1^{r+1}t_2 - t_1t_2^{r+1}$. Take a point $P = [(x_1^{q-1}, x_2^{q-1}x_3^k)]$ in $\mathbb{X}$. Then

$$f(P) = (x_1^{q-1})^{r+1}(x_2^{q-1}x_3^k) - (x_1^{q-1})(x_2^{q-1}x_3^k)^{r+1}.$$

We may assume $x_1 \neq 0$ and $x_2 \neq 0$. Then $f(P) = x_3^k - (x_3^k)^{r+1}$. If $x_3 \neq 0$, then $x_3 = \beta^i$ for some i and $(x_3^k)^{r+1} = x_3^k$, that is, $f(P) = 0$. Therefore, one has the inclusion $(f) \subset I(\mathbb{X})$.

Next we show the inclusion $I(\mathbb{X}) \subset (f)$. By Theorem 2.4, $I(\mathbb{X})$ is a binomial ideal. Take a non-zero binomial $g = t_1^{a_1}t_2^{a_2} - t_1^{b_1}t_2^{b_2}$ that vanishes on $\mathbb{X}$. Then $a_1 + a_2 = b_1 + b_2$ because $I(\mathbb{X})$ is graded. We may assume that $b_1 > a_1$ and $a_2 > b_2$. We may also assume that $a_1 > 0$ and $b_2 > 0$ because $\{[e_1], [e_2]\} \subset \mathbb{X}$. Then $g = t_1^{a_1}t_2^{b_2}(t_2^{a_2-b_2} - t_1^{b_1-a_1})$. As g vanishes on $\mathbb{X}$, making $y_3 = \beta$ and $y_1 = y_2 = 1$, we get $(\beta^k)^{a_2-b_2} = 1$. Hence $a_2 - b_2 = \lambda r$ for some $\lambda \in \mathbb{N}_+$, where $r = o(\beta^k)$. Thus $t_2^{a_2-b_2} - t_1^{b_1-a_1}$ is equal to $t_2^{\lambda r} - t_1^{\lambda r} \in (t_1^r - t_2^r)$. Therefore, g is a multiple of $f = t_1t_2(t_1^r - t_2^r)$ because $a_1 > 0$ and $b_2 > 0$. Thus $g \in (f)$. □

Lemma 2.17 *If $\{[e_1], [e_2]\} \subset \mathbb{Y} \subset \mathbb{P}^1$ and $\mathbb{Y} \cup \{0\}$ is a monoid under componentwise multiplication, then there is $0 \neq r \in \mathbb{N}$ such that $I(\mathbb{Y}) = (t_1^{r+1}t_2 - t_1t_2^{r+1})$ and r divides $q - 1$.*

Proof We set $f = t_1^{r+1}t_2 - t_1t_2^{r+1}$ and $X = \mathbb{Y} \cap T$, where T is a projective torus in $\mathbb{P}^1$. The set X is a group, under componentwise multiplication, because X is a finite monoid and the cancellation laws hold. By Theorem 2.4, $I(\mathbb{Y})$ is a binomial ideal. Clearly $(f) \subset I(\mathbb{Y})$. To show the other inclusion take a non-zero binomial

$g = t_1^{a_1}t_2^{a_2} - t_1^{b_1}t_2^{b_2}$ that vanish on $\mathbb{Y}$. Then $a_1 + a_2 = b_1 + b_2$ because $I(\mathbb{Y})$ is graded. We may assume that $b_1 > a_1$ and $a_2 > b_2$. We may also assume that $a_1 > 0$ and $b_2 > 0$ because $\{[e_1], [e_2]\} \subset \mathbb{X}$. Then $g = t_1^{a_1}t_2^{b_2}(t_2^{a_2-b_2} - t_1^{b_1-a_1})$. The subgroup of $\mathbb{F}_q^*$ given by $H = \{\xi \in \mathbb{F}_q^* \,|\, [(1, \xi)] \in X\}$ has order $r = |X|$. Pick a generator β of the cyclic group $\mathbb{F}_q^*$. Then H is a cyclic group generated by β^k for some $k \geq 0$. As g vanishes on $\mathbb{Y}$, one has that $t_2^{a_2-b_2} - t_1^{b_1-a_1}$ vanishes on X. In particular $(\beta^k)^{a_2-b_2} = 1$. Hence $a_2 - b_2 = \lambda r$ for some $\lambda \in \mathbb{N}_+$, where $r = o(\beta^k) = |X|$. Proceeding as in the proof of Lemma 2.16 one derives that $g \in (f)$. Noticing that H is a subgroup of $\mathbb{F}_q^*$, we obtain that r divides $q - 1$. □

