# Hypersurfaces in weighted projective spaces over finite fields with applications to coding theory

Yves Aubry, Wouter Castryck, Sudhir Ghorpade, Gilles Lachaud, Michael O 'Sullivan, Samrith Ram

# Chapter 1
# Hypersurfaces in weighted projective spaces over finite fields with applications to coding theory

Yves Aubry, Wouter Castryck, Sudhir R. Ghorpade, Gilles Lachaud,
Michael E. O'Sullivan, and Samrith Ram

**Abstract** We consider the question of determining the maximum number of $\mathbb{F}_q$-rational points that can lie on a hypersurface of a given degree in a weighted projective space over the finite field $\mathbb{F}_q$, or in other words, the maximum number of zeros that a weighted homogeneous polynomial of a given degree can have in the corresponding weighted projective space over $\mathbb{F}_q$. In the case of classical projective spaces, this question has been answered by J.-P. Serre. In the case of weighted projective spaces, we give some conjectures and partial results. Applications to coding theory are included and an appendix providing a brief compendium of results about weighted projective spaces is also included.

Yves Aubry
Institut de Mathématiques de Toulon (IMATH), Université de Toulon, France and Aix Marseille Univ., CNRS, Centrale Marseille, I2M, Marseille, France. e-mail: yves.aubry@univ-tln.fr

Wouter Castryck
Laboratoire Painlevé, Université de Lille-1, Cité Scientifique, 59 655, Villeneuve d'Ascq, cedex, France and Departement Elektrotechniek imec-Cosic, KU Leuven, Kasteelpark Arenberg 10, 3001 Leuven, Belgium. e-mail: wouter.castryck@kuleuven.be

Sudhir R. Ghorpade
Department of Mathematics, Indian Institute of Technology Bombay, Powai, Mumbai 400076, India. e-mail: srg@math.iitb.ac.in

Gilles Lachaud
Aix Marseille Univ., CNRS, Centrale Marseille, I2M, Marseille, France. e-mail: gilles.lachaud@univmed.fr

Michael E. O'Sullivan
Department of Mathematics and Statistics, San Diego State University, San Diego, CA 92182-7720, USA. e-mail: mosullivan@mail.sdsu.edu

Samrith Ram
Harish-Chandra Research Institute, Chhatnag Road, Jhusi, Allahabad 211019, India. e-mail: samrithram@hri.res.in

## 1.1 Introduction

Let $q$ be a prime power and let $\mathbb{F}_q$ denote the finite field with $q$ elements. Let $d \geq 0$ and $m \geq 1$ be integers. For any integer $r$, we define

$$p_r := \left|\mathbb{P}^r(\mathbb{F}_q)\right| = q^r + q^{r-1} + \cdots + 1 \quad \text{for } r \geq 0 \quad \text{and} \quad p_r := 0 \text{ for } r < 0.$$

In a letter to M. Tsfasman in 1989, J.-P. Serre [18] proved that for any nonzero homogeneous degree $d$ polynomial $F \in \mathbb{F}_q[X_0, X_1, \ldots, X_m]$, the hypersurface $V(F)$ consisting of $\mathbb{F}_q$-rational zeros of $F$ in the projective $m$-space $\mathbb{P}^m$ satisfies

$$|V(F)| \leq dq^{m-1} + p_{m-2}. \tag{1.1}$$

Note that if $d \geq q+1$, then $dq^{m-1} + p_{m-2} \geq p_m = \left|\mathbb{P}^m(\mathbb{F}_q)\right|$, and thus the above bound is trivial in this case; moreover, the polynomial $X_0^{d-q-1}(X_0^q X_1 - X_0 X_1^q)$ is evidently homogeneous of degree $d \geq q+1$ and has $p_m$ zeros in $\mathbb{P}^m(\mathbb{F}_q)$. On the other hand, in the nontrivial case when $d \leq q+1$, the bound (1.1) is met by

$$F = \prod_{i=1}^{d} (\alpha_i X_0 - \beta_i X_1), \tag{1.2}$$

whenever $(\alpha_1 : \beta_1), (\alpha_2 : \beta_2), \ldots, (\alpha_d : \beta_d)$ are distinct elements of $\mathbb{P}^1(\mathbb{F}_q)$. It follows that if we let $e_q(d,m)$ denote the maximum possible number of $\mathbb{F}_q$-rational zeros in $\mathbb{P}^m$ that a nonzero homogeneous polynomial of degree $d$ in $\mathbb{F}_q[X_0, X_1, \ldots, X_m]$ can admit, then

$$e_q(d,m) = \min\{p_m,\ dq^{m-1} + p_{m-2}\}. \tag{1.3}$$

Alternative proofs of (1.1), and hence (1.3), can be found in [19] and [6], whereas some extensions and generalizations are given in [5] and [7]. Serre's result has also been applied to determine the minimum distance of the projective Reed–Muller codes, which were introduced by Lachaud in [13], and further studied in [14] and [19].

In this paper we discuss how the bound (1.1) can possibly be generalized to weighted projective spaces, along with a number of partial results and some implications for coding theory. Let us recall that given any positive integers $a_0, a_1, \ldots, a_m$, the corresponding weighted projective space is defined by

$$\mathbb{P}(a_0, a_1, \ldots, a_m) := \left(\overline{\mathbb{F}}_q^{m+1} \setminus \{(0,0,\ldots,0)\}\right) / \sim$$

where $\overline{\mathbb{F}}_q$ denotes an algebraic closure of $\mathbb{F}_q$ and the equivalence relation $\sim$ is such that

$$(x_0, x_1, \ldots, x_m) \sim (\lambda^{a_0} x_0, \lambda^{a_1} x_1, \ldots, \lambda^{a_m} x_m) \quad \text{for every } \lambda \in \overline{\mathbb{F}}_q^*.$$

The corresponding equivalence class is denoted by $(x_0 : x_1 : \cdots : x_m)$ and is called a weighted projective point. We say that the point is $\mathbb{F}_q$-rational if $(x_0 : x_1 : \cdots : x_m) = (x_0^q : x_1^q : \cdots : x_m^q)$. It can be shown using Hilbert's theorem 90 that every $\mathbb{F}_q$-rational

point has at least one representative in $\mathbb{F}_q^{m+1} \setminus \{(0,0,\ldots,0)\}$. In fact, a finer analysis shows that it has exactly $q-1$ such representatives; see [16, §3]. In particular, the total number of $\mathbb{F}_q$-rational points equals $p_m$, i.e. it is the same as in the non-weighted case. The weighted projective spaces are fascinating objects. On the one hand, they are analogous to classical projective spaces, but they are often difficult to deal with, partly since they can admit singularities. For the convenience of the reader, and possible future use, we include at the end of this paper a fairly self-contained appendix that provides a glossary of various notions and results concerning weighted projective spaces.

Now let $\mathsf{S} = \mathbb{F}_q[X_0, X_1, \ldots, X_m]$ and consider a nonzero polynomial $F \in \mathsf{S}$ which is homogeneous of degree $d$ provided that we measure $X_i$ with weight $a_i$ for each $i = 0, 1, \ldots, m$, so that

$$F(\lambda^{a_0} X_0, \lambda^{a_1} X_1, \ldots, \lambda^{a_m} X_m) = \lambda^d F(X_0, X_1, \ldots, X_m) \quad \text{for all } \lambda \in \overline{\mathbb{F}}_q^*.$$

Thus it is meaningful to consider the weighted projective hypersurface $V(F)$ of $\mathbb{F}_q$-rational points of $\mathbb{P}(a_0, a_1, \ldots, a_m)$ at which $F$ vanishes. Our object of study is the quantity

$$e_q(d; a_0, a_1, \ldots, a_m) := \max_{F \in \mathsf{S}_d \setminus \{0\}} |V(F)|,$$

where $\mathsf{S}_d$ denotes the space of weighted homogeneous polynomials in $\mathsf{S}$ of degree $d$. One caveat is that $\mathsf{S}_d$ might be trivial for certain values of $d$ (namely those values that are not contained in the semigroup $a_0\mathbb{Z}_{\geq 0} + a_1\mathbb{Z}_{\geq 0} + \ldots + a_m\mathbb{Z}_{\geq 0}$), in which case we say that $e_q(d; a_0, a_1, \ldots, a_m)$ is *not defined*. Also note that $e_q(d; a_0, a_1, \ldots, a_m)$ is not necessarily increasing as a function in $d$: for instance $e_q(7; 3, 4) = 2$ while $e_q(8; 3, 4) = 1$ since the only monomials of (weighted) degree 7 and 8 are constant multiples of $X_0X_1$ and $X_1^2$ respectively.

Seeking inspiration in the example (1.2) that meets Serre's bound, it is natural to consider polynomials of the form

$$F = \prod_{i=1}^{d/a_{rs}} (\alpha_i X_r^{a_{rs}/a_r} - \beta_i X_s^{a_{rs}/a_s}), \tag{1.4}$$

where $r, s \in \{0, 1, \ldots, m\}$ are distinct indices, $a_{rs}$ is the least common multiple of $a_r$ and $a_s$, $d$ is a multiple of $a_{rs}$ satisfying $d \leq a_{rs}(q+1)$, and the $(\alpha_i : \beta_i)$'s are distinct elements of $\mathbb{P}^1(\mathbb{F}_q)$. In Section 1.2 we will prove that $|V(F)| = (d/a_{rs})\, q^{m-1} + p_{m-2}$, leading to the following lower bound:

**Lemma 1.** *Let $a = \min\{\operatorname{lcm}(a_r, a_s) : 0 \leq r < s \leq m\}$ and assume that $a \mid d$. Then*

$$e_q(d; a_0, a_1, \ldots, a_m) \geq \min\left\{ p_m,\ \frac{d}{a} q^{m-1} + p_{m-2} \right\}.$$

*Example 1.* Let us prove that equality holds in the lemma for $\mathbb{P}(a_0, a_1)$. Writing $a = \operatorname{lcm}(a_0, a_1)$, we want to prove that $e_q(d; a_0, a_1) = \min\{p_1, d/a\}$. Let $F \in \mathsf{S}_d \setminus \{0\}$ and note that

$$F(X_0,X_1)/X_1^{d/a_1}$$

can be viewed as a univariate polynomial in $T = X_0^{a/a_0}/X_1^{a/a_1}$. Indeed, if a monomial $X_0^{\beta_0}X_1^{\beta_1}$ is weighted homogeneous of degree $d$, so that $\beta_0 a_0 + \beta_1 a_1 = d$, then an easy calculation shows that

$$\frac{X_0^{\beta_0}X_1^{\beta_1}}{X_1^{d/a_1}} = \left(\frac{X_0^{a/a_0}}{X_1^{a/a_1}}\right)^{\beta_0 a_0/a}.$$

Let $d = ak$ and $b_i = a/a_i$ for $i = 0,1$. Now factor $F(X_0,X_1)/X_1^{b_1 k}$ and remultiply with $X_1^{b_1 k}$ to obtain

$$F(X_0,X_1) = c \cdot X_1^{b_1 \ell} \cdot \prod_{i=1}^{k-\ell} \left(X_0^{b_0} - t_i X_1^{b_1}\right)$$

for some $\ell \leq k$, some $t_i \in \overline{\mathbb{F}}_q$ and some leading coefficient $c \in \mathbb{F}_q^*$. Each factor for which $t_i \in \mathbb{F}_q$ has a unique $\mathbb{F}_q$-rational zero in $\mathbb{P}(a_0,a_1)$. Indeed, to see this it suffices to show that such a factor has exactly $q-1$ solutions $(X_0,X_1) \in \mathbb{F}_q^2 \setminus \{(0,0)\}$, which easily follows from the coprimality of $b_1,b_2$; see also Lemma 3 below. On the other hand, a factor for which $t_i \notin \mathbb{F}_q$ clearly cannot have any $\mathbb{F}_q$-rational zeroes. This shows that $e_q(d;a_0,a_1) = k = d/a$ for $d \leq q+1$.

In Section 1.2 we will generalize the class of polynomials (1.4) to a larger family which shows that the inequality may be strict if $m > 1$. We prudently conjecture that the actual value of $e_q(d;a_0,a_1,\ldots,a_m)$ is always attained by one of these generalizations (as soon as it is defined), but elaborating this into a concrete statement amounts to tedious additive number theory and is omitted.

One assumption that simplifies the combinatorics is $\operatorname{lcm}(a_0,a_1,\ldots,a_m) \mid d$; in what follows we will usually suppose that this is the case. Another hypothesis which turns out to simplify things significantly is that one of the weights (say $a_0$) equals 1. Under these assumptions, we conjecture:

*Conjecture 1. If $a_0 = 1$ and $\operatorname{lcm}(a_1,a_2,\ldots,a_m) \mid d$, then the bound from Lemma 1 is sharp. In other words, if we order the weights such that $a_1 \leq a_2 \leq \ldots \leq a_m$, then*

$$e_q(d;1,a_1,a_2,\ldots,a_m) = \min\left\{p_m, \frac{d}{a_1}q^{m-1} + p_{m-2}\right\}.$$

This immediately specializes to Serre's bound for $a_1 = \ldots = a_m = 1$. The right-hand side equals $\frac{d}{a_1}q^{m-1} + p_{m-2}$ if and only if $d \leq a_1(q+1)$, which will be assumed in practice because the other case is again easy to handle.

In the statement of Conjecture 1 it can be assumed without loss of generality that $\gcd(a_1,a_2,\ldots,a_m) = 1$. This follows from Delorme weight reduction [8], which states that for any index $i$ and any positive integer $b$ coprime to $a_i$,

$$\mathbb{P}(a_0 b,\ldots,a_{i-1}b,a_i,a_{i+1}b,\ldots,a_m b) \cong \mathbb{P}(a_0,a_1,\ldots,a_m),$$

the underlying observation being that an $(a_0b,\dots,a_{i-1}b,a_i,a_{i+1}b,\dots,a_mb)$-weighted homogeneous polynomial of degree $d=kb$ (with $k$ some integer) can be easily transformed into an $(a_0b,\dots,a_{i-1}b,a_ib,a_{i+1}b,\dots,a_mb)$-weighted homogeneous polynomial of the same degree, by replacing each occurrence of $X_i^b$ by $X_i$. A rescaling of the weights then allows us to view this as an $(a_0,a_1,\dots,a_m)$-weighted homogeneous degree $k$ polynomial. See the treatments in [12, §3.3], [17, §3.6], [10, §1] for more details. For our needs, the relevant observation is that there is a one-to-one correspondence between the respective $\mathbb{F}_q$-rational zeroes given by

$$(\alpha_0:\ldots:\alpha_{i-1}:\alpha_i:\alpha_{i+1}:\ldots:\alpha_m)\ \mapsto\ (\alpha_0:\ldots:\alpha_{i-1}:\alpha_i^b:\alpha_{i+1}:\ldots:\alpha_m).$$

In particular the Delorme isomorphism respects Conjecture 1 in the sense that $e_q(db;1,a_1b,a_2b,\dots,a_mb)$ and $e_q(d;1,a_1,a_2,\dots,a_m)$ have the same value.

For $m=1$, the validity of Conjecture 1 follows from the example discussed above; we note that alternatively this example could have been settled by reducing to the case of $\mathbb{P}^1(1,1)$ using Delorme weight reduction (preceded by a rescaling of the weights if needed to ensure that $\gcd(a_0,a_1)=1$). In Section 1.3 we give further evidence in favour of Conjecture 1:

**Theorem 1.** *Conjecture 1 is true if $m\leq 2$.*

The proof for $m=2$ is done by mimicking Serre's original method. In order to do so, our main task is to come up with a convenient notion of 'lines' inside the weighted projective plane, which is not obvious a priori. The handy property of $\mathbb{P}(1,a_1,a_2)$ is that it naturally arises as a completion of the affine plane $\mathbb{A}^2$, which leads us to consider completed affine lines; as we will see, these indeed allow for a working version of Serre's proof. Even though $\mathbb{P}(1,a_1,a_2)$ is a very particular case, we hope that our approach has the ingredients needed to establish Conjecture 1 in full generality.

Finally, in Section 1.4, we introduce the natural weighted analogue of projective Reed–Muller codes, reinterpret Conjecture 1 in terms of the minimal distance, and examine some further first properties. These codes do not seem to have seen previous study, even though a different notion bearing the name 'weighted projective Reed–Muller codes' was introduced and analyzed by Sørensen [20]. As noted earlier, an appendix giving a formal introduction to weighted projective spaces and many of its geometric aspects is provided at the end.

## 1.2 Polynomials with many zeros

In this section we generalize the class of polynomials considered in (1.4). As before, let $\mathsf{S}$ denote the polynomial ring $\mathbb{F}_q[X_0,X_1,\dots,X_m]$. Fix a grading on $\mathsf{S}$ with respect to weights $\mathsf{a}=(a_0,a_1,\dots,a_m)$ so that $\deg X_i=a_i\geq 1$ $(0\leq i\leq m)$, and for a monomial $M=X_0^{i_0}X_1^{i_1}\cdots X_m^{i_m}$, the (weighted) degree of $M$ is $\deg M=$

$i_0a_0 + i_1a_1 + \cdots + i_ma_m$. We now define a useful notion about pairs of monomials in $\mathsf{S}$.

**Definition 1.** Let $M_0, M_1 \in \mathsf{S}$ be monomials different from 1. If

- $\deg M_0 = \deg M_1$,
- $\gcd(M_0, M_1) = 1$, i.e. no variables appear in both $M_0$ and $M_1$,
- $\gcd(\text{exponents appearing in the monomial } M_0M_1) = 1$,

then we call $(M_0, M_1)$ a *primitive pair*. Denoting by $s_i$ $(i = 0, 1)$ the number of distinct variables appearing in $M_i$, we call $(s_0, s_1)$ the corresponding *signature*.

*Example 2.* For $\mathbb{P}(2,3,5)$, the pairs $(X_0X_1, X_2)$, $(X_0^3, X_1^2)$ are primitive of degrees 5, 6 and signatures $(2,1)$, $(1,1)$, respectively.

Our generalized class consists of weighted homogeneous polynomials of the form

$$F_{\ell,s_0,s_1,\sigma_0,\sigma_1} = \mu_0\mu_1 \prod_{i=1}^{\ell} (M_0 - t_iM_1) \tag{1.5}$$

where $1 \leq s_0 \geq \sigma_0 \geq 0$, $1 \leq s_1 \geq \sigma_1 \geq 0$ are integers and

- $(M_0, M_1)$ is a primitive pair of signature $(s_0, s_1)$,
- $t_1, \ldots, t_\ell$ are distinct elements of $\mathbb{F}_q^*$ (in particular $0 \leq \ell \leq q-1$),
- the (possibly trivial) monomial $\mu_i$ $(i = 0, 1)$ is only divisible by variables that also appear in $M_i$; more precisely it is divisible by $\sigma_i \leq s_i$ such variables.

It is allowed that $\ell = 0$, but in that case we assume that $\sigma_0 = s_0$ and $\sigma_1 = s_1$. In this case $F$ is just a monomial in at least two variables. Strictly speaking, since we assumed that $s_0 \geq 1$ and $s_1 \geq 1$, monomials in one variable (or $F = 1$) are not covered by the construction, but in order to have a chance of meeting $e_q(d; a_0, a_1, \ldots, a_m)$ for every value of $d$ one should include them; since this is speculative anyway, we omit a further discussion of such pathologies.

The construction indeed concerns a generalization of (1.4): modulo scaling, the polynomial

$$\prod_{i=1}^{d/a_{rs}} (\alpha_i X_r^{a_{rs}/a_r} - \beta_i X_s^{a_{rs}/a_s})$$

is of the form $F_{d/a_{rs}-\sigma_0-\sigma_1,1,1,\sigma_0,\sigma_1}$ with $\sigma_0, \sigma_1 \in \{0,1\}$, depending on whether $(1:0)$ or $(0:1)$ are among the points $(\alpha_i : \beta_i)$. Here the underlying primitive pair is $(X_r^{a_{rs}/a_r}, X_s^{a_{rs}/a_s})$.

Of course the polynomial $F_{\ell,s_0,s_1,\sigma_0,\sigma_1}$ is not uniquely determined by the integers $\ell, s_0, s_1, \sigma_0, \sigma_1$, but these are the parameters accounting for the number of $\mathbb{F}_q$-rational points at which it vanishes:

**Lemma 2.** $\left|V(F_{\ell,s_0,s_1,\sigma_0,\sigma_1})\right| = \lambda q^{m+1-s_0-s_1} + p_{m-s_0-s_1}$ *where*

$$\begin{aligned}\lambda = \ell \cdot (q-1)^{s_0+s_1-2} \\ + [(q^{s_0}-(q-1)^{s_0})(q^{s_1}-(q-1)^{s_1})-1]/(q-1) \\ + (q-1)^{s_1-1}q^{s_0-\sigma_0}(q^{\sigma_0}-(q-1)^{\sigma_0}) \\ + (q-1)^{s_0-1}q^{s_1-\sigma_1}(q^{\sigma_1}-(q-1)^{\sigma_1}).\end{aligned}$$

In order to prove this, let us denote the variables appearing in $M_0$ and $M_1$ by $Y_1, Y_2, \ldots, Y_{s_0}$ and $Z_1, Z_2, \ldots, Z_{s_1}$, respectively. These are distinct because of the primitivity of the pair $(M_0, M_1)$. The points at which all these variables vanish have the structure of a weighted projective space of dimension $m - s_0 - s_1$. Since there are $p_{m-s_0-s_1}$ such points which are $\mathbb{F}_q$-rational, our task easily reduces to the case where $s_0 + s_1 = m+1$, meaning that each of the variables $X_0, X_1, \ldots, X_m$ appears among the $Y_i$ or $Z_i$. In the latter case we need to show that $\left|V(F_{\ell,s_0,s_1,\sigma_0,\sigma_1})\right| = \lambda$. We claim that, respectively, the summands in the statement of Lemma 2 correspond to

(i) the zeros all of whose coordinates are nonzero,
(ii) the zeros for which at least one of the $Y_i$'s is zero and at least one of the $Z_i$'s is zero,
(iii) the zeros for which at least one of the $Y_i$'s is zero, but none of the $Z_i$'s is,
(iv) the zeros for which at least one of the $Z_i$'s is zero, but none of the $Y_i$'s is.

As for (i), this immediately follows from the lemma below, along with the primitivity of $(M_0, M_1)$ and the fact that every $\mathbb{F}_q$-rational weighted projective point has exactly $q-1$ rational representatives by [16, §3].

**Lemma 3.** *Let $a_1, a_2, \ldots, a_{s_0}, b_1, b_2, \ldots, b_{s_1}$ be mutually coprime integers and let $\alpha, \beta \in \mathbb{F}_q^*$. Then the number of solutions in the torus $\mathbb{T}_q^{s_0+s_1}(\mathbb{F}_q) := (\mathbb{F}_q^*)^{s_0+s_1}$ of the equation*

$$\alpha x_1^{a_1} x_2^{a_2} \cdots x_{s_0}^{a_{s_0}} - \beta y_1^{b_1} y_2^{b_2} \cdots y_{s_1}^{b_{s_1}} = 0$$

*is given by $(q-1)^{s_0+s_1-1}$.*

*Proof.* Since $a_0, a_1, \ldots, a_{s_0}, -b_0, -b_1, \ldots, -b_{s_1}$ are coprime, these integers can be viewed as the entries in the first row of a matrix $M \in \mathrm{GL}_{s_0+s_1}(\mathbb{Z})$; see [4]. Rewrite the equation as

$$x_1^{a_1} x_2^{a_2} \cdots x_{s_0}^{a_{s_0}} y_1^{-b_1} y_2^{-b_2} \cdots y_{s_1}^{-b_{s_1}} = \alpha^{-1}\beta.$$

Using $M$ it is easy to find a monomial transformation (= an invertible substitution of the variables by Laurent monomials) that takes this equation to

$$x_1 = \alpha^{-1}\beta.$$

This transformation determines a bijection between the respective sets of solutions inside $\mathbb{T}^{s_0+s_1}(\mathbb{F}_q)$, from which the lemma follows. □

As for (ii), note that if a point $(y_1 : y_2 : \ldots : y_{s_0} : z_1 : z_2 : \ldots : z_{s_1})$ satisfies $y_i = 0$ and $z_j = 0$ for at least one pair $y_i, z_j$ then it automatically concerns a zero of $F_{\ell,s_0,s_1,\sigma_0,\sigma_1}$. There are

$$(q^{s_0}-(q-1)^{s_0})(q^{s_1}-(q-1)^{s_1})-1$$

such points in $\mathbb{F}_q^{s_0+s_1}\setminus\{(0,0,\ldots,0)\}$, and so we find the desired contribution, again by using that every $\mathbb{F}_q$-rational point has $q-1$ representatives.

Concerning (iii): these are exactly the zeros of $\mu_0$ that were not counted elsewhere. Once more we adopt the strategy of first counting the number of $\mathbb{F}_q$-rational representatives, after which we divide by $q-1$. At least one of the $\sigma_0$ variables appearing in $\mu_0$ should be set to zero, accounting for the factor $q^{\sigma_0}-(q-1)^{\sigma_0}$, while the other $Y_i$'s can be chosen freely and the $Z_i$'s must be chosen nonzero, accounting for the factors $q^{s_0-\sigma_0}$ and $(q-1)^{s_1}$, respectively.

The case (iv) follows by symmetry. This completes the proof of Lemma 2.

*Example 3.* Consider $\mathbb{P}(2,3,5)$, let $d=30$, and assume $q\geq 5$. Let

$$F_{4,2,1,2,1}=X_0X_1X_2\prod_{i=1}^{4}(X_0X_1-t_iX_2).$$

According to Lemma 2, the number of $\mathbb{F}_q$-rational zeros of $F_{4,2,1,2,1}$ is $7q-4$. We believe that this equals $e_q(30;2,3,5)$, although we currently cannot offer a proof. But at least this shows that the lower bound from Lemma 1, which relied on the polynomial

$$F_{3,1,1,1,1}=X_0^3X_1^2\prod_{i=1}^{3}(X_0^3-t_iX_1^2),$$

can be strict: indeed, $F_{3,1,1,1,1}$ has only $5q+1$ zeros. On the other hand, for $q=4$, this last polynomial trivially meets $e_q(30;2,3,5)$ because it is 'space-filling', i.e., its set of $\mathbb{F}_q$-rational zeros equals all of $\mathbb{P}(2,3,5)(\mathbb{F}_q)$.

## 1.3 Hypersurfaces in Weighted Projective Planes $\mathbb{P}(1,a_1,a_2)$

In this section we prove Theorem 1, i.e. we prove Conjecture 1 for weighted projective planes $\mathbb{P}(1,a_1,a_2)$. Note that by Serre's result for classical projective spaces and by Delorme's isomorphism we may assume without loss of generality that $a_1<a_2$ and that these weights are coprime, so $\operatorname{lcm}(a_1,a_2)=a_1a_2$. Let $F\in\mathbb{F}_q[X_0,X_1,X_2]$ be a nonzero polynomial which is weighted homogeneous of degree $d$ with $a_1a_2\mid d$. Assuming that $d\leq a_1(q+1)$, our task is to prove

$$|V(F)|\leq\frac{d}{a_1}q+1. \tag{1.6}$$

This we will do by mimicking Serre's original proof, for which we need a convenient notion of 'lines' in the weighted projective plane. Note that if we define lines merely as subsets that are cut out by a weighted homogeneous polynomial of degree 1, in general the resulting notion is too poor to be of any use (we would usually only find $X_0=0$).

An easy but crucial feature of having $a_0 = 1$ is that every point $(x_0 : x_1 : x_2)$ for which $x_0 \neq 0$ has a unique representative of the form $(1 : x : y)$. Moreover, the point is $\mathbb{F}_q$-rational if and only if $x, y \in \mathbb{F}_q$. Thus the embedding

$$\mathbb{A}^2 \hookrightarrow \mathbb{P}(1, a_1, a_2) : (x, y) \mapsto (1 : x : y)$$

identifies $\mathbb{A}^2$ with the chart $X_0 \neq 0$, in an equivariant way (i.e. the identification continues to hold if one restricts to $\mathbb{F}_q$-rational points). We call $H_\infty : X_0 = 0$ the 'line at infinity'. Note that it naturally carries the structure of the weighted projective line $\mathbb{P}(a_1, a_2)$.

*Remark 1.* We can think of $\mathbb{P}(1, a_1, a_2)$ as the affine plane to which a line at infinity has been glued, albeit in a non-standard way. This can be made precise geometrically (see, for example, Dolgachev [10]) and it turns out (see, for example, Section 2 of the appendix) that, in general, the coordinate points at infinity are singular (we will not use this).

*Remark 2.* Writing $V(F)^{\text{aff}}$ for the set of affine $\mathbb{F}_q$-rational zeroes, it is not too hard to show that $\left|V(F)^{\text{aff}}\right| \leq (d/a_1)q$, for instance using Ore's inequality; see Section 1.A.5.3 of the appendix.

The affine zeros of $F$ are precisely the zeros of the dehomogenized polynomial

$$F(1, x, y) \in \mathbb{F}_q[x, y].$$

Conversely, given a polynomial in $x$ and $y$, there is a natural way of homogenizing it, by substituting $x \leftarrow X_1, y \leftarrow X_2$ and adding to each term as many factors $X_0$ as minimally needed. We define a 'line' in $\mathbb{P}(1, a_1, a_2)$ to be either a homogenized linear bivariate equation, or the line at infinity:

**Definition 2.** An *$\mathbb{F}_q$-rational line* in $\mathbb{P}(1, a_1, a_2)$ is a subset defined by an equation of one of the following types.

- Type 0: The line $X_0 = 0$, which we shall denote $H_\infty$ (the *line at infinity*). Points on this line may be called the *points at infinity*.
- Type 1: Lines of the form $\alpha X_0^{a_1} + X_1 = 0$ with $\alpha \in \mathbb{F}_q$ (*vertical* lines).
- Type 2: Lines of the form $\alpha X_0^{a_2} + \beta X_1 X_0^{a_2 - a_1} + X_2 = 0$ with $\alpha, \beta \in \mathbb{F}_q$ (*non-vertical* lines).

*Remark 3.* Note that using an $\mathbb{F}_q$-rational change of variables that respects the grading, any $\mathbb{F}_q$-rational line of type $i$ can be transformed into $X_i = 0$. For instance, for the vertical line $\alpha X_0^{a_1} + X_1 = 0$ this amounts to substituting $X_1 \leftarrow X_1 - \alpha X_0^{a_1}$.

**Lemma 4.** *Any $\mathbb{F}_q$-rational line in $\mathbb{P}(1, a_1, a_2)$ contains exactly $q+1$ rational points, and any pair of $\mathbb{F}_q$-rational lines in $\mathbb{P}(1, a_1, a_2)$ has at least one rational point in common.*

*Proof.* Being a copy of $\mathbb{P}(a_1,a_2)$, it is clear that the line at infinity in $\mathbb{P}(1,a_1,a_2)$ contains $q+1$ rational points, while all other $\mathbb{F}_q$-rational lines contain $q$ affine points along with a unique point at infinity. Clearly type 1 and type 2 lines meet the line $X_0=0$ and a type 1 line meets a type 2 line in the affine plane. Type 1 lines all meet at $(0:0:1)$ and type 2 lines all meet at $(0:1:0)$. This establishes the lemma. □

The points at infinity $(0:0:1)$ and $(0:1:0)$ on the coordinate axes will be denoted by $P_\infty$ and $P'_\infty$, respectively.

*Remark 4.* Figure 1.1 illustrates the intersection behaviour of lines in $\mathbb{P}(1,a_1,a_2)$; the point $P'_\infty$ acts as a vortex attracting all lines of type 2.

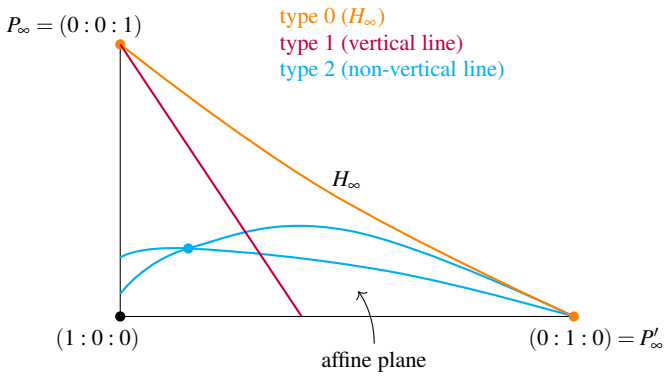



**Fig. 1.1** Lines in $\mathbb{P}(1,a_1,a_2)$.

We are now ready to prove the upper bound for $|V(F)|$ stated in (1.6). Let $H_1,H_2,\ldots,H_t \in \mathbb{F}_q[X_0,X_1,X_2]$ be the distinct 'linear' factors of $F$, i.e. the divisors of $F$ having one of the three forms mentioned in Definition 2. Note that

$$d \geq \deg H_1H_2\cdots H_t \geq 1+(t-1)a_1,$$

which leads to $t \leq d/a_1$ since $a_1 \mid d$. For each $i=1,2,\ldots,t$ we define $L_i = V(H_i)$, and we similarly write $L_\infty = V(X_0)$ for the set of $\mathbb{F}_q$-rational points on $H_\infty$. Let

$$L = \bigcup_{i=1}^{t} L_i.$$

As a first step in the proof, we show that $|L| \leq tq+1$ by induction on $t$. The case $t=0$ is trivial and the case $t=1$ follows from Lemma 4. In the general case we have

$$\begin{aligned}|L| &= \left|\bigcup_{i=1}^{t} L_i\right| \\ &= \left|\bigcup_{i=1}^{t-1} L_i\right| + |L_t| - \left|\bigcup_{i=1}^{t-1} L_i \cap L_t\right| \\ &\leq (t-1)q+1+q+1-1 \\ &= tq+1,\end{aligned}$$

where the second step again uses Lemma 4.

To proceed, we distinguish between three cases.

**Case 1**: Suppose that $V(F) \setminus L \subseteq L_\infty \setminus \{P_\infty\}$.

1. If $L_i = L_\infty$ for some $i$, then we have
$$|V(F)| = |L| \leq (d/a_1)q+1$$
by the previous observation.
2. Suppose $L_i \neq L_\infty$ for all $i$. Then:
   - either $t = d/a_1$, which is possible only if all $H_i$'s are vertical and $V(F) = L$, so again the bound follows (note that this case covers our example (1.4) proving sharpness),
   - or $t < d/a_1$, in which case the following estimate applies:
$$\begin{aligned}|V(F)| &\leq |L| + |L_\infty \setminus \{P_\infty\}| \\ &= |L| + q \\ &\leq tq+1+q \\ &\leq (d/a_1-1)q+1+q \\ &= (d/a_1)q+1.\end{aligned}$$

This concludes the proof in Case 1.

**Case 2**: There exists a point $P \in \mathbb{A}^2$ that lies in $V(F) \setminus L$. Let $X$ denote the set of pairs $(P', H)$ of $\mathbb{F}_q$-rational points and $\mathbb{F}_q$-rational lines such that $P, P' \in V(F) \cap H$ and $P \neq P'$. We are going to estimate the cardinality of $X$ in two ways. On the one hand

$$\begin{aligned}|X| &= \sum_{P' \in V(F)\setminus\{P\}} \left|\{L : L \text{ is a line with } P, P' \in L\}\right| \\ &\geq \sum_{P' \in V(F)^{\text{aff}}\setminus\{P\}} 1 \;=\; \left|V(F)^{\text{aff}} \setminus \{P\}\right|,\end{aligned}$$

where as before $V(F)^{\text{aff}} = V(F) \cap \mathbb{A}^2 = V(F) \setminus L_\infty$. On the other hand, we have

$$|X| = \sum_{\substack{H \ni P \\ H \text{ type } 1}} (|V(F) \cap H| - 1) + \sum_{\substack{H \ni P \\ H \text{ type } 2}} (|V(F) \cap H| - 1)$$

$$\leq \quad 1 \cdot \left( \frac{d}{a_2} - 1 \right) \quad + \quad q \left( \frac{d}{a_1} - 1 \right).$$

($\downarrow X_1 = 0 \rightsquigarrow \mathbb{P}(1, a_2)$ over the first term; $\downarrow X_2 = 0 \rightsquigarrow \mathbb{P}(1, a_1)$ over the second term)

The first vertical arrow above indicates that in order to estimate $|V(F) \cap H|$ for a line $H$ of type 1, we can assume that $H$ is defined by $X_1 = 0$, by using a change of variables if needed by the remark after Definition 2. But then our task is to estimate the number of $\mathbb{F}_q$-rational zeros of $F(X_0, 0, X_2)$ in the weighted projective line $\mathbb{P}(1, a_2)$, which is bounded by $d/a_2$ as observed in the example in Section 1.1, discussing the base case $m = 1$. Here we note that $F(X_0, 0, X_2) \neq 0$ because $H$ contains $P \notin L$. A similar justification goes along with the second vertical arrow.

Combining both estimates, we find that

$$\left| V(F)^{\text{aff}} \setminus \{P\} \right| = \left| V(F)^{\text{aff}} \right| - 1 \leq \frac{d}{a_2} - 1 + q \left( \frac{d}{a_1} - 1 \right).$$

Since $a_1 < a_2$ and $a_1$ and $a_2$ are coprime it follows that

$$\begin{aligned}
|V(F)| &\leq \frac{d}{a_2} + q \left( \frac{d}{a_1} - 1 \right) + |V(F) \cap H_\infty| \\
&\qquad\qquad\qquad\qquad \downarrow X_0 = 0 \rightsquigarrow \mathbb{P}(a_1, a_2) \\
&\leq \frac{d}{a_2} + q \left( \frac{d}{a_1} - 1 \right) \quad + \quad \frac{d}{a_1 a_2} \\
&= q \frac{d}{a_1} + 1 + \frac{d}{a_2} \frac{a_1 + 1}{a_1} - q - 1 \\
&\leq q \frac{d}{a_1} + 1 + \frac{d}{a_1} - q - 1 \\
&\leq q \frac{d}{a_1} + 1,
\end{aligned}$$

where the last inequality uses our assumption that $d \leq a_1(q+1)$. This ends the proof in Case 2.

**Case 3**: One has $P_\infty \in V(F) \setminus L$. This case is similar but easier. Using the same definition of $X$ with $P = P_\infty$, one finds on the one hand that

$$\begin{aligned}
|X| &= \sum_{P' \in V(F) \setminus \{P\}} \left| \{ L : L \text{ is a line with } P, P' \in L \} \right| \\
&= \sum_{P' \in V(F) \setminus \{P\}} 1 \\
&= |V(F)| - 1,
\end{aligned}$$

and, on the other hand, that

$$\begin{aligned} |X| &= \sum_{H \text{ type } 0} (|V(F)\cap H|-1) + \sum_{H \text{ type } 1} (|V(F)\cap H|-1) \\ &\qquad\qquad \downarrow X_0 = 0 \rightsquigarrow \mathbb{P}(a_1,a_2) \qquad\qquad \downarrow X_1 = 0 \rightsquigarrow \mathbb{P}(1,a_2) \\ &\leq \quad 1\cdot\left(\frac{d}{a_1a_2}-1\right) \quad + \quad q\left(\frac{d}{a_2}-1\right). \end{aligned}$$

Together, this combines to yield

$$\begin{aligned} |V(F)| &\leq \frac{d}{a_1a_2} + q\left(\frac{d}{a_2}-1\right) \\ &\leq \frac{d}{a_1} + q\frac{d}{a_1} - q \\ &\leq q\frac{d}{a_1} + 1, \end{aligned}$$

where the last step uses $d \leq a_1(q+1)$. Thus Theorem 1 is proved.

## 1.4 Weighted projective Reed–Muller codes

In this section, we outline how the considerations of the previous sections can be applied to coding theory. Recall that a ($q$-ary) linear code of length $n$ and dimension $k$ is, by definition, a $k$-dimensional subspace of $\mathbb{F}_q^n$. The minimum distance of such a code $C$ is defined by

$$d(C) := \min\{\mathrm{wt}(x) : x \in C \text{ with } x \neq 0\},$$

where for any $x = (x_1,\ldots,x_n)$, the Hamming weight $\mathrm{wt}(x)$ is the number of nonzero coordinates in $x$, i.e., $|\{i : x_i \neq 0\}|$. We usually say that a $q$-ary linear code $C$ has parameters $[n,k,d]$ or that $C$ is a $[n,k,d]_q$-code if $C$ has length $n$, dimension $k$, and minimum distance $d$. We shall begin by reviewing some classical families of linear codes.

### *1.4.1 Generalized Reed–Muller codes, projective Reed–Muller codes and projective nested cartesian codes*

The generalized Reed–Muller code over $\mathbb{F}_q$ of order $d$ and with $m$ variables has been introduced by Delsarte, Goethals and MacWilliams in 1970 in [9]. It is denoted by $\mathrm{RM}_q(d,m)$ and defined as the image of the evaluation map

$$c\colon \mathbb{F}_q[X_1,\dots,X_m]_{\le d} \longrightarrow \mathbb{F}_q^{q^m} \quad \text{given by} \quad c(f) = (f(P))_{P\in\mathbb{A}^m(\mathbb{F}_q)},$$

where $\mathbb{F}_q[X_1,\dots,X_m]_{\le d}$ denotes the $\mathbb{F}_q$-vector space of all polynomials in $m$ variables $X_1,\dots,X_m$ with coefficients in $\mathbb{F}_q$ and with degree $\le d$.

If $d < q$, then the evaluation map $c$ is injective, and so the dimension of $\mathrm{RM}_q(d,m)$ equals $\dim_{\mathbb{F}_q} \mathbb{F}_q[X_1,\dots,X_m]_{\le d}$, which is $\binom{d+m}{m}$. The minimum distance can be deduced from a classical result of Ore (cf. noted in [15, Thm. 6.13]), which implies that the maximal number of zeros in $\mathbb{A}^m(\mathbb{F}_q)$ of a polynomial in $\mathbb{F}_q[X_1,\dots,X_m]$ of degree $d$ is equal to $dq^{m-1}$. Thus we have:

**Proposition 1.** *If $d < q$, then the code $\mathrm{RM}_q(d,m)$ has parameters*

$$\left[q^m,\ \binom{d+m}{d},\ (q-d)q^{m-1}\right].$$

The projective Reed–Muller codes were introduced and studied by Lachaud [13, 14] and Sørensen [19] by the late 1980's and early 1990's. They can be defined as follows.

Choose representatives in $\mathbb{F}_q^{m+1}$ for $\mathbb{F}_q$-rational points of the (usual) projective space $\mathbb{P}^m$ in such a way that the first nonzero coordinate is 1. Let $P_1,\dots,P_{p_m}$ be a fixed collection of such representatives for the points of $\mathbb{P}^m(\mathbb{F}_q)$. Now the evaluation map

$$c\colon \mathbb{F}_q[X_1,\dots,X_m]_d \longrightarrow \mathbb{F}_q^{p_m} \quad \text{given by} \quad c(f) = (f(P_1),\dots f(P_{p_m}))$$

is injective if $d \le q$ and we define $\mathrm{PRM}_q(d,m)$ to be the image of this map. Using (1.3), we can deduce the following.

**Proposition 2.** *If $d \le q$, then the code $\mathrm{PRM}_q(d,m)$ has parameters*

$$\left[p_m,\ \binom{d+m}{d},\ (q-d+1)q^{m-1}\right].$$

This construction has been generalized in [1] where the evaluation of the homogeneous polynomials is done on the rational points of an hypersurface of $\mathbb{P}^m(\mathbb{F}_q)$, most notably on quadric hypersurfaces. The parameters of such codes have been improved in 3 and 4-dimensional projective spaces in a series of papers (see, for example, [11]).

Recently, Carvalho, Lopez Neumann and López have proposed in [3] another generalization of $\mathrm{PRM}_q(d,m)$. In their paper, the evaluation of homogeneous polynomials is done on suitable representatives in $\mathbb{F}_q^{m+1}$ of projective cartesian sets $\{(a_0 : a_1 : \cdots : a_m) \in \mathbb{P}^m(\mathbb{F}_q) : a_i \in A_i \text{ for } i = 0,1,\dots,m\}$, where $A_0, A_1, \dots, A_m$ are nonempty subsets of $\mathbb{F}_q$.

### *1.4.2 Weighted projective Reed–Muller codes*

Let $a_0,\dots,a_m$ be positive integers such that $\gcd(a_0,a_1,\dots,a_m)=1$. Denote the $(m+1)$-tuple $(a_0,a_1,\dots,a_m)$ by $\mathsf{a}$. