# CODES ON WEIGHTED PROJECTIVE PLANES

YAĞMUR ÇAKIROĞLU, JADE NARDİ, AND MESUT ŞAHİN

Abstract. We comprehensively study weighted projective Reed-Muller (WPRM) codes on weighted projective planes $\mathbb{P}(1,a,b)$. We provide the universal Gröbner basis for the vanishing ideal of the set $Y$ of $\mathbb{F}_q$–rational points of $\mathbb{P}(1,a,b)$ to get the dimension of the code. We determine the regularity set of $Y$ using a novel combinatorial approach. We employ footprint techniques to compute the minimum distance.

## 1. Introduction

Let $\mathbb{F}_q$ be the finite field with $q$ elements and $\mathbb{K}$ be its algebraic closure. We study linear codes from weighted projective planes $\mathbb{P}(1,a,b)$ for two positive integers $a \leq b$. Recall that the *weighted projective plane* is the quotient space

$$\mathbb{P}(1,a,b) = (\mathbb{K}^3 \setminus \{0\})/\mathbb{K}^*$$

under the following equivalence relation: for every $(x_0, x_1, x_2) \in \mathbb{K}^3$,

$$(x_0, x_1, x_2) \sim (\lambda x_0, \lambda^a x_1, \lambda^b x_2) \text{ for } \lambda \in \mathbb{K}^*.$$

We can assume without loss of generality that the integers $a$ and $b$ are coprime as $\mathbb{P}(1,a,b) \simeq \mathbb{P}(1,ac,bc)$ for every positive integer $c$ (see [11, Lemma 1.1]).

It is well known that the set $\mathbb{P}(1,a,b)(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points consists of equivalence classes $[x_0 : x_1 : x_2]$ having representatives with all coordinates $x_0$, $x_1$, $x_2$ lying in $\mathbb{F}_q$, see [17, Lemmas 6 and 7]. More precisely, one can choose representatives $[1 : y_1 : y_2]$ where $(y_1, y_2) \in \mathbb{F}_q^2$, together with $[0 : y_1 : y_2]$ as given in Remark 5.4.

The weighted projective plane $\mathbb{P}(1,a,b)$ is a simplicial toric variety. It thus comes with the polynomial ring $S = \mathbb{F}_q[x_0, x_1, x_2]$, which is graded via $\deg x_0 = 1$ $\deg x_1 = a$ and $\deg x_2 = b$. A degree $d \in \mathbb{N}$ defines a polygon

$$P_d := \left\{(x,y) \in \mathbb{R}^2 \,:\, x \geq 0,\, y \geq 0,\, ax + by \leq d\right\} \tag{1.1}$$

and the integral points of $P_d$ give rise to monomials of degree $d$:

$$\mathbb{M}_d := \left\{\mathbf{x}^{\mathbf{a},d} := x_0^{d-aa_1-ba_2} x_1^{a_1} x_2^{a_2} : \mathbf{a} = (a_1, a_2) \in P_d \cap \mathbb{Z}^2\right\}. \tag{1.2}$$

The polynomial ring $S$ can thus be written as follows.

$$S = \bigoplus_{d \geq 0} S_d \text{ where } S_d = \operatorname{Span} \mathbb{M}_d.$$

2020 *Mathematics Subject Classification.* Primary 14M25; 14G05 ; Secondary 94B27 ; 11T71.
*Key words and phrases.* toric code, weighted projective space, error-correcting code, Reed-Muller code.
The first and third authors are supported by TÜBİTAK Project No:119F177. This article is part of the first author's Ph.D. thesis under the supervision of the third author. The second author is supported by the French National Research Agency through ANR *Barracuda* (ANR-21-CE39-0009) and the French government *Investissements d'Avenir* program ANR-11-LABX-0020-01.

In order to obtain a linear code, we evaluate homogeneous polynomials of degree $d \geq 1$ at a subset $Y = \{P_1, \ldots, P_n\} \subseteq \mathbb{P}(1,a,b)(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points. As points of $\mathbb{P}(1,a,b)$ are orbits, we have to choose representatives for each of the points: given a point $P \in \mathbb{P}(1,a,b)(\mathbb{F}_q)$, we choose a representative triple $(y_0, y_1, y_2) \in \mathbb{F}_q^3$ and we define $f(P) = f(y_0, y_1, y_2)$ for any $f \in S_d$. This defines the following evaluation map

$$\mathrm{ev}_Y : \begin{array}{ccc} S_d & \to & \mathbb{F}_q^n \\ f & \mapsto & (f(P_1), \ldots, f(P_n)) \end{array} \tag{1.3}$$

whose image, denoted by $C_{d,Y}$, is the evaluation code at $Y$ of degree $d$. A different choice of representatives gives monomially equivalent code, *i.e.* each coordinate is multiplied by a non-zero element of $\mathbb{F}_q$.

We write $[n, k, d_{min}]_q$ for the main parameters of the code, which we recall next. The *length* $n$ is the cardinality $|Y|$ of the set $Y$. The *dimension* $k$ is the dimension of $C_{d,Y}$ as an $\mathbb{F}_q$–vector space. The *Hamming weight* $\omega(c)$ of a codeword $c = \mathrm{ev}_Y(f) = (f(P_1), \ldots, f(P_n)) \in C_{d,Y}$ is the number of non–zero components of $c$ which is also $n - |V_Y(f)|$, where $V_Y(f) := \{P \in Y : f(P) = 0\}$. Finally, the *minimum distance* $d_{min}$ of $C_{d,Y}$ is the minimum weight among all codewords $c \in C_{d,Y} \setminus \{0\}$.

If $Y$ consists only of affine points, *i.e.* of the form $(1, x, y)$ for $(x, y) \in \mathbb{F}_q^2$, then the code $C_{d,Y}$ is called the weighted (affine) Reed-Muller (WRM or WARM) code of $(a, b)$–weighted degree $d$. Its length is $n = \left|\mathbb{F}_q^2\right| = q^2$. The dimension and the minimum distance have been given by Sørensen [21, Theorem 1].

If $Y$ is the whole set of $\mathbb{F}_q$-rational points of the weighted projective plane $\mathbb{P}(1,a,b)$, then the code is simply denoted by $C_d$ and called a weighted projective Reed-Muller (WPRM) code. Its length is $n = |\mathbb{P}(1,a,b)(\mathbb{F}_q)| = q^2 + q + 1$ for any integers $a$ and $b$. The dimension and the minimum distance were given explicitly by Aubry et al. in [2] only for small degrees $d \leq q$ which are multiple of both $a$ and $b$. Recently, [1, Theorem 5.1] relaxed the divisibility hypothesis but still gave the minimum distance when $d \leq q$. Let us mention that Sørensen [21] also introduced some different codes bearing the name "weighted projective Reed-Muller codes", where the evaluation is done for a proper subspace of $\bigoplus_{d' \leq d} S_{d'}$ at the $\mathbb{F}_q$-rational points of the *classical* projective plane $\mathbb{P}^2$.

In the present paper, we deal with the case $Y = \mathbb{P}(1,a,b)(\mathbb{F}_q)$ with arbitrary degree $d$, thus extending and generalizing the results of the paper by Çakıroğlu and Şahin [9] given for the case where $a = 1$. We leverage the fact that weighted projective spaces are toric varieties and we follow the strategy described in [16], which connects the combinatorics of the polygon $P_d$ (see Equation 1.1) and the parameters of the code $C_d$.

The paper is organized as follows. Section 2 displays the universal Gröbner basis for the vanishing ideal of $Y = \mathbb{P}(1,a,b)(\mathbb{F}_q)$ and the projective reduction of the polygon $P_d$. This provides a basis, and thus the dimension, of $C_d$ for any degree $d \geq 1$. In Section 3, we determine the regularity set of $Y$ which helps eliminate the trivial codes as well as giving a lower bound for the minimum distance. In Section 4 we employ footprint techniques to bound the minimum distance from below. Candidates for minimal weight codewords are given in Section 5. Our results for the minimum distance are summarized in Section 6, followed by some refinements in the cases for which we are only able to determine a lower bound the minimum distance.

## 2. Dimension

In this section, our goal is to give a closed formula for the dimension of $C_d$. As an evaluation code, the code $C_d$ is isomorphic to the quotient of $S_d$ by the degree–$d$ part of the vanishing ideal of $Y$. In the case we are interested in, *i.e.* $Y = \mathbb{P}(1, a, b)(\mathbb{F}_q)$, we know a generating set of the vanishing ideal of $Y$, which we prove to be a universal Gröbner basis. This allows us to identify a combinatorial set called a *projective reduction* that corresponds to the standard monomials of degree $d$, giving rise to the basis of the code $C_d$.

### 2.1. The vanishing ideal of the set of the rational points of $Y = \mathbb{P}(1, a, b)$.

In this subsection, we give a unique (up to a constant factor) minimal generating set for the vanishing ideal of $I(Y)$, which is both the universal Gröbner basis and the Graver basis.

An ideal generated by binomials $\mathbf{x}^{\mathbf{u}} - \lambda \mathbf{x}^{\mathbf{v}}$, with $\lambda \in \mathbb{K} \setminus \{0\}$, is called a *binomial ideal*. The following reveals that the ideal $I(\mathbb{P}(1, a, b)(\mathbb{F}_q))$ is *pure binomial*, *i.e.* generated by pure difference binomials $\mathbf{x}^{\mathbf{u}} - \mathbf{x}^{\mathbf{v}}$.

**Theorem 2.1.** *[19, Corollary 5.8] The vanishing ideal $I(\mathbb{P}(1, a, b)(\mathbb{F}_q))$ of the set of $\mathbb{F}_q$–points of $\mathbb{P}(1, a, b)$ is generated by the following binomials.*

$$\begin{aligned}
f_0 &= x_1 x_2 \left( x_2^{(q-1)a} - x_1^{(q-1)b} \right) \\
f_1 &= x_0 x_2 \left( x_2^{q-1} - x_0^{(q-1)b} \right) \\
f_2 &= x_0 x_1 \left( x_1^{q-1} - x_0^{(q-1)a} \right)
\end{aligned}$$

**Remark 2.2.** *The polynomials $f_i$ are numbered so that $f_i$ does not involve the variable $x_i$ for every $i \in \{0, 1, 2\}$.*

*It is clear that the monomials of $f_0, f_1, f_2$ cannot divide each other and so $|G(M_{I(Y)})| = 6$ in the notation of [10, Corollary 3.6]. Thus, the binomials $f_0, f_1, f_2$ are indispensable, i.e. they appear (up to a nonzero constant) in every minimal binomial generating set of $I(Y)$. In other words, (up to a nonzero constant) $\{f_0, f_1, f_2\}$ is the unique minimal generating set.*

We would like to obtain the *universal* Gröbner basis of $I(Y)$ which is a Gröbner basis with respect to any monomial ordering. Since there are only finitely many distinct reduced Gröbner bases, their union is the universal Gröbner basis. To accomplish this goal, we appeal to [10, Proposition 4.2], saying that a binomial in the universal Gröbner basis must be *primitive,* which we define next.

**Definition 2.3.** *[10, Definition 4.1] A nonzero binomial $\mathbf{x}^{\mathbf{u}} - \mathbf{x}^{\mathbf{v}} := x_0^{u_0} x_1^{u_1} x_2^{u_2} - x_0^{v_0} x_1^{v_1} x_2^{v_2}$ in a pure binomial ideal $I$ is called a* primitive binomial *of $I$ if there exists no other binomial $\mathbf{x}^{\mathbf{u}'} - \mathbf{x}^{\mathbf{v}'} \in I \setminus \{0\}$ such that $\mathbf{x}^{\mathbf{u}'}$ divides $\mathbf{x}^{\mathbf{u}}$ and $\mathbf{x}^{\mathbf{v}'}$ divides $\mathbf{x}^{\mathbf{v}}$. The set of all primitive binomials of $I$ is called the* Graver basis *of $I$.*

We are ready to give the main result of this subsection showcasing a rare instance where an ideal has a unique minimal generating set which is both the universal Gröbner basis and the Graver basis. This generalizes [5, Theorem 2.8] which gives a reduced Gröbner basis which is also a universal Gröbner basis for the vanishing ideal of $Y = \mathbb{P}^m(\mathbb{F}_q)$ over an algebraic extension of $\mathbb{F}_q$.

**Theorem 2.4.** *The generating set $\{f_0, f_1, f_2\}$ is both the universal Gröbner basis and the Graver basis of $I(Y)$.*

*Proof.* Take a homogeneous binomial $\mathbf{x}^{\mathbf{u}} - \mathbf{x}^{\mathbf{v}}$ which is an element of the universal Gröbner basis of $I(Y)$. By [10, Proposition 4.2], it must be primitive. Thus, it suffices to show that there is no primitive homogeneous binomial other than $f_0, f_1, f_2$.

By [19, Proposition 5.6] and the proof of [19, Theorem 3.7], a homogeneous binomial in $I(Y)$ is of the form

$$\mathbf{x}^{\mathbf{u}} - \mathbf{x}^{\mathbf{v}} = \mathbf{x}^{\mathbf{a}}(\mathbf{x}^{m^+} - \mathbf{x}^{m^-}) \text{ with } \operatorname{supp}(\mathbf{x}^{m^+}) \cap \operatorname{supp}(\mathbf{x}^{m^-}) = \emptyset,$$

where $\operatorname{supp}(\mathbf{x}^{\mathbf{a}}) := \{j \in \{0,1,2\} : x_j \mid \mathbf{x}^{\mathbf{a}}\}$ and $m^+ - m^- \in (q-1)L_{\beta(\varepsilon)}$. Recall that $\beta = \begin{pmatrix} 1 & a & b \end{pmatrix}$, $\beta(\varepsilon)$ is the submatrix of the matrix $\beta$ with the columns $\beta_{j+1}$ where $j \in \varepsilon = \operatorname{supp}(\mathbf{x}^{\mathbf{a}}) \subseteq \{0,1,2\}$ and $L_{\beta(\varepsilon)}$ is the lattice, which is the integer points of the kernel of the linear map represented by the matrix $\beta(\varepsilon)$.

Suppose that $\varepsilon = \{0,1,2\}$. Then, without loss of generality, we may assume that $\mathbf{x}^{\mathbf{u}} - \mathbf{x}^{\mathbf{v}} = x_0^{a_0} x_1^{a_1} x_2^{a_2} (x_2^{m_2^+} - x_0^{m_0^-} x_1^{m_1^-})$, with positive $a_0, a_1, a_2$. Then,

$$\mathbf{x}^{\mathbf{u}} - \mathbf{x}^{\mathbf{v}} = x_0^{a_0-1} x_1^{a_1-1} x_2^{a_2-1} (x_0 x_1 x_2^{m_2^+ + 1} - x_0^{m_0^- + 1} x_1^{m_1^- + 1} x_2).$$

Thus, $\mathbf{x}^{\mathbf{u}} - \mathbf{x}^{\mathbf{v}}$ is not primitive, since $\mathbf{x}^{\mathbf{u}'} - \mathbf{x}^{\mathbf{v}'} := x_0 x_1 x_2^{m_2^+ + 1} - x_0^{m_0^- + 1} x_1^{m_1^- + 1} x_2$ belongs to $I(Y)$ and we have both $\mathbf{x}^{\mathbf{u}'}$ divides $\mathbf{x}^{\mathbf{u}}$ and $\mathbf{x}^{\mathbf{v}'}$ divides $\mathbf{x}^{\mathbf{v}}$.

Since $L_{\beta(\varepsilon)} = \{0\}$, when $|\varepsilon| = 1$, we just need to consider the case $|\varepsilon| = 2$. If $\varepsilon = \{1,2\}$ then $\beta(\varepsilon) = [a\ b]$, $L_{\beta(\varepsilon)}$ is the sublattice of $\mathbb{Z}^2$ spanned by $(b, -a)$ and we have $\mathbf{x}^{\mathbf{u}} - \mathbf{x}^{\mathbf{v}} = x_1^{a_1} x_2^{a_2} (x_1^{m_1^+} - x_2^{m_2^-})$ for some positive integers $a_1, a_2$ and $(m_1^+, 0) - (0, m_2^-) = (q-1)l(b, -a)$ with a positive integer $l$. Thus, the monomials $x_1 x_2 x_1^{(q-1)b} \mid \mathbf{x}^{\mathbf{u}}$ and $x_1 x_2 x_2^{(q-1)a} \mid \mathbf{x}^{\mathbf{v}}$. The only primitive binomial with these properties is clearly $f_0$. The other two cases are done similarly. $\square$

2.2. **Projective reduction.** We want to rely on the notion of *projective reduction* of the polygon $P_d$ introduced in [16, §3.1] to get canonical representatives for the cosets in $S_d/I(Y)_d$ through the identification of lattice points of $P_d$ with monomials in $S_d$. We follow the notations introduced in [16], which generalizes the notion of projective reduction for the classical projective spaces given in [5, §2.1].

**Remark 2.5.** *Remark 3.6 of [16] assumes that the polytope is integral and claims that the* projective reduction *is only relevant when the polytope has the same normal fan as the variety. The latter condition is always satisfied on $\mathbb{P}(1, a, b)$ for any $P_d$. But, when $a$ (resp. $b$) does not divide $d$, the vertex $(d/a, 0)$ (resp. $(0, d/b)$) of $P_d$ is not integral. This does not cause a problem because a vertex corresponds to a monomial involving only one variable, hence it cannot be equivalent to another monomial modulo $I(Y)$. In other words, the cosets in $S_d/I(Y)_d$ of these monomials are singletons. We just need to work out the other cosets, which can be done by the methods of [16]. The reader is invited to consult [19, Lemma 5.15 and Theorem 5.16] for more general toric varieties.*

Recall some definitions about lattice polygons. Let $P$ be a convex lattice polygon. We denote a face $Q$ of $P$ by $Q \prec P$ and define its *interior* to be the set of points not lying on any proper face, *i.e.*

$$P^\circ = P \setminus \bigcup_{\substack{Q \prec P \\ Q \neq P}} Q.$$

By [16, Theorem 3.5], a basis for the code $C_d$ is given by certain integral points of the polygon $P_d$, that are chosen with respect to the following equivalence relation.

**Definition 2.6.** *[16, Definition 3.4] Given a lattice polytope $P$, we define an equivalence relation $\sim_P$ on the set of its lattice points $P \cap \mathbb{Z}^N$ by*

$$m \sim_P m' \iff \exists Q \prec P \text{ such that } m, m' \in Q^\circ \text{ and } m - m' \in (q-1)\mathbb{Z}^N$$

*where $Q^\circ$ is the interior of $Q$. A* ***projective reduction*** $\operatorname{Red} P$ *of $P$ is defined to be a set of representatives of elements of $P \cap \mathbb{Z}^N$ modulo $\sim_P$ .*

As suggested by [16, Definition 4.3], we consider a particular projective reduction of $P_d$ coming from a monomial ordering. Throughout this paper, we will deal with the lex ordering with $x_2 > x_1 > x_0$: a monomial $x^{\mathbf{a},d} = x_2^{a_2} x_1^{a_1} x_0^{d-aa_1-ba_2}$ of degree $d$ is smaller than a monomial $x^{\mathbf{a}',d'} = x_2^{a_2'} x_1^{a_1'} x_0^{d'-aa_1'-ba_2'}$ of degree $d'$ if and only if the left most non-zero number in $(a_2 - a_2', a_1 - a_1', a(a_1' - a_1) + b(a_2' - a_2))$ is negative. In this case, we write $x^{\mathbf{a},d} <_{\text{lex}} x^{\mathbf{a}',d'}$.

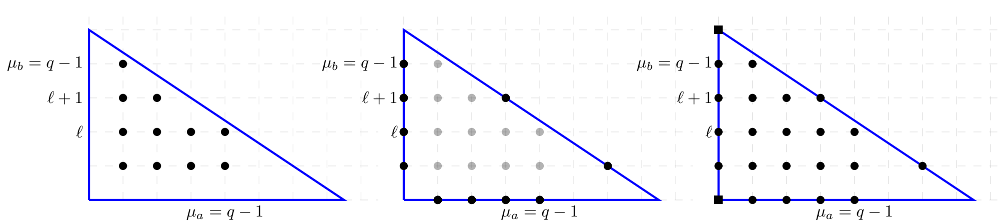
Note that the left most non-zero number in $(a_2 - a_2', a_1 - a_1', a(a_1' - a_1) + b(a_2' - a_2))$ being negative is equivalent to the left most non-zero number in $(a_2 - a_2', a_1 - a_1')$ being negative, *i.e.* $(a_1, a_2) <_{\text{lex}} (a_1', a_2')$.

We denote by $\operatorname{Red}(d)$ the projective reduction with respect to the aforementioned ordering, see Figure 1c, *i.e.*

$$\operatorname{Red}(d) = \left\{ \min_{\text{lex}} \{m \in \theta\} : \theta \in (P_d \cap \mathbb{Z}^2)/\sim_{P_d} \right\} \tag{2.1}$$

$$= \bigcup_{Q \prec P} \left\{ \min_{\text{lex}} \{m \in \theta\} : \theta \in (Q^\circ \cap \mathbb{Z}^2)/(q-1)\mathbb{Z}^2 \right\}. \tag{2.2}$$

**Remark 2.7.** *If $a = b = 1$, $\operatorname{Red}(d)$ identifies with the exponents of the projective reduction of monomials of degree $d$ defined in [5, Definition 2.1].*




(A) Reduction of $P^\circ$ (B) Reduction of edges (C) Total reduction of $P$

FIGURE 1. Reduction of a polygon associated to $\mathbb{P}(1,2,3)$ for $q = 5$ and $d = 15$.

**Theorem 2.8.** *[16, Theorem 3.5] A basis for the code $C_d$ is given by the images under the evaluation map $\mathrm{ev}_Y$ of the monomials in $\overline{\mathbb{M}}_d := \{\mathbf{x}^{\mathbf{a},d} : \mathbf{a} \in \mathrm{Red}(d)\}$. Therefore $k = \dim_{\mathbb{F}_q} C_d = |\operatorname{Red}(d)|$.*

We introduce the following notation that will be useful to compute the dimension of the code:

$$\mu_a = \min\left\{\left\lfloor \frac{d-1}{a} \right\rfloor, q-1\right\}, \qquad E_x(d) = \{(x,0) : 0 \le x \le \mu_a\} \tag{2.3}$$

$$\mu_b = \min\left\{\left\lfloor \frac{d-1}{b} \right\rfloor, q-1\right\}, \qquad E_y(d) = \{(0,y) : 0 \le y \le \mu_b\}. \tag{2.4}$$

If $N_0 = (x', y')$ is the first interior lattice point on the hypotenuse of the triangle $P_d$ (the one with the smallest positive $y$-coordinate and with $x' > 0$), set

$$t = \min\left\{q-2, \left\lfloor \frac{d - by' - 1}{ab} \right\rfloor\right\} \tag{2.5}$$

and define

$$E_h(d) = \left\{(x' - ib, y' + ia) \in \mathbb{N}^2 : 0 \le i \le t\right\}, \tag{2.6}$$

and if there is no such point $N_0$, we let $E_h(d) = \emptyset$.

**Remark 2.9.** *The numbers $\alpha_2 = \left\lfloor \frac{d-1-a(q-1)}{b} \right\rfloor$ and $\ell = \max\{0, \min\{q-1, \alpha_2\}\}$ will play an important role for the rest of the paper. The integer $\ell$ is the biggest integer $y \in [1, \mu_b]$ satisfying the inequality $a(q-1) + by \le d-1$, i.e. such that the lattice point $(q-1, y)$ lies in $P_d^\circ$. Notice that we have*

$$\begin{cases} \mu_a = \lfloor \frac{d-1}{a} \rfloor, & \alpha_2 < 0 & \text{and } \ell = 0 & \text{if } d \le a(q-1), \\ \mu_a = q-1, & \alpha_2 = 0 & \text{and } \ell = 0 & \text{if } a(q-1) < d \le a(q-1)+b, \\ \mu_a = q-1, & 1 \le \alpha_2 \le q-2 & \text{and } \ell = \alpha_2 & \text{if } a(q-1)+b < d \le (q-1)(a+b), \\ \mu_a = q-1, & q-1 \le \alpha_2 & \text{and } \ell = q-1 & \text{if } (q-1)(a+b) < d. \end{cases}$$

**Lemma 2.10.** *Let $\ell$ be as in Remark 2.9. Then, the set $\mathrm{Red}(d)$ corresponding to the lex ordering with $x_2 > x_1 > x_0$ is the union*

$$R(d) \cup T(d) \cup H(d), \text{ where}$$

$$\begin{aligned} R(d) &= \left\{(x,y) \in \mathbb{Z}^2 : 0 \le x \le \mu_a \text{ and } 0 \le y \le \ell\right\}, \\ T(d) &= \left\{(x,y) \in \mathbb{Z}^2 : 0 \le x \le \left\lfloor \frac{d-1-by}{a} \right\rfloor \text{ and } \ell+1 \le y \le \mu_b\right\}, \\ H(d) &= E_h(d) \cup \left[\{(0, d/b), (d/a, 0)\} \cap \mathbb{Z}^2\right]. \end{aligned}$$

*Proof.* In order to determine elements of $\mathrm{Red}(d)$ as described in Equation (2.2), we run through the faces $Q \prec P_d$ and we choose the "smallest" non–equivalent points $\mathbf{a} \in Q^\circ$ with respect to the aforementioned lex ordering.

First of all, the vertex $(0,0)$ lies in the set $R(d)$. The vertices $(0, \frac{d}{b})$ and $(\frac{d}{a}, 0)$ clearly belong to the set $H(d)$ when $b|d$ or $a|d$, respectively.

Now let us deal with the edges of $P_d$. If $Q$ is the edge of $P_d$ on $x$-axis, then the lattice points in the interior $Q^\circ$ of $Q$ are of the form $(x, 0)$ for $1 \le x \le \left\lfloor \frac{d-1}{a} \right\rfloor$. By definition of the reduction, one can easily check that

$$Q^\circ \cap \mathrm{Red}(d) = \{(x,0) : 1 \le x \le \mu_a\} = E_x(d) \subseteq R(d).$$

If $Q$ is the edge of $P_d$ on $y$-axis, then

$$Q^\circ \cap \mathrm{Red}(d) = \{(0,y) : 1 \le y \le \mu_b\} = E_y(d) \subseteq R(d) \cup T(d).$$

Let $Q$ be the edge of $P_d$ lying on the line $ax + by = d$. If $N_0 = (x', y')$ is the smallest lattice point on $Q^\circ$ (the one with the smallest positive $y$-coordinate) then all the lattice points on $Q^\circ$ are of the form $N_i = (x' - ib, y' + ia)$ for some non-negative integer $i$.

Note that the biggest lattice point on $Q^\circ$ (the one with the biggest $y$-coordinate and positive $x$-coordinate on the line $ax+by = d$) is $N_{i_{max}} = (x' - i_{max} b, y' + i_{max} a)$ where $i_{max} = \left\lfloor \frac{d-by'-1}{ab} \right\rfloor$. Indeed, by the definition of the floor part, the coordinates of $N_{i_{max}}$ satisfy

$$\begin{aligned} x' - i_{max} b &\in \left[\frac{1}{a}, \frac{1}{a} + b\right), \\ y' + i_{max} a &\in \left(\frac{d-1}{b} - a, \frac{d-1}{b}\right]. \end{aligned}$$

Moreover, for any nonnegative integers $i$ and $j$, we have $N_i - N_j = (i-j)(-b, a)$. As $a$ and $b$ are coprime, the points $N_i$ and $N_j$ are equivalent if and only if $q-1$ divides $i - j$. Therefore, since $t = \min\{q-2, i_{max}\}$ (see Equation (2.5)), the reduction $Q^\circ \cap \mathrm{Red}(d)$ is exactly $E_h(d)$.

Finally, let $Q$ be $P_d$ itself. With the same reasoning as for the horizontal and vertical edges, we can deduce that the reduction of $Q^\circ$ lies in the square $[1, \mu_a] \times [1, \mu_b]$. More precisely, we have

$$Q^\circ \cap \mathrm{Red}(d) = P_d^\circ \cap ([1, \mu_a] \times [1, \mu_b]).$$

Let us make the intersection $P_d^\circ \cap ([1, \mu_a] \times [1, \mu_b])$ more explicit by looking at each horizontal line $y = y_0$ for $1 \le y_0 \le \mu_b$.

On the line $y = y_0$, notice that $\left\lfloor \frac{d-1-by_0}{a} \right\rfloor$ is the $x$-coordinate of the right most lattice point of $P_d^\circ$. Then

$$P_d^\circ \cap \mathrm{Red}(d) = \bigcup_{1 \le y \le \mu_b} \left\{ (x,y) : 1 \le x \le \min\left\{ q-1, \left\lfloor \frac{d-1-by}{a} \right\rfloor \right\} \right\}. \tag{2.7}$$

- If $\ell = 0$, then $d - 1 < a(q-1) + b$ by Remark 2.9. Then for every $y \ge 1$, we have $\lfloor \frac{d-1-by}{a} \rfloor < \lfloor \frac{d-1-b}{a} \rfloor \le q - 1$. The set in Equation (2.7) is simply

  $$P_d^\circ \cap \mathrm{Red}(d) = \bigcup_{1 \le y \le \mu_b} \left\{ (x,y) : 1 \le x \le \left\lfloor \frac{d-1-by}{a} \right\rfloor \right\} \subset T(d).$$

  In this case, the whole reduction $\mathrm{Red}(d)$ is the union of
  - $R(d) = \{(0,0)\} \cup E_x(d)$ which contains the reductions of the vertex $(0,0)$ and of the horizontal edge,
  - $T(d) = \{(x,y) : 0 \le x \le \left\lfloor \frac{d-1-by}{a} \right\rfloor$ and $1 \le y \le \mu_b\}$, which consists of the reduction of the vertical edge $E_y(d)$ and of the interior of $P_d$,
  - $H(d)$, the lattice points among the last two vertices and the reduction of the interior of the edge lying on the line $ax + by = d$.

- If $\ell \geq 1$, then by the virtue of Remark 2.9, we can rewrite Equation (2.7) as follows.

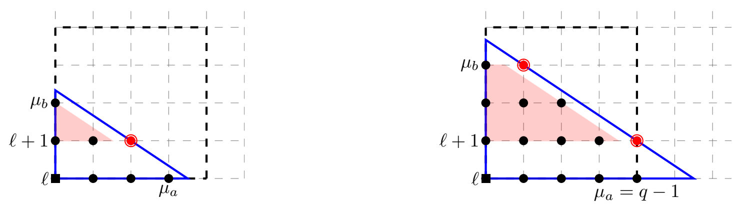
$$P_d^\circ \cap \mathrm{Red}(d) = \bigcup_{1 \leq y \leq \ell} \{(x,y) : 1 \leq x \leq q-1 = \mu_a\}$$
$$\cup \bigcup_{\ell+1 \leq y \leq \mu_b} \left\{(x,y) : 1 \leq x \leq \left\lfloor \frac{d-1-by}{a} \right\rfloor \right\}.$$

  The first union lies in the rectangular area $R(d)$, whereas the second union lies in the trapeze area $T(d)$.

In both cases, the description given via Equation (2.2) agrees with the one given in the statement, which completes the proof. □

**Example 2.11.** *Let $q = 5$, $X = \mathbb{P}(1,2,3)$ and $Y = X(\mathbb{F}_q)$.*

*Firstly let $d = 7$. We count the number of points of* $\mathrm{Red}(d)$ *in Figure 2a. Clearly, $\ell = 0$ and $R(d) = \{(0,0),(1,0),(2,0),(3,0)\}$. So, $|R(d)| = 4$. Similarly, we have $T(d) = \{(0,1),(1,1),(0,2)\}$. Thus, $|T(d)| = 3$. Also, since $H(d) = \{(2,1)\}$ we get $|H(d)| = 1$. Therefore,* $\dim_{\mathbb{F}_5}(C_{7,Y}) = |\mathrm{Red}(7)| = 4+3+1 = 8$.

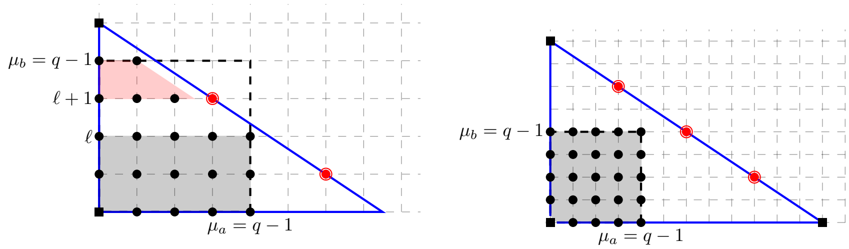



(A) $\mathrm{Red}(7) = P_7 \cap \mathbb{Z}^2$ with $\ell = 0$, $\mu_a = 3$ *and* $\mu_b = 2$.

(B) $\mathrm{Red}(11)$ with $\ell = 0$, $\mu_a = 4$ and $\mu_b = 3$

FIGURE 2. The set $\mathrm{Red}(d)$ for $d = 7, 11$ with $(q,a,b) = (5,2,3)$.

*Figure 2b shows $|R(11)| = 5$, $|T(11)| = 8$, $|H(11)| = 2$ and* $\dim_{\mathbb{F}_5}(C_{11,Y}) = 15$.




(A) $\mu_a = \mu_b = q-1$ and $T(15) \neq \varnothing$

(B) $\ell = \mu_a = \mu_b = q-1$ and $T(24) = \varnothing$

FIGURE 3. The set $\mathrm{Red}(d)$ for $d = 15, 24$ with $(q,a,b) = (5,2,3)$.

*Figure 3a reveals similarly that* $\dim_{\mathbb{F}_5}(C_{15,Y}) = 15+5+3 = 23$.
*Finally, Figure 3b proves that* $\dim_{\mathbb{F}_5}(C_{24,Y}) = 25+5 = 30$.

Example 2.11 illustrates how the dimension of the code $C_d$ can be computed combinatorially by using Theorem 2.8 and Lemma 2.10.

In order to express the cardinality of the set $H(d)$, we appeal to a very classical function in the theory of numerical semigroups.

**Definition 2.12.** *[18] Let $a, b$ and $d$ be positive integers. The **denumerant** function $\mathrm{den}(d; a, b)$ is defined as the number of non-negative integer representations of $d$ by $a$ and $b$, that is, the number of solutions $(m_a, m_b) \in \mathbb{N}^2$ of*

$$d = m_a a + m_b b.$$

The quantity $den(d; a, b)$ is positive if and only if $d$ belongs to the semigroup $\langle a, b\rangle_{\mathbb{N}}$ generated by $a$ and $b$ over $\mathbb{N}$. It is known that (see [18, Chapter 4] or [20]) if $d = \lambda ab + s$ with $0 \leq s < ab$ then $den(d; a, b) = \lambda + den(s; a, b)$ with $den(s; a, b) \in \{0, 1\}$. More precisely, we have

$$\mathrm{den}(s; a, b) = \begin{cases} 0 \text{ or } 1 & \text{if } 0 < s < ab \\ 1 & \text{for all } ab - a - b < s < ab \\ 0 & \text{if } s = ab - a - b. \end{cases}$$

**Theorem 2.13.** *Let $Y = \mathbb{P}(1, a, b)(\mathbb{F}_q)$ for two relatively prime positive integers $a \leq b$. Let $d \geq 1$ and let $\ell$ be as in Remark 2.9. We write $\mathbf{1}_{a|d}$ (resp. $\mathbf{1}_{b|d}$) for the integer being $1$ when $a$ (resp. $b$) divides $d$, and $0$ otherwise.*

*Then, the dimension of the code $C_d$ is given by*

$$\dim_{\mathbb{F}_q}(C_d) = (\ell + 1)\mu_a + \mu_b + 1 + \sum_{y=\ell+1}^{\mu_b} \left\lfloor \frac{d - 1 - by}{a} \right\rfloor + |H(d)| \tag{2.8}$$

*where*

$$|H(d)| = \begin{cases} \mathrm{den}(d; a, b) & \text{if } d \leq ab(q-1), \\ q - 1 + \mathbf{1}_{a|d} + \mathbf{1}_{b|d} & \text{if } d > ab(q-1). \end{cases}$$

*Proof.* By Theorem 2.8, the dimension of $C_d$ is equal to the number of lattice points inside $\mathrm{Red}(d)$. By Lemma 2.10, we have

$$\mathrm{Red}(d) = R(d) \cup T(d) \cup H(d).$$

Clearly, the cardinality of the set $R(d)$ of lattice points of the rectangular area is

$$|R(d)| = (\ell + 1)(\mu_a + 1) = (\ell + 1)\mu_a + \ell + 1. \tag{2.9}$$

As the definition of $\ell$ ensures that $\mu_b \geq \ell$, the set $T(d)$ is empty when $\mu_b = \ell$ so the sum in Equation (2.8) means 0. Furthermore, when $\mu_b \geq \ell + 1$, $T(d)$ is the set of lattice points of a trapezoidal region with cardinality

$$|T(d)| = \sum_{y=\ell+1}^{\mu_b} \left( \left\lfloor \frac{d - 1 - by}{a} \right\rfloor + 1 \right) = \mu_b - \ell + \sum_{y=\ell+1}^{\mu_b} \left\lfloor \frac{d - 1 - by}{a} \right\rfloor. \tag{2.10}$$

It remains to deal with the cardinality of $H(d) = E_h(d) \cup [\{(0, \frac{d}{b}), (\frac{d}{a}, 0)\} \cap \mathbb{Z}^2]$, that is the set of lattice points of $\mathrm{Red}(d)$ lying on the hypotenuse of the triangle $P_d$. It is clear that $\mathrm{den}(d; a, b)$ is the number of lattice points on the hypotenuse of the triangle $P_d$, which are equivalent, containing the corners if they have integral coordinates. As $|E_h(d)| = \min\{q - 1, i_{max} + 1\}$, we have the following formula

$$i_{max} + 1 = \mathrm{den}(d, a, b) - \epsilon \text{ where } \epsilon = \mathbf{1}_{a|d} + \mathbf{1}_{b|d} \tag{2.11}$$

and $|H(d)|$ can be reformulated as follows

$$|H(d)| = \min\{q - 1 + \epsilon, \mathrm{den}(d; a, b)\}. \tag{2.12}$$

Recall that if $d = \lambda ab + s$ with $0 \leq s < ab$ then $\operatorname{den}(d;a,b) = \lambda + \operatorname{den}(s;a,b)$ with $\operatorname{den}(s;a,b) \in \{0,1\}$ depending on whether $s \in \langle a,b\rangle_{\mathbb{N}}$ or not.

- When $d < ab(q-1)$, we have $\lambda < q-1$ and $\operatorname{den}(d;a,b) \leq q-1$. As $\epsilon \geq 0$, we clearly have $|H(d)| = \operatorname{den}(d;a,b)$.
- If $d = (q-1)ab$, then both $a|d$ and $b|d$ so $\epsilon = 2$. Besides
$$\operatorname{den}(d;a,b) = q-1+\operatorname{den}(0;a,b) = q \leq q-1+\epsilon.$$
Therefore, $|H(d)| = \operatorname{den}(d;a,b)$.
- Now assume that $d > ab(q-1)$. Then $\operatorname{den}(d;a,b) \geq q-1+\operatorname{den}(s;a,b)$.
  - If $\epsilon = 0$, Equation (2.12) gives $|H(d)| = q-1$.
  - If $\epsilon = 1$, then either $a$ or $b$ divides $s$, which implies that $\operatorname{den}(s;a,b) = 1$. So $\operatorname{den}(d;a,b) \geq q = q-1+\epsilon$, hence $|H(d)| = q$.
  - If $\epsilon = 2$, then both $a$ or $b$ divides $d$, which means that $d = \lambda ab$ for some integer $\lambda \geq q$. Then, we have
$$\operatorname{den}(d;a,b) = \lambda + \operatorname{den}(0;a,b) = \lambda + 1 \geq q-1+\epsilon,$$
and $|H(d)| = q+1$.

The quantities in Equations (2.9), (2.10) and (2.12) add up to the number in the stated formula in Equation (2.8), completing the proof. □

**Corollary 2.14.** *Let $Y = \mathbb{P}(1,1,b)(\mathbb{F}_q)$ for a positive integer $b$ and $d \geq 1$. Then, we have $\ell = \max\left\{0, \min\left\{q-1, \left\lfloor \frac{d-q}{b} \right\rfloor\right\}\right\}$ and $\dim_{\mathbb{F}_q}(C_d)$ is given by*
$$(\ell+1)(\mu_a+1) + (\mu_b-\ell)d - b\binom{\mu_b+1}{2} + b\binom{\ell+1}{2} + \mu_b + 1 + \mathbf{1}_{b|d}.$$

*In addition, we have $\ell = 0$ and $\mu_a = d-1$ if $d \leq q$.*

*Proof.* If $a = 1$, then $\mu_a = \min\{q-1, d-1\}$ and Equation (2.8) becomes
$$\dim_{\mathbb{F}_q}(C_d) = (\ell+1)\mu_a + \mu_b + 1 + \sum_{y=\ell+1}^{\mu_b} (d-1-by) + |H(d)|.$$

Rearranging this sum we get the following formula
$$\begin{aligned}\dim_{\mathbb{F}_q}(C_d) &= (\ell+1)\mu_a + \mu_b + 1 + (\mu_b-\ell)(d-1) - b\sum_{y=\ell+1}^{\mu_b} y + |H(d)| \\ &= (\ell+1)(\mu_a+1) + (\mu_b-\ell)d - b\binom{\mu_b+1}{2} + b\binom{\ell+1}{2} + |H(d)|.\end{aligned}$$

Since $E_h(d) = \emptyset$ if $d \leq b$ and $N_0 = (x', y') = (d-b, 1)$ is the first interior lattice point if $d > b$, it follows from Equation (2.6) that we have
$$E_h(d) = |\{(d-by, y) : 1 \leq y \leq \mu_b\}| = \mu_b.$$

Therefore, we get $|H(d)| = |E_h(d)| + 1 + \mathbf{1}_{b|d} = \mu_b + 1 + \mathbf{1}_{b|d}$ as desired. □

**Remark 2.15.** *The formula for the dimension agrees with [13, Theorem 6.4] for the case $a = b = 1$.*

## 3. The Regularity Set

In this section, we describe the so–called regularity set of the $\mathbb{F}_q$-rational points $Y = \mathbb{P}(1,a,b)(\mathbb{F}_q)$ of the weighted projective plane $\mathbb{P}(1,a,b)$. The importance of this set stems from the fact that its elements give rise to trivial codes as we explain shortly. Recall that the Hilbert function of a *zero dimensional* subvariety $Y$ of the weighted projective plane $\mathbb{P}(1,a,b)$ is defined to be the Hilbert function of the ring $S/I(Y)$:

$$H_Y(d) := \dim_{\mathbb{K}} S_d - \dim_{\mathbb{K}} I_d(Y) = \dim_{\mathbb{F}_q} S_d - \dim_{\mathbb{F}_q} I_d(Y),$$

where $I_d(Y) := I(Y) \cap S_d$ is the degree–$d$ part of the vanishing ideal $I(Y)$ generated by the homogeneous polynomials vanishing on $Y$. If $Y = \mathbb{P}(1,a,b)(\mathbb{F}_q)$, the kernel of the evaluation map in (1.3) is $I_d(Y)$ and hence $\dim_{\mathbb{F}_q} C_d = H_Y(d) \leq |Y|$.

**Definition 3.1.** *The regularity set of $Y = \mathbb{P}(1,a,b)(\mathbb{F}_q)$ is defined by*

$$\operatorname{reg}(Y) = \{d \in \mathbb{N}W : H_Y(d) = |Y|\}.$$

**Remark 3.2.** *If $d \in \operatorname{reg}(Y)$ then the dimension of the code is maximum possible, i.e. $C_d = \mathbb{F}_q^n$, where $n = |Y|$. Thus, it is a trivial code with parameters $[n, n, 1]$.*

**Proposition 3.3.** *Let $a$ and $b$ be two relatively prime integers with $1 \leq a \leq b$. An integer $d$ belongs to the regularity set of $Y = \mathbb{P}(1,a,b)(\mathbb{F}_q)$ if and only if there exists $d_0 \geq q$ such that $d = d_0ab$ and $(a+b)(q-1) < d$.*

*Proof.* It follows from the description of $\operatorname{Red}(d)$ given by Lemma 2.10 that $d \in \operatorname{reg}(Y)$ if and only if $|\operatorname{Red}(d)| = |Y| = q^2 + q + 1 = (q-1)^2 + 3(q-1) + 3$ if and only if $|P_d^\circ| = (q-1)^2$, $|E_x(d)| = |E_y(d)| = |E_h(d)| = q-1$, $a \mid d$ and $b \mid d$.

One can easily check that $|P_d^\circ| = (q-1)^2$ if and only if the point $(q-1, q-1)$ lies in the interior of $P_d$, which is equivalent to $(a+b)(q-1) < d$. In this case, $(q-1, 0) \in E_x(d)$ and $(0, q-1) \in E_y(d)$, so $|E_x(d)| = |E_y(d)| = q-1$.

Since the integers $a$ and $b$ are coprime, $a \mid d$ and $b \mid d$ if and only if $ab \mid d$ which is equivalent to the fact that there exists an integer $d_0$ such that $d = d_0ab$. Then $\operatorname{den}(d; a, b) = d_0 + 1$. By Equation 2.11,

$$|E_h(d)| = \min\{q-1, \operatorname{den}(d; a, b) - 2\} = q - 1 \Leftrightarrow d_0 \geq q,$$

which concludes the proof. □

**Theorem 3.4.** *Let $a$ and $b$ be two relatively prime positive integers with $1 < a < b$. The regularity set of $Y = \mathbb{P}(1,a,b)(\mathbb{F}_q)$ is given as follows.*

$$\operatorname{reg}(Y) = \{d \in \mathbb{N} : d = d_0ab \text{ with } d_0 \geq q\} = qab + \mathbb{N}ab.$$

*Proof.* By Proposition 3.3, it is enough to check that writing $d = d_0ab$ with $d_0 \geq q$ implies that $(a+b)(q-1) < d$.

Since $a \geq 2$ and $b > a$ we have $ab \geq 2b > a + b$, leading to the following

$$d = d_0ab \geq qab \geq q(a+b) > (q-1)(a+b)$$

completing the proof. □

We also recover [9, Corollary 3.9] more directly in the case $a = 1$.

**Theorem 3.5.** *Let $b$ be a positive integer. The regularity set of $Y = \mathbb{P}(1,1,b)(\mathbb{F}_q)$ is given as follows.*

$$\operatorname{reg}(Y) = \{d \in \mathbb{N} : d = d_0b \text{ with } d_0 \geq q + \lfloor (q-1)/b \rfloor\} = \left(q + \left\lfloor \frac{q-1}{b} \right\rfloor\right) b + \mathbb{N}b.$$

*Proof.* By noticing that

$$d_0 b > (1+b)(q-1) \iff d_0 \geq \left\lfloor \frac{q-1}{b} \right\rfloor + q,$$

the proof follows straightforwardly from Proposition 3.3. $\square$

## 4. A lower bound for the minimum distance

In this section we aim at grasping the minimum distance of a projective weighted Reed-Muller code obtained from $\mathbb{P}(1,a,b)$ by first establishing a lower bound. For every $f \in S_d \setminus I_d(Y)$, we denote by $Y_f$ the subvariety $V_Y(f)$ of $Y$ consisting of the roots of $f$ and we write $n_f := |Y_f|$. As usual for evaluation codes, we have

$$d_{min}(C_d) = n - \max\{n_f : f \in S_d \setminus I_d(Y)\}.$$

By the virtue of Remark 3.2, from now on, we assume that $d \in \mathbb{N} \setminus \mathrm{reg}(Y)$. To give a lower bound on the minimum distance, it suffices to give an upper bound on $n_f$. Such a bound can be obtained using Gröbner basis theory, which is known in the literature as *the footprint bound*, see e.g. [5, 12, 14] for the affine and projective space cases, [15] for Hirzebruch surfaces, and [16] for more general toric varieties.

The *footprint* of a homogeneous ideal $I$ of $S$ with respect to a monomial ordering $\prec$ on the set $\mathbb{M}$ of all monomials in $S$ is defined as follows

$$\Delta(I) := \{M \in \mathbb{M} : M \neq \mathrm{LM}(g) \text{ for any } g \in I \text{ with } g \neq 0\}.$$

A relevant *finite* subset is $\Delta_{\tilde{d}}(I) = \Delta(I) \cap \mathbb{M}_{\tilde{d}}$ for $\tilde{d} \in \mathbb{N}$. It is well known from Gröbner basis theory that a monomial $M \neq \mathrm{LM}(g)$ for any $g \in I \setminus \{0\}$ if and only if $\mathrm{LM}(g) \nmid M$ for any $g$ in the Gröbner basis of $I$ with respect to $\prec$. By [22, Proposition 1.1], the value $H_I(\tilde{d})$ of the Hilbert function of $I$ at $\tilde{d} \in \mathbb{N}$ is the cardinality of $\Delta_{\tilde{d}}(I)$. In particular, it implies that $\left|\Delta_{\tilde{d}}(I)\right|$ is independent of the ordering $\prec$.

We rewrite [16, Lemma 5.5] in the notation used here.

**Lemma 4.1.** *[16, Lemma 5.5] Let $Y = \mathbb{P}(1,a,b)(\mathbb{F}_q)$ and $I(Y,f)$ denote the ideal $I(Y)+(f)$, for a homogeneous polynomial $f \in S$. Then for any $f \in S_d \setminus I_d(Y)$ and $\tilde{d} \in \mathrm{reg}(Y)$, we have $n_f \leq \tilde{n}_f(\tilde{d}) := H_{I(Y,f)}(\tilde{d}) = |\Delta_{\tilde{d}}(I(Y,f))|$.* $\square$

By [7, Theorem 4.3.5] there exists a uniquely determined quasi-polynomial $P_M$ with $H_M(d) = P_M(d)$ for all $d > a(M)$ for the module $M = S/I(Y,f)$, where $a(M)$ denotes the degree of the rational function representing the Hilbert series $HS_M(t)$. In other words, there exists a positive integer $g$ (period) and some polynomials $P_0, \dots, P_{g-1}$ such that $H_M(d) = P_i(d)$ for $d > a(M)$ and $d \equiv i \mod g$.

Since $I(Y) \subseteq I(Y,f) \subseteq I(Y_f)$, the Krull dimension of $I(Y,f)$ is 1, if $f$ is a zerodivisor of $S/I(Y)$. Therefore, the Hilbert quasi-polynomial of $S/J$ has degree 0 if $J = I(Y,f)$ and $f$ is a zerodivisor of $S/I(Y)$, see [8, Proposition 5] or [4]. Therefore, there are finitely many constants appearing as the values of $\tilde{n}_f(\tilde{d})$ for sufficiently large $\tilde{d}$. We thus define $\tilde{n}_f$ as the maximum of all these constants. This gives the following lower bound for the minimum distance.

$$d_{min}(C_d) \geq n - \max\{\tilde{n}_f : f \in S_d \setminus I_d(Y) \text{ is a zerodivisor of } S/I(Y)\}. \tag{4.1}$$

4.1. **A lower bound for the minimum distance using Gröbner basis theory.** In practice, it is difficult to compute Hilbert quasi-polynomials to get $\tilde{n}_f$. Therefore, we appeal to a classical trick (see [14, Lemma 2.5] for instance) of Gröbner basis theory to give an easy upper bound for $\tilde{n}_f(\tilde{d})$, which will be independent of $\tilde{d}$.

**Lemma 4.2.** *Let $X$ be a simplicial toric variety and $Y \subset X$ a subvariety.*

*Let $\mathcal{G}$ denote the Gröbner basis of $I(Y)$ with respect to a term order $\prec$. Let*

$$\overline{\Delta}_{\tilde{d}}(f) = \left\{ M \in \mathbb{M}_{\tilde{d}} : \forall g \in \mathcal{G} \cup \{f\}\,,\ LM(g) \nmid M \right\}.$$

*Then, for any $f \in S_d \setminus I_d(Y)$ we have*

$$\tilde{n}_f(\tilde{d}) = H_{I(Y,f)}(\tilde{d}) \leq \left|\overline{\Delta}_{\tilde{d}}(f)\right|, \tag{4.2}$$

*and $\tilde{n}_f(\tilde{d}) = \left|\overline{\Delta}_{\tilde{d}}(f)\right| \iff \mathcal{G} \cup \{f\}$ is the Gröbner basis of $I(Y,f)$ for $\prec$.* □

In our case, *i.e.* $X = \mathbb{P}(1,a,b)$ and $Y = X(\mathbb{F}_q)$, the set of monomials of degree $\tilde{d}$ that are not divisible by $\mathrm{LM}(g)$ for all $g \in \mathcal{G}$ (for $\prec = <_{\mathrm{lex}}$) is $\overline{\mathbb{M}}_{\tilde{d}}$. Thus,

$$\overline{\Delta}_{\tilde{d}}(f) = \left\{ M \in \overline{\mathbb{M}}_{\tilde{d}} : \mathrm{LM}(f) \nmid M \right\}. \tag{4.3}$$

For the upper bound $\left|\overline{\Delta}_{\tilde{d}}(f)\right|$, it suffices to consider $f$ to be a monomial as $\overline{\Delta}_{\tilde{d}}(f) = \overline{\Delta}_{\tilde{d}}(\mathrm{LM}(f))$. We can also assume that $\mathrm{LM}(f) = \mathbf{x}^{\mathbf{a},d}$ with $\mathbf{a} \in \mathrm{Red}(d)$. Thus, for a fixed $\mathbf{a} \in \mathrm{Red}(d)$ and $\tilde{d} \geq d$, we consider the *projective shadow* in degree $\tilde{d}$ of the monomial $\mathbf{x}^{\mathbf{a},d}$

$$\overline{\nabla}_{\tilde{d}}(\mathbf{x}^{\mathbf{a},d}) = \left\{ \mathbf{x}^{\tilde{\mathbf{a}},\tilde{d}} \in \overline{\mathbb{M}}_{\tilde{d}} : \mathbf{x}^{\tilde{\mathbf{a}},\tilde{d}} \text{ is divisible by } \mathbf{x}^{\mathbf{a},d} \right\} = \overline{\mathbb{M}}_{\tilde{d}} \setminus \overline{\Delta}_{\tilde{d}}(\mathbf{x}^{\mathbf{a},d}).$$

**Corollary 4.3.** *Consider the lexicographic order $\prec = <_{lex}$. Suppose that $\tilde{d} \in \mathrm{reg}(Y)$. Then for every $f \in S_d \setminus I(Y)$, we have*

$$\left|\overline{\Delta}_{\tilde{d}}(f)\right| = \left|\overline{\Delta}_{\tilde{d}}(LM(f))\right| = n - \overline{\nabla}_{\tilde{d}}(LM(f)).$$

*Proof.* When $\tilde{d} \in \mathrm{reg}(Y)$, $|\overline{\mathbb{M}}_{\tilde{d}}| = H_{I(Y)}(\tilde{d}) = n$. The formula for the cardinality of $\left|\overline{\Delta}_{\tilde{d}}(f)\right|$ follows directly from Equation (4.3). □

For every $\mathbf{a} \in \mathrm{Red}(d)$ and $\tilde{d} \in \mathrm{reg}(Y)$, we set

$$L(\mathbf{a},\tilde{d}) := \left|\overline{\nabla}_{\tilde{d}}(\mathbf{x}^{\mathbf{a},d})\right| = n - \left|\overline{\Delta}_{\tilde{d}}(\mathbf{x}^{\mathbf{a},d})\right|. \tag{4.4}$$

**Lemma 4.4.** *Let $d \in \mathbb{N} \setminus \mathrm{reg}(Y)$ and $\tilde{d} \in \mathrm{reg}(Y)$. Then*

$$d_{min}(C_d) \geq \min\left\{ L(\mathbf{a},\tilde{d}) : \mathbf{a} \in \mathrm{Red}(d) \right\}.$$

*Proof.* Clearly, we have

$$d_{min}(C_d) = n - \max\{|V_Y(f)| : f \in S_d \setminus I_d(Y)\}.$$

Let $f \in S_d \setminus I_d(Y)$ and write $\mathrm{LM}(f) = \mathbf{x}^{\mathbf{a},d}$. By Theorem 2.8, we can assume that $\mathbf{a} \in \mathrm{Red}(d)$. Lemmas 4.1 and 4.2 imply that $|V_Y(f)| \leq \left|\overline{\Delta}_{\tilde{d}}(\mathrm{LM}(f))\right|$, and thus

$$d_{min}(C_d) \geq n - \max\{\left|\overline{\Delta}_{\tilde{d}}(\mathbf{x}^{\mathbf{a},d})\right| : \mathbf{a} \in \mathrm{Red}(d)\} = \min\{L(\mathbf{a},\tilde{d}) : \mathbf{a} \in \mathrm{Red}(d)\},$$

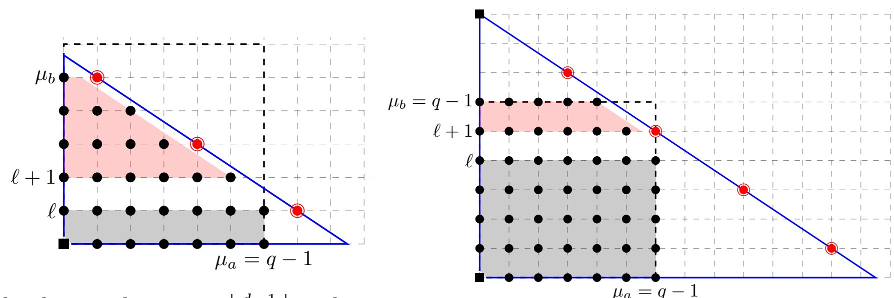
as claimed. □

**Remark 4.5.** *Let* $\mathbf{a} \in \operatorname{Red}(d)$*. When* $\tilde{d} \in \operatorname{reg}(Y)$*, the monomials* $x_0^{\tilde{d}}$*,* $x_1^{\tilde{d}/a}$ *and* $x_2^{\tilde{d}/b}$ *must belong to* $\overline{\mathbb{M}}_{\tilde{d}}$*. So, if* $\mathbf{x}^{\mathbf{a},d}$ *divides two of these, it must be a constant forcing* $d = 0$*. Then if* $d \geq 1$*, we have* $L(\mathbf{a}, \tilde{d}) \leq n - 2$*. Moreover, if* $d \leq \tilde{d}$*, the monomial* $\mathbf{x}^{\mathbf{a},d}$ *divides* $\mathbf{x}^{\mathbf{a},\tilde{d}}$*, resulting in* $L(\mathbf{a}, \tilde{d}) \geq 1$ *as* $d \notin \operatorname{reg}(Y)$*. As a consequence, the bound provided by Lemma 4.4 is not trivial.*

4.2. **Computation of the lower bound for the minimum distance.** Our strategy is the following. We first get rid of the dependency of the lower bound on the degree $\tilde{d}$: Proposition 4.6 provides a formula for the cardinality of the projective shadow of monomials in $\overline{\mathbb{M}}_d$ in degree $\tilde{d}$ that do not depend on $\tilde{d}$.

We will then determine the minimum of $L = L(\cdot, \tilde{d})$ on the convex area $\operatorname{Red}(d) \cap \{a_2 \leq \mu_b\}$ in §4.2.1. One can easily check from the definition of $\operatorname{Red}(d)$ that

- if $d \leq bq - 1$, then $\mu_b = \left\lfloor \frac{d-1}{b} \right\rfloor$ and $a_2 \leq \mu_b$ for every $\mathbf{a} \in \operatorname{Red}(d)$ except for $\mathbf{a} = (0, d/b)$ in the case $b \mid d$ (see Figure 4a for an example);
- if $d \geq bq$, then $\mu_b = q - 1$. If $d - bq \in \langle a, b \rangle$, then there exists some $\mathbf{a} = (a_1, a_2) \in \operatorname{Red}(d)$ such that $a_2 \geq q$. By definition of $\operatorname{Red}(d)$ such an element $\mathbf{a}$ should belong to $H(d)$ (see Figure 4b for an example). In this case, we will have to compare the minimum on the area $\operatorname{Red}(d) \cap \{a_2 \leq \mu_b\}$ and the values outside, which is the heart of §4.3.




(A) $d \leq bq - 1$ then $\mu_b = \left\lfloor \frac{d-1}{b} \right\rfloor$ and $a_2 \leq \mu_b$ for every $\mathbf{a} \in \operatorname{Red}(d)$

(B) $d \geq bq$, then $\mu_b = q - 1$.

FIGURE 4. Lattice points $\mathbf{a} \in \operatorname{Red}(d)$ for $\mathbb{P}(1,2,3)(\mathbb{F}_7)$, and $d = 17$ and $d = 27$ respectively.

**Proposition 4.6.** *For* $\tilde{d} \in \operatorname{reg}(Y)$ *satisfying* $\tilde{d} \geq d + (q-1)\max\{a+b, ab\}$ *and for every* $\mathbf{a} = (a_1, a_2) \in \operatorname{Red}(d)$*, the quantity* $L(\mathbf{a}, \tilde{d})$ *does not depend on* $\tilde{d}$ *and equals the following number denoted by* $L(\mathbf{a})$

$$\begin{cases} (q-a_1)(q-a_2) & \text{if } aa_1 + ba_2 \neq d \\ \max\{q-a_1, 0\}\max\{q-a_2, 0\} + q - 1 - \left\lfloor \frac{a_2-1}{a} \right\rfloor & \text{if } aa_1 + ba_2 = d \text{ and } a_1 \neq 0, \\ q \cdot \max\{q - \frac{d}{b}, 0\} + \max\{q - \left\lfloor \frac{d-b}{ab} \right\rfloor, 1\} & \text{if } (a_1, a_2) = (0, \frac{d}{b}) \text{ and } b \mid d. \end{cases}$$

*Proof.* Fix $\mathbf{a} = (a_1, a_2) \in \operatorname{Red}(d)$ and let $\mathbf{x}^{\mathbf{a},d} = x_0^{d - aa_1 - ba_2} x_1^{a_1} x_2^{a_2}$. Let us count the number of couples $\tilde{\mathbf{a}} = (\tilde{a}_1, \tilde{a}_2) \in \operatorname{Red}(\tilde{d})$ such that the monomial $\mathbf{x}^{\mathbf{a},d}$ divides $\mathbf{x}^{\tilde{\mathbf{a}},\tilde{d}} = x_0^{\tilde{d} - a\tilde{a}_1 - b\tilde{a}_2} x_1^{\tilde{a}_1} x_2^{\tilde{a}_2}$. We clearly have the following equivalence.

$$\mathbf{x}^{\mathbf{a},d} \text{ divides } \mathbf{x}^{\tilde{\mathbf{a}},\tilde{d}} \iff \begin{cases} a_1 & \leq & \tilde{a}_1, \\ a_2 & \leq & \tilde{a}_2 \\ d - aa_1 - ba_2 & \leq & \tilde{d} - a\tilde{a}_1 - b\tilde{a}_2. \end{cases} \tag{4.5}$$

Before going further, let us notice that the hypothesis $\tilde{d} \in \operatorname{reg}(Y)$ ensures that $|\operatorname{Red}(\tilde{d})| = q^2 + q + 1$. In particular, $\operatorname{Red}(\tilde{d}) = R(\tilde{d}) \cup H(\tilde{d})$ with

$$R(\tilde{d}) = \{(\tilde{a}_1, \tilde{a}_2) \in \mathbb{Z}^2 : 1 \leq \tilde{a}_1 \leq q-1 \text{ and } 1 \leq \tilde{a}_2 \leq q-1\} \tag{4.6}$$

and

$$H(\tilde{d}) = \{(b(d_0 - y_0), y_0 a) \in \mathbb{Z}^2 : 0 \leq y_0 \leq q-1 \text{ and } y_0 = d_0\}, \tag{4.7}$$

where $\tilde{d} = d_0 ab$, for some $d_0 \in \mathbb{N}$ with $d_0 \geq q$ (see Proposition 3.3).

If $\mathbf{a} = (a_1, a_2) \in \operatorname{Red}(d) \setminus H(d)$ then $aa_1 + ba_2 < d$ and so a necessary requirement for the third condition to hold in (4.5) is to have $a\tilde{a}_1 + b\tilde{a}_2 < \tilde{d}$ as well. This means that $(\tilde{a}_1, \tilde{a}_2) \in R(\tilde{d})$ and so $\tilde{a}_1 \leq q-1$ and $\tilde{a}_2 \leq q-1$. Then

$$\tilde{d} - d \geq (q-1)(a+b) \geq a\tilde{a}_1 + b\tilde{a}_2 \geq a(\tilde{a}_1 - a_1) + b(\tilde{a}_2 - a_2),$$

implying the third condition in (4.5). Hence, all the conditions in (4.5) hold for $0 \leq a_1 \leq \tilde{a}_1 \leq q-1$ and $0 \leq a_2 \leq \tilde{a}_2 \leq q-1$. Therefore, $\tilde{a}_1$ and $\tilde{a}_2$ respectively admit $q - a_1$ and $q - a_2$ possible values, proving the first description of $L$.

Now assume that $\mathbf{a} \in H(d) \setminus \{(0, d/b)\}$. Then, $aa_1 + ba_2 = d$, which means that the third condition in (4.5) is satisfied, and we have $\mathbf{x}^{\mathbf{a},d}$ divides $\mathbf{x}^{\tilde{\mathbf{a}},\tilde{d}}$ if and only if $a_1 \leq \tilde{a}_1$ and $a_2 \leq \tilde{a}_2$. The number of such tuples $\tilde{\mathbf{a}} \in R(\tilde{d})$ is given by $\max\{q - a_1, 0\} \max\{q - a_2, 0\}$, as $a_1$ and $a_2$ may be larger than $q-1$ but $\tilde{a}_1 \leq q-1$ and $\tilde{a}_2 \leq q-1$. Note that $\mathbf{a} \neq (0, d/b)$ implies that $a_1 \geq 1$ and $0 \leq a_2 < aq$, see Equation (2.6). By Equation (4.7), for every $\tilde{\mathbf{a}} = (\tilde{a}_1, \tilde{a}_2) \in H(\tilde{d})$ we have

$$\begin{aligned} a_1 \leq \tilde{a}_1 \iff & \quad d - ba_2 \leq \tilde{d} - aby_0 \\ \iff & \quad aby_0 \leq \tilde{d} - d + ba_2 \end{aligned}$$

so the hypothesis $\tilde{d} \geq d + (q-1)\max\{a+b, ab\}$ reduces the condition $a_1 \leq \tilde{a}_1$ to $\tilde{a}_1 \geq 1$ for every $(\tilde{a}_1, \tilde{a}_2) \in H(\tilde{d}) \setminus \{(0, \tilde{d}/b)\}$. As there are exactly $\left\lfloor \frac{a_2 - 1}{a} \right\rfloor$ tuples $\tilde{\mathbf{a}}$ such that $\tilde{a}_2 = ay_0 < a_2$, we obtain the formula

$$L(\mathbf{a}) = \max\{q - a_1, 0\} \max\{q - a_2, 0\} + q - 1 - \left\lfloor \frac{a_2 - 1}{a} \right\rfloor$$

proving the second case.

Finally, assume that $\mathbf{a} = (0, d/b)$ with $b \mid d$. The only difference with the previous case is that $\tilde{a}_1$ can also be 0. So, inserting $a_1 = 0$, $a_2 = d/b$ in the previous formula, and adding 1 for the corner $(0, \tilde{d}/b)$, we obtain the last formula: $q \cdot \max\{q - \frac{d}{b}, 0\} + \max\{q - \left\lfloor \frac{d-b}{ab} \right\rfloor, 1\}$, completing the proof. $\square$

**Remark 4.7.** *Even though the second formula for $L(\mathbf{a})$ in Proposition 4.6 can take on the value 0, this occurs only if $\mathbf{a} \notin \operatorname{Red}(d)$, by the virtue of Remark 4.5.*

*We recover [5, Lemma 4.1] when plugging $a = b = 1$ in Proposition 4.6.*

The next example shows that the lower bound for $\tilde{d}$ in Proposition 4.6 is sharp.

**Example 4.8.** *Let $q = 2$, $X = \mathbb{P}(1, 1, 3)$ and $Y = X(\mathbb{F}_q)$. By Theorem 2.4, the following is the universal Gröbner basis for $I(Y)$:*

$$\mathcal{G} = \{f_0 = x_2^2 x_1 + x_2 x_1^4, f_1 = x_2^2 x_0 + x_2 x_0^4, f_2 = x_1^2 x_0 + x_1 x_0^2\}.$$

*One can compute the minimum distance of the code $C_{4,Y}$ to be 2 using one of the algorithms given by [3]. This reveals that a homogeneous polynomial $f$ having the* *maximum possible number of roots has $n_f = |Y| - 2 = 5$. We use this to analyze the smallest possible element $\tilde{d}$ for which Proposition 4.6 works.*

*For $d = (q-1)(a+b) = 4$, a basis for $S_d/I_d(Y)$ is given by*

$$\overline{\mathbb{M}}_4 = \{x_2x_1,\, x_2x_0,\, x_1^4,\, x_1x_0^3,\, x_0^4\}.$$

*For any $\tilde{d} \in \operatorname{reg}(Y)$, we have*

$$\overline{\mathbb{M}}_{\tilde{d}} = \{x_2^{\tilde{d}/3}, x_2x_1^{\tilde{d}-3}, x_2x_1x_0^{\tilde{d}-4}, x_2x_0^{\tilde{d}-3}, x_1^{\tilde{d}}, x_1x_0^{\tilde{d}-1}, x_0^{\tilde{d}}\}.$$

*Using the formulae of Proposition 4.6, we get*

$$L(a_1, a_2) = \begin{cases} 4 & \text{if } (a_1,a_2) = (0,0), \\ 2 & \text{if } (a_1,a_2) \in \{(1,1),(0,1),(4,0),(1,0)\}. \end{cases}$$

*Since $\operatorname{reg}(Y) = 6 + 3\mathbb{N}$ by Theorem 3.5, we first look at the values of the Hilbert function of $I(Y) + \langle f \rangle$ for every $f \in \overline{\mathbb{M}}_4$ and get*

$$H_{I(Y)+\langle f\rangle}(6) = \begin{cases} 6 & \text{for } f = x_1x_0^3, \\ 5 & \text{for } f \in \overline{\mathbb{M}}_4 \setminus \{x_1x_0^3\}. \end{cases}$$

*This reveals that for $f = x_1x_0^3$, $H_{I(Y)+\langle f\rangle}(6)$ is bigger than the biggest $n_f$.*

*However, taking $\tilde{d} \geq 2(q-1)(a+b) = 8$, i.e. $\tilde{d} \in 9 + 3\mathbb{N}$, remedies the problem. Indeed, one can observe that $\tilde{n}_f(\tilde{d}) = \left|\overline{\Delta}_{\tilde{d}}(f)\right| = 5$ for all $\tilde{d} \in 9 + 3\mathbb{N}$ and for $f = x_1x_0^3$, as the Gröbner basis of $I(Y) + \langle f\rangle$ is $\mathcal{G} \cup \{f\}$ and a basis for $S_{\tilde{d}}/I_{\tilde{d}}(Y,f)$ is obtained as $\overline{\Delta}_{\tilde{d}}(f) = \{x_2^{\tilde{d}/3}, x_2x_1^{\tilde{d}-3}, x_2x_0^{\tilde{d}-3}, x_1^{\tilde{d}}, x_0^{\tilde{d}}\}$.*

*For any $\tilde{d} \in 9 + 3\mathbb{N}$, we check that $\tilde{n}_f(\tilde{d}) = \left|\overline{\Delta}_{\tilde{d}}(f)\right| = 5$ for $f \in \{x_2x_1,\, x_2x_0\}$, $\tilde{n}_f(\tilde{d}) = 3 < \left|\overline{\Delta}_{\tilde{d}}(f)\right| = 5$ for $f = x_1^4$ and $\tilde{n}_f(\tilde{d}) = \left|\overline{\Delta}_{\tilde{d}}(f)\right| = 3$ for $f = x_0^4$.*

Example 4.8 shows that the minimum of the function $L$ on the set $\operatorname{Red}(d)$ provided by Lemma 4.4 seems to give the exact minimum distance. Let us start with large degrees $d$, corresponding to high rate codes $C_d$, for which the minimum value of the function $L$ is exactly equal to 1.

**Proposition 4.9.** *If $\tilde{d} \geq d > (a+b)(q-1)$, then* $\min_{\mathbf{a}\in\operatorname{Red}(d)} L(\mathbf{a}, \tilde{d}) = 1$.

*Proof.* The hypothesis $d > (a+b)(q-1)$ is equivalent to $(q-1, q-1)$ lying in $P_d^\circ$, hence in $\operatorname{Red}(d)$. The minimum of $L$ is thus clearly reached at this point, since $\mathbf{x}^{\tilde{\mathbf{a}},\tilde{d}}$ is divisible by $\mathbf{x}^{\mathbf{a},d} = x_0^{d-(q-1)(a+b)}x_1^{q-1}x_2^{q-1}$ if and only if $\tilde{a}_1 = q-1$, $\tilde{a}_2 = q-1$ and $\tilde{d} \geq d$. □

4.2.1. *Minimum of $L(a_1,a_2)$ on* $\operatorname{Red}(d) \cap \{a_2 \leq \mu_b\}$. Our first observation eliminates lots of the points $(a_1,a_2) \in \operatorname{Red}(d) \cap \{a_2 \leq \mu_b\}$ for which the function $L(a_1,a_2)$ does not attain its minimum value. In other words, it does not only say that the minimum is reached at an interior point but it also describes the $a_1$ coordinate of such a point on each horizontal line $y = a_2$ (see Figure 5).

**Lemma 4.10.** *Fix $a_2 \in \{0, \ldots, \mu_b\}$. Write $\mathcal{X}_{a_2} = \{a_1 \in \mathbb{N} : (a_1,a_2) \in \operatorname{Red}(d)\}$ and $M_{a_2} = \max \mathcal{X}_{a_2}$.*

*If $aM_{a_2} + ba_2 < d$, then the minimum of the univariate function $a_1 \mapsto L(a_1,a_2)$ on $\mathcal{X}_{a_2}$ is reached exactly at $a_1 = M_{a_2}$.*

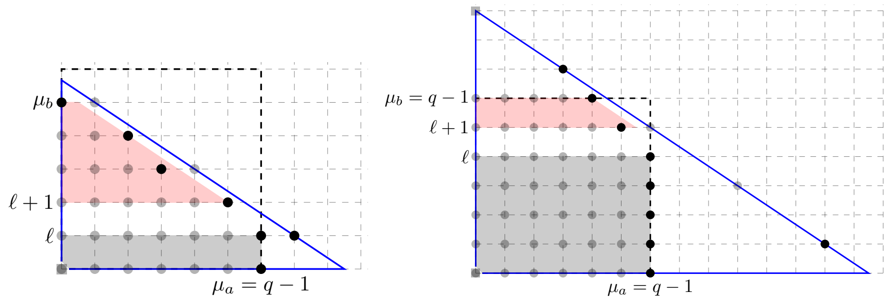



FIGURE 5. Candidates for the minimum of $L$ on $\mathrm{Red}(d) \cap \{a_2 \le \mu_b\}$ by virtue of Lemma 4.10 with $a, b = 2, 3$, $q = 7$ and the degrees $d = 17, 27$, respectively.

*If $aM_{a_2} + ba_2 = d$, then it is reached at*

$$\operatorname*{argmin}_{a_1 \in \mathcal{X}_{a_2}} L(\cdot, a_2) = \begin{cases} \{\min\{M_{a_2}, q\} - 1, M_{a_2}\} & \text{if } a_2 = 0, 1 \text{ or } a = 1, \\ \{\min\{M_{a_2}, q\} - 1\} & \text{otherwise.} \end{cases}$$

*Proof.* If $aM_{a_2} + ba_2 \neq d$, then $(M_{a_2}, a_2) \notin H(d)$ which means that $M_{a_2} \le q-1$. Therefore the function $a_1 \mapsto L(a_1, a_2)$ is defined by $L(a_1, a_2) = (q - a_1)(q - a_2)$ on the set $\mathcal{X}_{a_2}$ by Proposition 4.6. It is thus strictly decreasing with respect to $a_1$.

Otherwise, $aM_{a_2} + ba_2 = d$. Then $M_{a_2} \ge 1$ (as $a_2 \le \mu_b$) and it is clear that the function $a_1 \mapsto L(a_1, a_2)$ is strictly decreasing on $\mathcal{X}_{a_2} \setminus \{M_{a_2}\}$ and we have two cases:

(1) $M_{a_2} \le q$, which implies that $\mathcal{X}_{a_2} = \{0, \dots, M_{a_2}\}$.
(2) $M_{a_2} > q$, which corresponds to $\mathcal{X}_{a_2} = \{0, \dots, q-1\} \cup \{M_{a_2}\}$.

In the first case, it remains to compare

$$L(M_{a_2}, a_2) = (q - M_{a_2})(q - a_2) + q - 1 - \left\lfloor \frac{a_2 - 1}{a} \right\rfloor$$

and $L(M_{a_2} - 1, a_2) = (q - M_{a_2} + 1)(q - a_2) = (q - M_{a_2})(q - a_2) + q - a_2$. Computing the difference, we get

$$\begin{aligned} L(M_{a_2}, a_2) - L(M_{a_2} - 1, a_2) &= -1 - \left\lfloor \frac{a_2 - 1}{a} \right\rfloor + a_2 \\ &= \left\lceil \frac{(a-1)(a_2-1)}{a} \right\rceil \ge 0 \end{aligned}$$

In the second case, we just have to compare $L(M_{a_2}, a_2) = q - 1 - \left\lfloor \frac{a_2 - 1}{a} \right\rfloor$ and $L(q-1, a_2) = q - a_2$. Their difference also equals to

$$L(M_{a_2}, a_2) - L(q-1, a_2) = \left\lceil \frac{(a-1)(a_2-1)}{a} \right\rceil.$$

In both cases, the minimum of the function $a_1 \mapsto L(a_1, a_2)$ on $\mathcal{X}_{a_2}$ is thus reached by $\min\{M_{a_2}, q\} - 1$, and also by $M_{a_2}$ if $a_2 \in \{0, 1\}$ or $a = 1$. □

Let us define the following univariate function:

$$a_2 \mapsto \tilde{L}(a_2) = L\left(\min\left\{\left\lfloor \frac{d - 1 - ba_2}{a} \right\rfloor, q - 1\right\}, a_2\right) \tag{4.8}$$

**Corollary 4.11.** *Under the hypothesis above, we have*

$$\min_{\substack{(a_1,a_2)\in \mathrm{Red}(d)\\ a_2\leq \mu_b}} L(a_1,a_2) = \min_{a_2\in\{0,\dots,\mu_b\}} \tilde{L}(a_2)$$

*Proof.* This directly follows from Lemma 4.10, noticing that

$$\min\left\{\left\lfloor\frac{d-1-ba_2}{a}\right\rfloor, q-1\right\} = \begin{cases} M_{a_2} & \text{if } aM_{a_2}+ba_2<d,\\ \min\{M_{a_2},q\}-1 & \text{if } aM_{a_2}+ba_2=d,\end{cases}$$

completing the proof. □

Recall the number $\alpha_2 = \left\lfloor \frac{d-1-a(q-1)}{b}\right\rfloor$ as described in Remark 2.9. To obtain the minimum value of the function $L(a_1,a_2)$ on $\mathrm{Red}(d)\cap\{a_2\leq\mu_b\}$, let us study how the univariate function $\tilde{L}$ varies on $\{0,\dots,\mu_b\}$.

**Remark 4.12.** *The hypothesis $a\leq b$ implies that if $(a_1,a_2)\in \mathrm{Red}(d)\setminus H(d)$ with $a_2>a_1$, then so does $(a_2,a_1)$. Moreover, the function $L$ defined in Proposition 4.6 is clearly symmetric on the interior of $P_d$, i.e. $L(a_1,a_2)=L(a_2,a_1)$ if both $(a_1,a_2)$ and $(a_2,a_1)$ belong to $\mathrm{Red}(d)\setminus H(d)$. Therefore, when investigating for the minimum of $L$ on $\mathrm{Red}(d)\setminus H(d)$, we can restrict to the subset where $a_2\leq a_1$.*

By Remark 4.12, it is enough to study $\tilde{L}$ on $\left\{0,\dots,\left\lfloor\frac{d-1}{a+b}\right\rfloor\right\}$. Let us make the form of $\tilde{L}$ explicit on $\left\{0,\dots,\left\lfloor\frac{d-1}{a+b}\right\rfloor\right\}$.

**Lemma 4.13.** *On the set $\left\{0,\dots,\left\lfloor\frac{d-1}{a+b}\right\rfloor\right\}$, the function $\tilde{L}$ defined in (4.8) is given as follows.*

*(1) If $d\leq a(q-1)$ (i.e. $\alpha_2<0$), then*

$$\tilde{L}(a_2) = \left(q-\left\lfloor\frac{d-1-ba_2}{a}\right\rfloor\right)(q-a_2).$$

*(2) If $d>a(q-1)$ (i.e. $\alpha_2\geq 0$), then*

$$\tilde{L}(a_2) = \begin{cases} q-a_2 & \text{if } a_2\leq\alpha_2,\\ \left(q-\left\lfloor\frac{d-1-ba_2}{a}\right\rfloor\right)(q-a_2) & \text{otherwise.}\end{cases}$$

*Proof.* The first description follows from Proposition 4.6 and Equation (4.8) by the virtue of the observation that $\left\lfloor\frac{d-1-ba_2}{a}\right\rfloor \leq \left\lfloor\frac{d}{a}\right\rfloor\leq q-1$. The second part follows similarly, by noticing that

$$\left\lfloor\frac{d-1-ba_2}{a}\right\rfloor\geq q-1 \iff a_2\leq \left\lfloor\frac{d-1-a(q-1)}{b}\right\rfloor=\alpha_2, \tag{4.9}$$

finishing the proof. □

**Lemma 4.14.** *If $\tilde{L}(a_2)=\left(q-\left\lfloor\frac{d-1-ba_2}{a}\right\rfloor\right)(q-a_2)$ as in Lemma 4.13, then it is strictly increasing on the set $\left\{\max\{0,\alpha_2\},\dots,\left\lfloor\frac{d-1}{a+b}\right\rfloor\right\}$.*

*Proof.* For all the values of $a_2$ satisfying

$$\max\left\{0,\left\lfloor\frac{d-1-a(q-1)}{b}\right\rfloor\right\}+1\leq a_2\leq\min\left\{\left\lfloor\frac{d-1}{a+b}\right\rfloor,q-1\right\},$$

the difference $\tilde{L}(a_2) - \tilde{L}(a_2-1)$ is

$$(q-a_2+1)\left(\left\lfloor \frac{d-1-b(a_2-1)}{a}\right\rfloor - \left\lfloor \frac{d-1-ba_2}{a}\right\rfloor\right) - q + \left\lfloor \frac{d-1-ba_2}{a}\right\rfloor.$$

If $a=1$, the expression above boils down to

$$\tilde{L}(a_2) - \tilde{L}(a_2-1) = d + (q+1)(b-1) - 2a_2 b$$

which is positive because $a_2 \leq \left\lfloor \frac{d-1}{b+1} \right\rfloor$ and $a_2 \leq q-1$.

If $a \neq 1$, note that for all $x, y \in \mathbb{Z}$, we have

$$\left\lfloor \frac{x}{a} \right\rfloor - \left\lfloor \frac{y}{a} \right\rfloor = \left\lfloor \frac{x}{a} \right\rfloor - \left\lceil \frac{y+1}{a} \right\rceil + 1 \geq \left\lfloor \frac{x-y-1}{a} \right\rfloor. \tag{4.10}$$

Applying this to $x = d-1-b(a_2-1)$ and $y = d-1-ba_2$, we get

$$\tilde{L}(a_2) - \tilde{L}(a_2-1) \geq (q-a_2+1)\left\lfloor \frac{b-1}{a} \right\rfloor - q + \left\lfloor \frac{d-1-ba_2}{a} \right\rfloor.$$

Since we have $a_2 \leq \left\lfloor \frac{d-1}{a+b} \right\rfloor$, which is tantamount to $\left\lfloor \frac{d-1-ba_2}{a} \right\rfloor \geq a_2$, we have

$$\tilde{L}(a_2) - \tilde{L}(a_2-1) \geq (q-a_2+1)\left(\left\lfloor \frac{b-1}{a} \right\rfloor - 1\right) + 1,$$

which is positive since $q > a_2$ and $b > a$. □

**Proposition 4.15.** *The minimum value of $\tilde{L}$ on $\{0, \ldots, \mu_b\}$ is*

$$\tilde{L}(\ell) = \begin{cases} q(q - \lfloor \frac{d-1}{a} \rfloor) & \textit{if } d \leq a(q-1), \\ q - \ell & \textit{if } a(q-1) < d. \end{cases}$$

*Proof.* The assumption $d \leq (a+b)(q-1)$ is equivalent to $\alpha_2 = \left\lfloor \frac{d-1-a(q-1)}{b} \right\rfloor \leq q-2$. Therefore, by Remark 2.9, $\ell = \max\{0, \alpha_2\}$.

(1) If $d \leq a(q-1)$ (i.e. $\alpha_2 < 0$), then the function $\tilde{L}$ is given by Lemma 4.13 (1) and it is strictly increasing on the whole set $\left\{0, \ldots, \min\left\{\left\lfloor \frac{d-1}{a+b} \right\rfloor, q-1\right\}\right\}$ by Lemma 4.14. Thus we clearly have that $\tilde{L}$ reaches its minimum at $\ell = 0$.

(2) If $a(q-1) < d$, then $\ell = \alpha_2 \geq 0$. The function $\tilde{L}$ is given by Lemma 4.13 (2). Therefore, it follows from Lemma 4.14 that we only need to compare $\tilde{L}(\ell) = q - \ell$ with

$$\tilde{L}(\ell+1) = (q-\ell-1)\left(q - \left\lfloor \frac{d-1-b(\ell+1)}{a} \right\rfloor\right).$$

By definition of the floor function (for more details about this function see [23]) and $\ell \leq \frac{d-1-a(q-1)}{b} < \ell+1$, one can easily check that

$$\left\lfloor \frac{d-1-b(\ell+1)}{a} \right\rfloor < q-1,$$

so $\tilde{L}(\ell+1) > q-\ell-1$. Then $\tilde{L}(\ell+1) - \tilde{L}(\ell) \geq (q-\ell) - (q-\ell) = 0$.

The proof is complete as the minimum value is always $\tilde{L}(\ell)$. □

4.3. **Minimum of $L$ over the whole set** $\mathrm{Red}(d)$**.** In this part, we give the lower bound provided by Lemma 4.4 by comparing the minimum value $\tilde{L}(\ell)$ of $\tilde{L}$ and the minimum of $L$ outside the domain $a_2 \leq \mu_b$.

4.3.1. *The case where $d < bq$.*

**Proposition 4.16.** *Assume that $(a,b) \neq (1,1)$. If $d < bq$, then*

$$\min_{\mathbf{a}\in \mathrm{Red}(d)} L(\mathbf{a}) = \begin{cases} q(q - \lfloor \frac{d-1}{a} \rfloor) & \text{if } d \le a(q-1), \\ q - \ell & \text{if } a(q-1) < d. \end{cases}$$

*Proof.* If $b \nmid d$, then for every $\mathbf{a} \in \mathrm{Red}(d)$, $a_2 \le \mu_b$ so the statement follows from Corollary 4.11 and Proposition 4.15.

If $b \mid d$, we have to compare the minimum provided by Proposition 4.15 and the value $L(0, \frac{d}{b})$. Since $d < bq$, we have $q - \frac{d}{b} \ge 1$ and Proposition 4.6 states that

$$L\left(0, \frac{d}{b}\right) = q\left(q - \frac{d}{b}\right) + \max\left\{q - \left\lfloor \frac{d-b}{ab} \right\rfloor, 1\right\}.$$

i. If $d \le a(q-1)$, then $\alpha_2 < 0$ and so $\ell = 0$. It follows that we have

$$\frac{d-b}{ab} \le \frac{d-b}{a} \le q-1 \text{ and so } q - \left\lfloor \frac{d-b}{ab} \right\rfloor \ge 1.$$

If $a \nmid d$ , then by Lemma 4.13 (1), we have

$$\tilde{L}(0) = q\left(q - \left\lfloor \frac{d-1}{a} \right\rfloor\right) = q\left(q - \left\lfloor \frac{d}{a} \right\rfloor\right) \le q\left(q - \frac{d}{b}\right) \le L\left(0, \frac{d}{b}\right).$$

If $a \mid d$ and $b > 1$, then $b \ge a+1$, $d = d_0 ab$ for some integer $d_0 \ge 1$ and $d/a - 1 = d_0 b - 1 \ge d_0 a = d/b$. Thus, by Lemma 4.13 (1), we have

$$\tilde{L}(0) = q\left(q - \left\lfloor \frac{d-1}{a} \right\rfloor\right) = q\left(q - \left\lfloor \frac{d}{a} \right\rfloor + 1\right) \le q\left(q - \frac{d}{b}\right) \le L\left(0, \frac{d}{b}\right).$$

Therefore, the minimum of $L$ is $\tilde{L}(0) = q(q - \mu_a)$ (unless $a = b = 1$).

ii. If $a(q-1) < d$, then $\ell = \alpha_2 \ge 0$. By Lemma 4.13 (2), we have

$$\tilde{L}(\ell) = q - \ell \le q < q + 1 \le L\left(0, \frac{d}{b}\right).$$

In all cases, the minimum is the one given by Proposition 4.15. □

**Remark 4.17.** *If $a = b = 1$, let us stress out that*

$$\tilde{L}(0) = q(q-d+1) \ge q(q-d) + q - (d-1) = L\left(0, \frac{d}{b}\right),$$

*whereas it is well–known that $d_{min}(C_d) = \tilde{L}(0) = q(q-d+1)$. In this case, the bound provided by Lemma 4.4 is not sharp. However, this issue can be overcome using the 3–transitivity of the projective plane $\mathbb{P}^2$ (see [5, Proposition 4.2]).*

4.3.2. *The case where $qb \le d \le (a+b)(q-1)$.* In this case, we have $a < b \le a(q-1)$, which induces $q \ge 3$.

Let us first deal with the case $a = 1$.

**Proposition 4.18.** *If $a = 1$ and $d \ge bq$, then*

$$\min_{\mathbf{a}\in \mathrm{Red}(d)} L(\mathbf{a}) = \begin{cases} 1 & \text{if } b \mid d, \\ q - \ell & \text{otherwise.} \end{cases}$$

*Proof.* If $a = 1$ and $d \geq bq$, then every $\mathbf{a} \in \mathrm{Red}(d)$ satisfies $a_2 \leq q-1$ except $(0, d/b)$ if $b \mid d$. If $b \nmid d$, the minimum of $L$ on $\mathrm{Red}(d)$ is $q - \ell$ as given by Proposition 4.15. If $b \mid d$, then $\left\lfloor \frac{d-b}{ab} \right\rfloor = \frac{d}{b} - 1 \geq q - 1$ and the minimum of $L$ on $\mathrm{Red}(d)$ is 1. □

Now let us assume that $a \geq 2$.

**Proposition 4.19.** *Assume that $a \geq 2$ and $d \geq bq$.*
*If $b \geq a+2$ or $b = a+1$ and $d \geq (a+1)q + \frac{q}{a-1} + 1$, then $\min_{\mathbf{a} \in \mathrm{Red}(d)} L(\mathbf{a}) = q - \ell$.*
*Assume $b = a+1$ and $(a+1)q \leq d < (a+1)q + \frac{q}{a-1} + 1$.*

- *If $d - (a+1)q \notin \langle a, a+1 \rangle$, then $\min_{\mathbf{a} \in \mathrm{Red}(d)} L(\mathbf{a}) = q - \ell$.*
- *If $d - (a+1)q \in \langle a, a+1 \rangle$, set $s = d - \left\lfloor \frac{d}{ab} \right\rfloor ab$. Then $\min_{\mathbf{a} \in \mathrm{Red}(d)} L(\mathbf{a})$ is*

$$\begin{cases} q - \max\left\{\ell, \left\lfloor \frac{d}{ab} \right\rfloor - 1\right\} & \text{if } s = 0 \ (i.e.\ a(a+1) \mid d), \\ q - \max\left\{\ell, \left\lfloor \frac{d}{ab} \right\rfloor\right\} & \text{if } s \notin \langle a, a+1 \rangle \text{ or either } a \mid d \text{ or } a+1 \mid d, \\ q - \max\left\{\ell, \left\lfloor \frac{d}{ab} \right\rfloor + 1\right\} & \text{if } s \in \langle a, b \rangle \text{ with } a \nmid d \text{ and } a+1 \nmid d. \end{cases}$$

*Proof.* If $d - bq \notin \langle a, b \rangle$, then for every $\mathbf{a} \in \mathrm{Red}(d)$, we have $a_2 \leq \mu_b = q - 1$ and the minimum of $L$ is $\tilde{L}(\ell) = q - \ell$ by Proposition 4.15.

Otherwise, there exists $\mathbf{a} = (a_1, a_2) \in H(d)$ such that $a_2 \geq q$ and the minimum of $L$ is given by the minimum of $\tilde{L}(\ell) = q - \ell$ and $\min\{L(\mathbf{a}) : \mathbf{a} \in H(d) \text{ such that } a_2 \geq q\}$.

For $\mathbf{a} = (a_1, a_2) = (x' - ib, y' + ia) \in H(d)$ such that $a_1 \geq 1$ and $a_2 \geq q$ (which is only possible if $d - a - bq \in \langle a, b \rangle$), we have

$$L(a_1, a_2) = q - 1 - \left\lfloor \frac{a_2 - 1}{a} \right\rfloor = q - 1 - i,$$

which is a decreasing function of $i$, whose minimum is $q - 1 - i_{max}$ (see Equation (2.11) for a formula for $i_{\max}$).

If $b \mid d$, then

$$L(0, d/b) = q - \left\lfloor \frac{d-b}{ab} \right\rfloor$$

and $(x' - i_{\max} b, y' + i_{\max} a) = (b, d/b - a)$. If $d/b - a < q$, then $(0, d/b)$ is the only point of $H(d)$ such that $a_2 \geq q$. Otherwise, one can easily check $L(b, d/b - a) = L(0, d/b)$, *i.e.* $\left\lfloor \frac{d-b}{ab} \right\rfloor = i_{\max} + 1$.

We are thus led to compare $\ell$ and $i_{\max} + 1$, when $d$ is large enough.

First, let us prove that for any $d \geq bq$, we have

$$i_{max} + 1 \in \left\lfloor \frac{d-b}{ab} \right\rfloor + \{0, 1\}. \tag{4.11}$$

Writing $d = \lambda ab + s$ with $0 \leq s < ab$, we have

$$\left\lfloor \frac{d-b}{ab} \right\rfloor = \lambda + \left\lfloor \frac{s-b}{ab} \right\rfloor = \begin{cases} \lambda - 1 & \text{if } s < b, \\ \lambda & \text{if } s \geq b, \end{cases} \tag{4.12}$$

and using Equation (2.11) gives

$$i_{max} + 1 = \lambda + \mathrm{den}(s, a, b) - \mathbf{1}_{a|d} - \mathbf{1}_{b|d}. \tag{4.13}$$

(i) If $s < b$, $\mathrm{den}(s, a, b) = 1$ if and only if $a$ divides $s$, *i.e.* $\mathrm{den}(s, a, b) = \mathbf{1}_{a|d}$. In this case, $i_{max} + 1 = \lambda - \mathbf{1}_{b|d} = \lambda - \mathbf{1}_{s=0}$.

(ii) If $s \geq b$, then $\mathrm{den}(s, a, b) - \mathbf{1}_{a|d} - \mathbf{1}_{b|d} \in \{0, 1\}$ because $\mathbf{1}_{a|d} = \mathbf{1}_{b|d} = 1$ if and only if $s = 0$.

Secondly, note that $\ell \geq \left\lfloor \frac{d-b}{ab} \right\rfloor + 1 \geq i_{\max} + 1$ when $d \geq \frac{a^2(q-1)+a}{a-1} + b$. It is enough to check that

$$d \geq \frac{a^2(q-1)+a}{a-1} + b \Leftrightarrow \frac{d-1-a(q-1)}{b} \geq \frac{d-b}{ab} + 1.$$

and to use the monotony of the floor function. In this case, $\min_{\mathbf{a} \in \mathrm{Red}(d)} L(\mathbf{a}) = q - \ell$.

On the contrary, if $bq \leq d < \frac{a^2(q-1)+a}{a-1} + b$, this forces

$$b(q-1) < \frac{a^2(q-1)+a}{a-1}. \tag{4.14}$$

Let us prove that (4.14) can only hold if $b = a+1$, except the case where $a = q = 3$ and $b = 5$.

If $a = 2$ and $q \geq 3$, the condition in (4.14) can be written

$$b(q-1) < 4(q-1) + 2 \leq 5(q-1),$$

which implies that $b = 3$, because $a$ and $b$ are coprime.

Assume that $a \geq 3$, then isolating $b$ in the inequality (4.14) gives

$$b < \frac{a^2}{a-1} + \frac{a}{(a-1)(q-1)} = a + 1 + \frac{q+a-1}{(a-1)(q-1)}.$$

- If $a \geq 4$ or $q \geq 4$, then $q + a - 1 \leq (q-1)(a-1)$. Then $b < a+2$, hence $b = a+1$.
- If $a = q = 3$, then a direct computation gives $a < b < \frac{21}{4}$, *i.e.* $b \in \{4, 5\}$.

If $a = q = 3$ and $b = 5$, the only case we have to consider is $d = 15$, for which $\ell = 1 > \left\lfloor \frac{d-b}{ab} \right\rfloor = 0$.

As a result, if $b \geq a+2$, then necessarily $\ell \geq \left\lfloor \frac{d-b}{ab} \right\rfloor + 1$, which means that the minimum of $L$ over $\mathrm{Red}(d)$ is equal to $q - \ell$. When $b = a+1$, we can rewrite

$$\frac{a^2(q-1)+a}{a-1} + b = (a+1)q + \frac{q}{a-1} + 1.$$

It remains to determine the value of $i_{\max} + 1$ in terms of $\lambda$. In case (i), we have $s \leq a$ so $s \in \langle a, a+1 \rangle$ if and only if $s = 0$, in which case $i_{\max} + 1 = \lambda - 1$, or $s = a$. If $1 \leq s \leq a$, $i_{\max} + 1 = \lambda$. In case (ii), we have $s \geq a+1$ and $\mathrm{den}(s, a, b) - \mathbf{1}_{a|d} - \mathbf{1}_{b|d} = 1$ if and only if $s \in \langle a, a+1 \rangle$ with $a \nmid s$ and $a+1 \nmid s$. Therefore, we have

$$i_{\max} + 1 = \begin{cases} \lambda - 1 & \text{if } s = 0 \text{ (i.e. } a(a+1) \mid s), \\ \lambda & \text{if } s \notin \langle a, a+1 \rangle \text{ or either } a \mid s \text{ or } a+1 \mid s, \\ \lambda + 1 & \text{if } s \in \langle a, a+1 \rangle \text{ with } a \nmid s \text{ and } a+1 \nmid s, \end{cases}$$

which completes the proof. □

## 5. Polynomials of designated weights

In order to assert that the lower bound for the minimum distance provided by Propositions 4.16, 4.18 and 4.19 are sharp, it is enough to display a polynomial of the corresponding weight.

**Proposition 5.1.** *Assume that $b > a$, with $a$ and $b$ coprime. For every degree $d$, there exists a polynomial of weight*

$$\tilde{L}(\ell) = \begin{cases} q(q - \lfloor \frac{d-1}{a} \rfloor) & \text{if } d \leq a(q-1), \\ q - \ell & \text{if } a(q-1) < d \leq (a+b)(q-1), \\ 1 & \text{if } d > (a+b)(q-1). \end{cases}$$

*Proof.* We provide a polynomial $f$ with $n_f = n - \tilde{L}(\ell)$ roots for each case.

(i) If $d \leq a(q-1)$, then $\alpha_2 < 0$ and $\ell = 0$. We consider the following polynomial,

$$f = x_0^{r+1} \prod_{y_1 \in J} (x_1 - y_1 x_0^a)$$

where $r$ is the remainder of the division of $d-1$ by $a$ and $J$ is any subset of $\mathbb{F}_q$ with $|J| = \lfloor \frac{d-1}{a} \rfloor$. So, $\deg(f) = r + 1 + a|J| = d$. The polynomial $f$ has $q+1$ roots with $x_0 = 0$ and $q|J|$ roots of the form $[1 : y_1 : y_2]$. In total, it has $q + 1 + q|J| = q + 1 + q \lfloor \frac{d-1}{a} \rfloor$ roots. Since,

$$n - n_f = q^2 + q + 1 - (q + 1 + q \left\lfloor \frac{d-1}{a} \right\rfloor) = q \left( q - \left\lfloor \frac{d-1}{a} \right\rfloor \right) = \tilde{L}(0),$$

the claim follows.

(ii) If $a(q-1) < d \leq a(q-1) + b$, then $\ell = \alpha_2 = 0$. The following polynomial

$$f = x_0^{d-(q-1)a} \prod_{y_1 \in \mathbb{F}_q^*} (x_1 - y_1 x_0^a)$$

has $(q+1)$ roots with $x_0 = 0$ and $(q-1)q$ roots of the form $[1 : y_1 : y_2]$. In total, it has $q^2 + 1$ roots. Hence, $n - n_f = q^2 + q + 1 - (q^2 + 1) = q = \tilde{L}(0)$.

(iii) If $a(q-1) + b < d \leq (a+b)(q-1)$, then $d - 1 - a(q-1) = \ell b + r$ with $\ell = \alpha_2 \geq 1$ and $0 \leq r < b$. Let $J'$ be any subset of $\mathbb{F}_q$ with $|J'| = \ell$. It is clear that the following polynomial

$$f = x_0^{r+1} \prod_{y_1 \in \mathbb{F}_q^*} (x_1 - y_1 x_0^a) \prod_{y_2 \in J'} (x_2 - y_2 x_0^b)$$

has degree $d = r + 1 + (q-1)a + \ell b$ and $n_f = q^2 + \ell + 1$, since $f$ has $q+1$ roots with $x_0 = 0$, $(q-1)(q-\ell)$ roots of the form $[1 : y_1 : y_2]$ where $y_2 \in \mathbb{F}_q \setminus J'$ and $q\ell$ roots of the form $[1 : y_1 : y_2]$ where $y_2 \in J'$. Thus,

$$n - n_f = q^2 + q + 1 - (q^2 + \ell + 1) = q - \ell = \tilde{L}(\ell).$$

(iv) If $(a+b)(q-1) < d$, then $\ell = q - 1$. The following polynomial

$$f = x_0^{d-(q-1)(a+b)} \prod_{y_1 \in \mathbb{F}_q^*} (x_1 - y_1 x_0^a) \prod_{y_2 \in \mathbb{F}_q^*} (x_2 - y_2 x_0^b) \in S_d$$

has $q+1$ roots with $x_0 = 0$, $(q-1)q$ roots of the form $[1 : y_1 : y_2]$ and $(q-1)$ roots of the form $[1 : 0 : y_2]$ comprising $q^2 + q$ roots in total. This means that the weight of the codeword $ev_Y(f)$ is $\tilde{L}(\ell) = 1$.

∎

It remains to deal with polynomials with leading term $\mathbf{x^a}$ of weight $L(a_1, a_2)$ for $a_2 \geq q$.

**Proposition 5.2.** *Let $a = 1$ and $d = d_0 b$ with $d_0 \geq q$, then the polynomial*

$$f = x_2^{1+d_0-q}\left(x_2^{q-1} - x_0^{b(q-1)} - x_1^{(q-1)(b-1)}\left(x_1^{q-1} - x_0^{q-1}\right)\right) \in S_d$$

*satisfies $w(ev_Y(f)) = 1$.*

*Proof.* The polynomial $f$ vanishes everywhere except at $[0:0:1]$. So, $n_f = q^2 + q$ and $w(ev_Y(f)) = 1$. □

The following example shows that polynomials of weight $L(a_1, a_2)$ for $a_2 \geq q$ may not always exist when $a \geq 2$.

**Example 5.3.** *For $q = 8$, $(a, b) = (2, 3)$ and $d = 29$, there is exactly one point $\mathbf{a} = (1, 9)$ in $\mathrm{Red}(d)$ with $a_2 > \mu_b = q - 1$. The lower bound on the minimum distance provided by Proposition 4.19 is $L(1, 9) = 3$. Using* Magma, *we checked that the actual minimum distance is $q - \ell = 4$. This means that no polynomial with leading term $x_1 x_2^9$ has $q^2 + q - 2$ zeroes.*

Therefore, as in the case $a = b = 1$ (see Remark 4.17), the footprint bound may not provide the actual minimum distance. For the purpose of finding the minimum distance, it is enough to deal with the cases where $\min_{\mathbf{a} \in \mathrm{Red}(d)} L(\mathbf{a}) \neq q - \ell$.

Polynomials of the form $f = g_1\left(x_2^q - x_0^{b(q-1)} x_2\right) + g_2\left(x_1^q - x_0^{a(q-1)} x_1\right)$, as provided by Proposition 6.3, clearly vanish on the domain $x_0 \neq 0$. In order to check if the lower bound of Proposition 4.19 is reached, we need to count the number of zeroes of polynomials of this form on the line $x_0 = 0$.

**Remark 5.4.** *The $\mathbb{F}_q$-rational points on the line $x_0 = 0$ consist of the following: the two special points $[0:1:0]$ and $[0:0:1]$ and the points of the form $[0:y_1:y_2]$ for which the ratio $y_2^a/y_1^b$ belongs to $\mathbb{F}_q^*$. Among these, there are exactly $q-1$ such points of the second type, since each nonzero element of $\mathbb{F}_q^*$ uniquely determines a value of the ratio $y_2^a/y_1^b$, and hence a corresponding point $[0:y_1:y_2]$ up to scalar equivalence. We now analyze when we can simplify the representatives by assuming $y_1 = 1$ and $y_2 \in \mathbb{F}_q^*$. This is always possible if $\gcd(a, q-1) = 1$, because in this case the map $y_2 \mapsto y_2^a$ is a bijection on $\mathbb{F}_q^*$. Therefore, for every value of $y_2^a/y_1^b \in \mathbb{F}_q^*$, we can find a unique $y_2 \in \mathbb{F}_q^*$ such that $[0:1:y_2]$ represents the point. However, if $\gcd(a, q-1) \neq 1$, then this simplification is only possible for certain points. Specifically, let $\eta$ be a generator of the multiplicative group $\mathbb{F}_q^*$. Then the equation $y_2^a = \eta^j$ has a solution $y_2 = \eta^{j_2} \in \mathbb{F}_q^*$ if and only if the congruence*

$$a j_2 \equiv j \pmod{q-1}$$

*has a solution. This happens if and only if $\gcd(a, q-1)$ divides $j$. Consequently, the number of such solvable $j$ values (and hence the number of such points in the form $[0:1:\eta^i]$) is exactly*

$$\frac{q-1}{\gcd(a, q-1)}.$$

*So, the points for which a representative of the form $[0:1:\eta^i]$ exists are precisely those with $i = 1, \ldots, (q-1)/\gcd(a, q-1)$.*

**Proposition 5.5.** *Assume that $a \mid q-1$ and $b = a+1$. Let $\mathbf{a} = (a_1, a_2) \in H(d)$ with $a_2 \geq q$. Write $a_2 = q + k_2 a + r_2$ with $0 \leq r_2 \leq a-1$. Write $\mathbb{F}_q^* = \langle \eta \rangle$ and take $J \subset \{1, \ldots, q-1\} \setminus \{ia : i \in \{1, \ldots, (q-1)/a\}\}$ of cardinality $k_2$.*

$$f=\left(\prod_{j\in J}(x_2^a-\eta^j x_1^b)\right)x_1^{a_1}x_2^{1+r_2}\left(x_2^{q-1}-x_0^{b(q-1)}-x_1^{(q-1)/a}\left(x_1^{q-1}-x_0^{a(q-1)}\right)\right)$$

*has weight* $L(a_1,a_2)$.

*Proof.* Since $a_2\geq q$, Proposition 4.6 says $f$ has at most $n-L(a_1,a_2)$ roots, where

$$L(a_1,a_2)=q-\mathbb{1}_{a_1>0}-\left\lfloor\frac{q+k_2a+r_2-1}{a}\right\rfloor=q-\mathbb{1}_{a_1>0}-k_2-\frac{q-1}{a}.$$

Notice that if $d\notin\operatorname{reg}(Y)$, then

$$k_2+\frac{q-1}{a}=\left\lfloor\frac{d-bq-aa_1+b(q-1)}{ab}\right\rfloor=\left\lfloor\frac{d-b-aa_1}{ab}\right\rfloor\leq\left\lfloor\frac{d}{ab}\right\rfloor\leq q-1.$$

Clearly, the associated polynomial $f$ vanishes at $[1:y_1:y_2]$ for every $y_1,y_2\in\mathbb{F}_q$. On the line $x_0=0$, we have

$$f(0,x_1,x_2)=\left(\prod_{j\in J}(x_2^a-\eta^j x_1^b)\right)x_1^{a_1}x_2^{1+r_2}\left(x_2^{q-1}-x_1^{(q-1)/a}x_1^{q-1}\right).$$

Obviously, $f$ vanishes at $[0:1:0]$. It vanishes at $[0:0:1]$ if and only if $a_1>0$. The first factor of $f$ vanishes at the $k_2$ points $[0:y_1:y_2]$ such that $y_2^a/y_1^b=\eta^j$ for $j\in J$. The last factor of $f$ vanishes at the $(q-1)/a$ points $[0:1:\eta^i]$ for $i\in\{1,\dots,(q-1)/a\}$. Since $[0:1:\eta^i]=[0:1:\eta^{i'}]\iff q-1$ divides $a(i'-i)$, these points are all distinct. As a result, we have $w(\mathrm{ev}(f))=L(a_1,a_2)$. ☐

## 6. Conclusion and open questions

**Theorem 6.1.** *Assume that $b\geq a$ are coprime.*

*If $a=1$, then*

$$d_{min}(C_d)=\begin{cases}q(q-d+1) & \text{if } d\leq q-1,\\ q-\left\lfloor\frac{d-q}{b}\right\rfloor & \text{if } q\leq d<bq,\\ 1 & \text{if } d\geq bq.\end{cases}$$

*Assume $a\geq 2$. Set $\ell=\left\lfloor\frac{d-1-a(q-1)}{b}\right\rfloor$.*

*If $b\geq a+2$, then*

$$d_{min}(C_d)=\begin{cases}q(q-\lfloor\frac{d-1}{a}\rfloor) & \text{if } d\leq a(q-1),\\ q-\ell & \text{if } a(q-1)<d\leq(a+b)(q-1),\\ 1 & \text{if } d>(a+b)(q-1).\end{cases}$$

*If $b=a+1$, then*

$$d_{min}(C_d)=\begin{cases}q(q-\lfloor\frac{d-1}{a}\rfloor) & \text{if } d\leq a(q-1),\\ q-\ell & \text{if } a(q-1)<d<bq \text{ or } d\geq bq+\frac{q}{a-1}+1,\\ 1 & \text{if } d>(a+b)(q-1).\end{cases}$$

*If $b=a+1$ and $bq\leq d<bq+\frac{q}{a-1}+1$, several cases have to be distinguished, according to whether $d-(a+1)q$ lies in the semigroup $\langle a,a+1\rangle_{\mathbb{N}}$ generated by $a$ and $b=a+1$.*

- *If* $d-(a+1)q \notin \langle a, a+1\rangle_{\mathbb{N}}$, *then* $d_{min}(C_d) = q-\ell$.
- *If* $d-(a+1)q \in \langle a, a+1\rangle_{\mathbb{N}}$, *set* $s = d - \left\lfloor \frac{d}{ab} \right\rfloor ab$. *Then* $d_{min}(C_d)$ *is* bounded from below *by*

$$\begin{cases} q-\max\left\{\ell, \left\lfloor \frac{d}{ab}\right\rfloor - 1\right\} & \text{if } s = 0 \; (i.e.\ a(a+1) \mid d), \\ q-\max\left\{\ell, \left\lfloor \frac{d}{ab}\right\rfloor\right\} & \text{if } s \notin \langle a, a+1\rangle \text{ or } a \mid s \text{ or } a+1 \mid s, \\ q-\max\left\{\ell, \left\lfloor \frac{d}{ab}\right\rfloor + 1\right\} & \text{if } s \in \langle a, b\rangle \text{ with } a \nmid s \text{ and } a+1 \nmid s. \end{cases}$$

*The equality holds when the value is* $q-\ell$ *or when* $a \mid q-1$.

*Proof.* The minimum distance and the minimum weight codewords when $a=b=1$ are provided by [13, Corollary 3.3 & Theorem 4.3]. Let us assume that $b>a$.

For degrees $d < bq$, the inequality $d_{min}(C_d) \geq \tilde{L}(\ell)$ follows from Proposition 4.16. Proposition 5.1 yields the reverse inequality.

For degrees $d \geq bq$, the lower bound for the minimum distance is given by Proposition 4.19. When the bound is $q-\ell$, the equality follows from Proposition 5.1. Proposition 5.5 guarantees the equality when $a \mid q-1$. □

**Remark 6.2.** *Proposition 6.3 forces polynomials* $f$ *with weight* $w(ev(f)) \neq q-\ell$ *that reach the minimum distance to vanish on the affine plane* $x_0 \neq 0$. *The lower bound displayed in Theorem 6.1 could also be obtained by factorizing* $f(0,x_1,x_2)$*:*

$$f(0,x_1,x_2) = h(x_1,x_2) \cdot \prod_{i=1}^{j} (x_2^a - \alpha_i x_1^b)$$

*for some* $j \leq \left\lfloor \frac{d}{ab} \right\rfloor$, $\alpha_1, \ldots, \alpha_j \in \mathbb{F}_q$ *and where* $h$ *is not divible by any factor of the form* $(x_2^a - \alpha x_1^b)$. *In this case,* $f$ *has either* $j$, $j+1$ *or* $j+2$ *roots, depending on whether* $x_1$ *or* $x_2$ *divide* $h$. *Indeed, if* $a \nmid d$ *(respectively* $b \nmid d$*), then* $x_2$ *(respectively* $x_1$*) divides* $h$ *(hence* $f(0,x_1,x_2)$*), which implies that* $f$ *vanishes at* $[0:1:0]$ *(resp.*$[0:0:1]$*).*

*Finally, one can easily check that if* $s \notin \langle a, b\rangle$, *then* $j \leq \left\lfloor \frac{d}{ab} \right\rfloor - 1$ *and* $f$ *is divisible by* $x_1$ *and* $x_2$, *which yields at most* $\left\lfloor \frac{d}{ab} \right\rfloor + 1$ *roots.*

6.1. **Refining the lower bound when** $b = a+1$ **and** $bq \leq d < bq + \frac{q}{a-1} + 1$**.** In this paragraph, we focus on the case where Theorem 6.1 only gives a lower bound on the minimum distance, because we are not able to guarantee the existence of polynomials of a specified weight. Note that if $w(\mathrm{ev}(f)) = L(a_1,a_2)$ then, by Lemma 4.2, the union set $\mathcal{G} \cup \{f\} = \{f_0, f_1, f_2, f\}$ is a Gröbner basis of $I(Y,f)$ (see Theorem 2.1 for the definition of $\mathcal{G}$). In particular, this means that $\overline{S(f,f_1)}^{\mathcal{G}\cup\{f\}} = 0$. The next proposition characterizes (modulo $I(Y)$) polynomials with such a property.

**Proposition 6.3.** *Assume that* $b > a \geq 2$, *with* $a$ *and* $b$ *coprime. Let* $d \geq bq$ *and* $f \in S_d \setminus I(Y)$ *such that* $LM(f) = x_1^{a_1}x_2^{a_2}$ *with* $a_2 \geq q$. *If* $\overline{S(f,f_1)}^{\mathcal{G}\cup\{f\}} = 0$, *which is the case when* $w(ev(f)) = L(a_1,a_2)$, *there exists* $g_1 \in S_{d-bq}$ *with* $LM(g_1) = x_1^{a_1}x_2^{a_2-q}$ *and* $g_2 \in S_{d-aq}$ *such that*

$$f = g_1\left(x_2^q - x_0^{b(q-1)}x_2\right) + g_2\left(x_1^q - x_0^{a(q-1)}x_1\right) \text{ modulo } I(Y).$$

*Proof.* Assume that the leading coefficient of $f$ is 1 and write $f = x_1^{a_1}x_2^{a_2} + g$ with $a_2 \geq q$ and $\mathrm{LM}(g) < x_1^{a_1}x_2^{a_2}$. On one hand, we have

$$S(f,f_1) = x_0 f - x_1^{a_1}x_2^{a_2-q}f_1 = x_0 g + x_0^{(q-1)b+1}x_1^{a_1}x_2^{a_2-q+1}. \tag{6.1}$$

On the other hand, as $\mathcal{G}\cup\{f\}$ is a Gröbner basis of $I(Y,f)$, the division algorithm enables us to write

$$S(f,f_1) = g_0 f_0 + g_1 f_1 + g_2 f_2 + g_3 f$$

with some homogeneous polynomials $g_0$, $g_1$, $g_2$ and $g_3$, such that that the leading monomials of each term $g_i f_i$ and $g_3 f$ are smaller than or equal to $\mathrm{LM}(S(f,f_1))$. As $\deg S(f,f_1) = \deg f + 1$, we have either $\deg g_3 = 1$ or $g_3 = 0$. The $S$-polynomial satisfies $\mathrm{LM}(S(f,f_1)) < \mathrm{lcm}(\mathrm{LM}(f),\mathrm{LM}(f_1)) = x_0 x_1^{a_1} x_2^{a_2}$, so having $\mathrm{LM}(g_3 f) \leq \mathrm{LM}(S(f,f_1))$ forces $g_3 = 0$ as $S_1 = \mathrm{Span}\{x_0\}$.

Noticing that $f_0$ does not depend on $x_0$, we get

$$g = -x_0^{(q-1)b} x_1^{a_1} x_2^{a_2-q+1} + (g_0/x_0) f_0 + g_1 (f_1/x_0) + g_2 (f_2/x_0).$$

Modulo $\mathcal{G}$, we can assume without loss of generality that $g_0 = 0$. Then

$$\begin{aligned} f &= x_1^{a_1} x_2^{a_2} - x_0^{(q-1)b} x_1^{a_1} x_2^{a_2-q+1} + g_1(f_1/x_0) + g_2(f_2/x_0) \\ &= (x_1^{a_1} x_2^{a_2-q} + g_1) f_1/x_0 + g_2 f_2/x_0, \end{aligned}$$

completing the proof. □

**Remark 6.4.** *Modulo $I(Y)$, we can assume that the polynomials $g_1$ and $g_2$ do not involve the variable $x_0$. However, the resulting polynomial $f$ may not be reduced. For instance take a reduced polynomial $f = x_1\left(x_1^{2(q-1)} - x_0^{2a(q-1)}\right) \in \mathrm{Span}(\overline{\mathbb{M}}_d)$. We can write $f = \tilde{g}_2(x_1^q - x_0^{a(q-1)} x_1)$ with $\tilde{g}_2 = x_1^{q-1} + x_0^{a(q-1)}$. Modulo $f_2$, we have $f \equiv x_1^{2q-1} - x_0^{a(q-1)} x_1^q = g_2(x_1^q - x_0^{a(q-1)} x_1)$ with $g_2 = x_1^{q-1}$.*

**Proposition 6.5.** *Let $f \in S_d \setminus I_d(Y)$ such that $LM(f) = \mathbf{x}^{\mathbf{a},d}$ with $\mathbf{a} \in \mathrm{Red}(d)$ and $a_2 \geq q$. Assume that $\overline{S(f,f_1)}^{\mathcal{G}\cup\{f\}} \neq 0$ where $f_1 = x_0 x_2^q - x_0^{(q-1)b+1} x_2$ is as in Theorem 2.1. Then $w(ev_Y(f)) \geq q - \ell$.*

*Proof.* For $\tilde{d} \geq d$ we define

$$\overline{\Delta}'_{\tilde{d}}(f) = \left\{ M \in \overline{\mathbb{M}}_{\tilde{d}} : \mathrm{LM}(f) \nmid M \text{ and } \mathrm{LM}(\overline{S(f,f_1)}^{\mathcal{G}\cup\{f\}}) \nmid M \right\}.$$

A similar argument as in Lemma 4.2 leads to

$$\tilde{n}_f(\tilde{d}) = H_{I(Y,f)}(\tilde{d}) \leq \left| \overline{\Delta}'_{\tilde{d}}(f) \right|. \tag{6.2}$$

We can express $\overline{\Delta}'_{\tilde{d}}(f)$ in terms of projective shadows as follows:

$$\overline{\Delta}'_{\tilde{d}}(f) = \overline{\mathbb{M}}_{\tilde{d}} \setminus \left( \overline{\nabla}_{\tilde{d}}(\mathrm{LM}(f)) \cup \overline{\nabla}_{\tilde{d}}(\mathrm{LM}(\overline{S(f,f_1)}^{\mathcal{G}\cup\{f\}})\right).$$

Note that no monomial $\mathbf{x}^{\tilde{\mathbf{a}},\tilde{d}} \in \overline{\mathbb{M}}_{\tilde{d}}$ is divisible by both $\mathrm{LM}(f) = x_1^{a_1} x_2^{a_2}$ and $\mathrm{LM}(\overline{S(f,f_1)}^{\mathcal{G}\cup\{f\}}$, *i.e.*

$$\overline{\nabla}_{\tilde{d}}(\mathrm{LM}(f)) \cap \overline{\nabla}_{\tilde{d}}(\mathrm{LM}(\overline{S(f,f_1)}^{\mathcal{G}\cup\{f\}}) = \varnothing.$$

Indeed, as $a_2 \geq q$ and $x_0 \mid \mathrm{LM}(\overline{S(f,f_1)}^{\mathcal{G}\cup\{f\}}$ (see Equation (6.1)), such a monomial would be divisible by $x_0 x_2^q = \mathrm{LM}(f_1)$, which is impossible by definition of $\overline{\mathbb{M}}_{\tilde{d}}$. This means that

$$\left| \overline{\Delta}'_{\tilde{d}}(f) \right| = n - \left| \overline{\nabla}_{\tilde{d}}(\mathrm{LM}(f)) \right| - \left| \overline{\nabla}_{\tilde{d}}(\mathrm{LM}(\overline{S(f,f_1)}^{\mathcal{G}\cup\{f\}}) \right|.$$

Write $\mathrm{LM}(\overline{S(f,f_1)}^{\mathcal{G}\cup\{f\}}) = \mathbf{x}^{\mathbf{a}',d+1}$. Provided that $\tilde{d}$ is large enough, Equation (6.2) can be rewritten

$$\begin{aligned} w(\mathrm{ev}_Y(f)) \geq n - \left|\overline{\Delta}'_{\tilde{d}}(f)\right| &= \left|\overline{\nabla}_{\tilde{d}}(\mathrm{LM}(f))\right| + \left|\overline{\nabla}_{\tilde{d}}\left(\mathrm{LM}(\overline{S(f,f_1)}^{\mathcal{G}\cup\{f\}})\right)\right| \\ &= L(\mathbf{a}) + L(\mathbf{a}'). \end{aligned}$$

On one hand, we have $L(\mathbf{a}) \geq 1$ (see Remark 4.5). On the other hand, note that $\mathbf{a}' \in \mathrm{Red}(d+1) \setminus H(d+1) \subseteq \mathrm{Red}(d+1) \cap \{a_2 \leq \mu_b\}$ and we can apply Proposition 4.15 on degree $d+1$ to bound $L(\mathbf{a}')$ from below. Gathering up, we get

$$w(\mathrm{ev}_Y(f)) \geq 1 + L(\mathbf{a}') \geq 1 + q - \left\lfloor \frac{d - a(q-1)}{b} \right\rfloor \geq q - \ell,$$

which proves the statement. $\square$

If one wants to compute exactly the minimum distance in cases for which Theorem 6.1 only supplies for a lower bound, previous results indicate that the study can be restricted to a smaller code.

**Corollary 6.6.** *Let $d \geq bq$. Denote by $Z \subset \mathbb{P}(1,a,b)$ the set formed by the $q+1$ $\mathbb{F}_q$-points on the line $\{x_0 = 0\}$. Let us consider the code*

$$\begin{aligned} \tilde{C}_{d,Z} = &\mathrm{Span}\left(\left\{ ev_Z(\mathbf{x}^{\mathbf{a},d-bq}x_2^q) : \mathbf{a} \in H(d-bq)\right\}\right) \\ &+ \mathrm{Span}\left(\left\{ ev_Z(\mathbf{x}^{\mathbf{a},d-aq}x_1^q) : \mathbf{a} \in H(d-aq)\right\}\right) \end{aligned}$$

*The code $\tilde{C}_{d,Z}$ has length $q+1$ and its dimension satisfies*

$$\dim(\tilde{C}_{d,Z}) \leq \mathrm{den}(d-aq,a,b) \cdot \mathrm{den}(d-bq,a,b).$$

*Moreover, we have $d_{min}(C_d) = \min(q-\ell, d_{min}(\tilde{C}_{d,Z}))$.*

*Proof.* The dimension of $\tilde{C}_{d,Z}$ follows from Equation (2.12). We separate $C_{Y,d}$ in three sets: $C_{Y,d} = \mathrm{ev}_{Y,d}(S_d^{(1)} \cup S_d^{(2)} \cup S_d^{(3)})$ where

$$\begin{aligned} S_d^{(1)} &= \left\{f \in S_d \text{ such that } \mathrm{LM}(f) = \mathbf{x}^{\mathbf{a},d} \text{ with } a_2 < q\right\}, \\ S_d^{(2)} &= \left\{f \in S_d \text{ such that } \mathrm{LM}(f) = \mathbf{x}^{\mathbf{a},d} \text{ with } a_2 \geq q \text{ and } \overline{S(f,f_1)}^{\mathcal{G}\cup\{f\}} \neq 0\right\}, \\ S_d^{(3)} &= \left\{f \in S_d \text{ such that } \mathrm{LM}(f) = \mathbf{x}^{\mathbf{a},d} \text{ with } a_2 \geq q \text{ and } \overline{S(f,f_1)}^{\mathcal{G}\cup\{f\}} = 0\right\}. \end{aligned}$$

Then $d_{min}(C_{Y,d}) = \min\left\{\min\left\{w(\mathrm{ev}_Y(f)) : f \in S_d^{(i)}\right\} : i \in \{1,2,3\}\right\}$.

As in Theorem 6.1, $\min\left\{w(\mathrm{ev}_Y(f)) : f \in S_d^{(1)}\right\} = q - \ell$. Proposition 6.5 ensures that $w(\mathrm{ev}_Y(f)) \geq q - \ell$ for $f \in S_d^{(2)}$. If $f \in S_d^{(3)}$, we can assume that $f = g_1\left(x_2^q - x_0^{b(q-1)}x_2\right) + g_2\left(x_1^q - x_0^{a(q-1)}x_1\right)$ modulo $I(Y)$ by Proposition 6.3. In this case $f$ is zero on $Y \setminus Z$ so $w(\mathrm{ev}_Y(f)) = w(\mathrm{ev}_Z(g_1x_2^q + g_2x_1^q))$. We deduce from Remark 6.4 that $\mathrm{ev}_Y\left(S_d^{(3)}\right) = \tilde{C}_{d,Z}$, which concludes the proof. $\square$

**Example 6.7.** *Let $q = 16$, $X = \mathbb{P}(1,2,3)$, $Y = X(\mathbb{F}_q)$ and $d = 48 = bq$. We have $\ell = 5$, hence $q - \ell = 16 - 5 = 11$. Since $d - (a+1)q \in \langle a,b \rangle$ and $ab \mid d$, then $s = 0$. Theorem 6.1 gives $d_{min}(C_d) \geq q - \max\{\ell, \left\lfloor \frac{d}{ab} \right\rfloor - 1\} = \min\{11, 9\} = 9$. But we checked using Magma [6] that the actual minimum distance is $11$. This also follows from Corollary 6.6 as the minimum distance of the smaller code $\tilde{C}_{d,Z}$ is $13 > 11$.*

## Acknowledgements

The second author expresses her deep gratitude to Rodrigo San José Rubio for some discussions that revealed some mistakes in the early version of the present work. The authors thank the anonymous referees for their valuable questions and suggestions.


## References


[1] Yves Aubry and Marc Perret. Maximum number of rational points on hypersurfaces in weighted projective spaces over finite fields. *Journal of Algebra and Its Applications*, page 2541015, 2025. doi: 10.1142/S0219498825410154. URL `https://doi.org/10.1142/S0219498825410154`.

[2] Yves Aubry, Wouter Castryck, Sudhir R. Ghorpade, Gilles Lachaud, Michael E. O'Sullivan, and Samrith Ram. Hypersurfaces in weighted projective spaces over finite fields with applications to coding theory. In *Algebraic geometry for coding theory and cryptography*, volume 9 of *Assoc. Women Math. Ser.*, pages 25–61. Springer, Cham, 2017. doi: 10.1007/978-3-319-63931-4_2. URL `https://doi.org/10.1007/978-3-319-63931-4_2`.

[3] Fadime Baldemir and Mesut Şahin. Calculating the minimum distance of a toric code via algebraic algorithms. *Math. Comput. Sci.*, 17(3-4):Paper No. 20, 12, 2023. ISSN 1661-8270,1661-8289. doi: 10.1007/s11786-023-00566-7. URL `https://doi.org/10.1007/s11786-023-00566-7`.

[4] V. V. Bavula. Identification of the Hilbert function and Poincaré series, and the dimension of modules over filtered rings. *Izv. Ross. Akad. Nauk Ser. Mat.*, 58(2):19–39, 1994.

[5] Peter Beelen, Mrinmoy Datta, and Sudhir R. Ghorpade. Vanishing ideals of projective spaces over finite fields and a projective footprint bound. *Acta Math. Sin. (Engl. Ser.)*, 35(1):47–63, 2019. ISSN 1439-8516,1439-7617. doi: 10.1007/s10114-018-8024-7. URL `https://doi.org/10.1007/s10114-018-8024-7`.

[6] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. ISSN 0747-7171. doi: 10.1006/jsco.1996.0125. URL `http://dx.doi.org/10.1006/jsco.1996.0125`. Computational algebra and number theory (London, 1993).

[7] Winfried Bruns and Jürgen Herzog. *Cohen-Macaulay rings*, volume 39 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1993. ISBN 0-521-41068-1.

[8] Massimo Caboara and Carla Mascia. On the Hilbert quasi-polynomials for non-standard graded rings. *ACM Communications in Computer Algebra*, 49: 101–104, 11 2015. doi: 10.1145/2850449.2850461.

[9] Yağmur Çakıroğlu and Mesut Şahin. Algebraic invariants of codes on weighted projective planes. *Journal of Algebra and Its Applications*, 2024. doi: 10.1142/S0219498825503487. URL `https://doi.org/10.1142/S0219498825503487`.

[10] Hara Charalambous, Apostolos Thoma, and Marius Vladoiu. Binomial fibers and indispensable binomials. *Journal of Symbolic Computation*, 74: 578–591, 2016. ISSN 0747-7171. doi: https://doi.org/10.1016/j.jsc.2015.09.005. URL `https://www.sciencedirect.com/science/article/pii/S0747717115000966`.

[11] Igor Dolgachev. Weighted projective varieties. In *Group Actions and Vector Fields: Proceedings of a Polish-North American Seminar Held at the University of British Columbia January 15–February 15, 1981*, pages 34–71. Springer, 1981.

[12] Olav Geil and Tom Høholdt. Footprints or generalized Bezout's theorem. *IEEE Trans. Inform. Theory*, 46(2):635–641, 2000. ISSN 0018-9448,1557-9654. doi: 10.1109/18.825832. URL `https://doi.org/10.1109/18.825832`.

[13] Sudhir R. Ghorpade and Rati Ludhani. On the minimum distance, minimum weight codewords, and the dimension of projective Reed-Muller codes. *Advances in Mathematics of Communications*, 2023. ISSN 1930-5338. doi: 10.3934/amc.2023035. URL `http://dx.doi.org/10.3934/amc.2023035`.

[14] José Martínez-Bernal, Yuriko Pitones, and Rafael H. Villarreal. Minimum distance functions of graded ideals and Reed-Muller-type codes. *J. Pure Appl. Algebra*, 221(2):251–275, 2017. ISSN 0022-4049,1873-1376. doi: 10.1016/j.jpaa.2016.06.006. URL `https://doi.org/10.1016/j.jpaa.2016.06.006`.

[15] Jade Nardi. Algebraic geometric codes on minimal Hirzebruch surfaces. *J. Algebra*, 535:556–597, 2019. ISSN 0021-8693. doi: 10.1016/j.jalgebra.2019.06.022. URL `https://doi.org/10.1016/j.jalgebra.2019.06.022`.

[16] Jade Nardi. Projective toric codes. *Int. J. Number Theory*, 18(1):179–204, 2022. ISSN 1793-0421. doi: 10.1142/S1793042122500142. URL `https://doi.org/10.1142/S1793042122500142`.

[17] Marc Perret. On the number of points of some varieties over finite fields. *Bulletin of the London Mathematical Society*, 35(3):309–320, 2003. doi: https://doi.org/10.1112/S0024609302001820. URL `https://londmathsoc.onlinelibrary.wiley.com/doi/abs/10.1112/S0024609302001820`.

[18] J. L. Ramírez Alfonsín. *The Diophantine Frobenius problem*, volume 30 of *Oxford Lecture Series in Mathematics and its Applications*. Oxford University Press, Oxford, 2005. doi: 10.1093/acprof:oso/9780198568209.001.0001. URL `https://doi.org/10.1093/acprof:oso/9780198568209.001.0001`.

[19] Mesut Şahin. Computing vanishing ideals for toric codes, 2022. URL `https://arxiv.org/abs/2207.01061`.

[20] S. Sertöz and A. Özlük. On the number of representations of an integer by a linear form. *İstanbul Üniv. Fen Fak. Mat. Derg.*, 50, 1991.

[21] Anders Bjært Sørensen. Weighted Reed-Muller codes and algebraic-geometric codes. *IEEE Trans. Inform. Theory*, 38(6):1821–1826, 1992. ISSN 0018-9448. doi: 10.1109/18.165459. URL `https://doi.org/10.1109/18.165459`.

[22] Bernd Sturmfels. *Grobner bases and convex polytopes*, volume 8. American Mathematical Soc., 1996.

[23] Xingbo Wang. Brief summary of frequently-used properties of the floor function. *IOSR Journal of Mathematics*, 13:46–48, 09 2017. doi: 10.9790/5728-1305024648.

Department of Mathematics, Hacettepe University, Ankara, TURKEY

Irmar, Ufr Mathématiques, Université de Rennes 1, Rennes, FRANCE

*Email address*: `yagmur.cakiroglu@hacettepe.edu.tr`
*Email address*: `jade.nardi@univ-rennes.fr`
*Email address*: `mesut.sahin@hacettepe.edu.tr`