Definition 2.18 An ideal $I \subset S$ is called a *complete intersection* if there exists $g_1, \ldots, g_r$ in S such that $I = (g_1, \ldots, g_r)$, where r is the height of I.

Recall that a graded ideal I is a complete intersection if and only if I is generated by a homogeneous regular sequence with $\mathrm{ht}(I)$ elements (see [20, Proposition 2.3.19, Lemma 2.3.20]).

Theorem 2.19 *Let $\mathbb{F}_q$ be a finite field and let $\mathbb{X}$ be a set in $\mathbb{P}^{s-1}$ parameterized by a set of monomials $y^{v_1}, \ldots, y^{v_s}$ such that* $\mathrm{supp}(y^{v_i}) \not\subset \mathrm{supp}(y^{v_j})$ *for any $i \neq j$. Then $I(\mathbb{X})$ is a complete intersection if and only if $s \leq 4$ and, up to permutation of variables, $I(\mathbb{X})$ has one of the following forms:*

(i) $s = 4$, *q is odd and* $I = (t_1t_2 - t_3t_4, t_1t_3 - t_2t_4, t_2t_3 - t_1t_4)$.
(ii) $s = 3$ *and* $I = (t_1t_2 - t_2t_3, t_1t_3 - t_2t_3)$.
(iii) $s = 2$ *and* $I = (t_1^{r+1}t_2 - t_1t_2^{r+1})$, *where* $0 \neq r \in \mathbb{N}$ *is a divisor of* $q - 1$.
(iv) $s = 1$ *and* $I = (0)$.

Proof ⇒): Assume that $I(\mathbb{X})$ is a complete intersection. By Lemma 2.6(d) one has $s \leq 4$. Case (i): Assume that $s = 4$. Setting $I = I(\mathbb{X})$, by hypothesis I is generated by 3 binomials g_1, g_2, g_3. By parts (b) and (c) of Lemma 2.6, for each pair $1 \leq i < j \leq 4$ there are positive integers c_{ij} and a_{ij} such that $t_i^{c_{ij}}t_j$ and $t_it_j^{a_{ij}}$ occur as terms in g_1, g_2, g_3. Since there are at most 6 monomials that occur in the g_i's, we get that $c_{ij} = a_{ij} = 1$ for $1 \leq i < j \leq 4$. Fixing the monomial t_1t_2 as a member of the first binomial, up to permutation of variables, there are 3 subcases to consider:

$$
\begin{aligned}
&(a): \quad g_1 = t_1(t_2 - t_3), \qquad g_2 = t_1t_4 - t_2t_3, \qquad g_3 = t_4(t_2 - t_3).\\
&(b): \quad g_1 = t_1(t_2 - t_3), \qquad g_2 = t_4(t_1 - t_3), \qquad g_3 = t_2(t_3 - t_4).\\
&(c): \quad g_1 = t_1t_2 - t_3t_4, \qquad g_2 = t_1t_3 - t_2t_4, \qquad g_3 = t_2t_3 - t_1t_4.
\end{aligned}
$$

Subcase (a): This case cannot occur because the ideal (g_1, g_2, g_3) has height 2.

Subcase (b): The reduced Gröbner basis of $I = (g_1, g_2, g_3)$ with respect to the GRevLex order $\prec$ is given by

$$
\begin{aligned}
&g_1 = t_1t_2 - t_1t_3, \qquad g_2 = t_1t_4 - t_3t_4, \qquad g_3 = t_2t_3 - t_2t_4,\\
&g_4 = t_3^2t_4 - t_2t_4^2, \qquad g_5 = t_1t_3^2 - t_2t_4^2, \qquad g_6 = t_2^2t_4^2 - t_2t_4^3.
\end{aligned}
$$

Hence the binomial $h = t_2t_4 - t_3t_4 \notin I$ because t_2t_4 does not belong to $\text{in}_\prec(I)$, the initial ideal of I. Since $h^2 = -2t_4^2g_3 + t_4g_4 + g_6$, we get that $h \in \text{rad}(I)$. Thus I is not a radical ideal which is impossible because $I = I(\mathbb{X})$ is a vanishing ideal. Therefore, this case cannot occur.

Subcase (c): In this case, one has $I = (t_1t_2 - t_3t_4, t_1t_3 - t_2t_4, t_2t_3 - t_1t_4)$, as required. From Lemma 2.7, we obtain that q is odd.

Case (ii): Assume that $s = 3$. By hypothesis $I = I(\mathbb{X})$ is generated by 2 binomials g_1, g_2. By parts (b) and (c) of Lemma 2.6, for each pair $1 \leq i < j \leq 3$ there are positive integers c_{ij} and a_{ij} such that $t_i^{c_{ij}}t_j$ and $t_it_j^{a_{ij}}$ occur as terms in g_1, g_2. Since there are at most 4 monomials that occur in the g_i's it is seen that, up to permutation of variables, there are 2 subcases to consider:

$$\text{(a)}: \ g_1 = t_1t_3 - t_2t_3, \ g_2 = t_1^{c_{12}}t_2 - t_1t_2^{a_{12}} \text{ with } c_{12} = a_{12} \geq 2.$$
$$\text{(b)}: \ g_1 = t_1t_2 - t_2t_3, \ g_2 = t_1t_3 - t_2t_3.$$

Subcase (a) cannot occur because the ideal $I = (g_1, g_2)$, being contained in $(t_1 - t_2)$, has height 1. Thus we are left with subcase (b), that is, $I = (t_1t_2 - t_2t_3, t_1t_3 - t_2t_3)$, as required.

Case (iii): If $s = 2$, then $\mathbb{X}$ is parameterized by y^{v_1}, y^{v_2}. Pick $y_k \in \text{supp}(y^{v_1}) \setminus \text{supp}(y^{v_2})$. Making $y_k = 0$ and $y_\ell = 1$ for $\ell \neq k$, we get that $[e_2] \in \mathbb{X}$, and by a similar argument $[e_1] \in \mathbb{X}$. As $\mathbb{X} \cup \{[0]\}$ is a monoid under componentwise multiplication, by Lemma 2.17, $I(\mathbb{X})$ has the required form.

Case (iv): If $s = 1$, this case is clear.

$\Leftarrow$) The converse is clear because the vanishing ideal $I(\mathbb{X})$ has height $s - 1$. □

Proposition 2.20 *If I is an ideal of S of one of the following forms:*

(i) $s = 4$, *q is odd and* $I = (t_1t_2 - t_3t_4, t_1t_3 - t_2t_4, t_2t_3 - t_1t_4)$,
(ii) $s = 3$ *and* $I = (t_1t_2 - t_2t_3, t_1t_3 - t_2t_3)$,
(iii) $s = 2$ *and* $I = (t_1^{r+1}t_2 - t_1t_2^{r+1})$, *where* $0 \neq r \in \mathbb{N}$ *and r divides* $q - 1$,

then there is a set $\mathbb{X}$ in $\mathbb{P}^{s-1}$ of clutter type such that I is the vanishing ideal $I(\mathbb{X})$.

Proof The result follows from Lemma 2.7 and Remark 2.11, Lemma 2.13 and Remark 2.14, and Lemma 2.16, respectively. □

Problem 2.21 Let $\mathbb{X}$ be a set of clutter type such that $I(\mathbb{X})$ is a complete intersection. Using the techniques of [4, 10, 13, 14] and Theorem 2.19 find formulae for the *basic parameters* of the Reed–Muller-type codes associated to $\mathbb{X}$.

Acknowledgements We thank the referees for their careful reading of the paper and for the improvements they suggested.

References

1. Carvalho, C.: On the second Hamming weight of some Reed-Muller type codes. Finite Fields Appl. **24**, 88–94 (2013)
2. Cox, D., Little, J., O'Shea, D.: Ideals, Varieties, and Algorithms. Springer, New York (1992)

3. Delsarte, P., Goethals, J.M., MacWilliams, F.J.: On generalized Reed-Muller codes and their relatives. Inf. Control **16**, 403–442 (1970)
4. Duursma, I.M., Rentería, C., Tapia-Recillas, H.: Reed-Muller codes on complete intersections. Appl. Algebra Eng. Commun. Comput. **11**(6), 455–462 (2001)
5. Gasca, M., Sauer, T.: Polynomial interpolation in several variables. Adv. Comput. Math. **12**(4), 377–410 (2000)
6. Geil, O., Thomsen, C.: Weighted Reed-Muller codes revisited. Des. Codes Cryptogr. **66**, 195–220 (2013)
7. Gold, L., Little, J., Schenck, H.: Cayley-Bacharach and evaluation codes on complete intersections. J. Pure Appl. Algebra **196**(1), 91–99 (2005)
8. González-Sarabia, M., Rentería, C., Tapia-Recillas, H.: Reed-Muller-type codes over the Segre variety. Finite Fields Appl. **8**(4), 511–518 (2002)
9. Hansen, J.: Linkage and codes on complete intersections. Appl. Algebra Eng. Commun. Comput. **14**(3), 175–185 (2003)
10. López, H.H., Rentería, C., Villarreal, R.H.: Affine cartesian codes. Des. Codes Cryptogr. **71**(1), 5–19 (2014)
11. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North-Holland, Amsterdam (1977)
12. Matsumura, H.: Commutative Ring Theory, Cambridge Studies in Advanced Mathematics 8. Cambridge University Press, Cambridge (1986)
13. Rentería, C., Simis, A., Villarreal, R.H.: Algebraic methods for parameterized codes and invariants of vanishing ideals over finite fields. Finite Fields Appl. **17**(1), 81–104 (2011)
14. Sarmiento, E., Vaz Pinto, M., Villarreal, R.H.: The minimum distance of parameterized codes on projective tori. Appl. Algebra Eng. Commun. Comput. **22**(4), 249–264 (2011)
15. Sarmiento, E., Vaz Pinto, M., Villarreal, R.H.: On the vanishing ideal of an algebraic toric set and its parameterized linear codes. J. Algebra Appl. **11**(4), 1250072 (2012)
16. Sørensen, A.: Projective Reed-Muller codes. IEEE Trans. Inf. Theory **37**(6), 1567–1576 (1991)
17. Tochimani, A., Villarreal, R.H.: Binomial vanishing ideals. J. Algebra Comb. Discrete Appl. **2**(2), 77–82 (2015)
18. Tochimani, A., Villarreal, R.H.: Vanishing ideals over rational parameterizations. Preprint, arXiv:1502.05451v1 (2015)
19. Tsfasman, M., Vladut, S., Nogin, D.: Algebraic Geometric Codes: Basic Notions, Mathematical Surveys and Monographs 139. American Mathematical Society, Providence (2007)
20. Villarreal, R.H.: Monomial Algebras, Monographs and Research Notes in Mathematics, 2nd edn. Chapman and Hall/CRC, Boca Raton (2015)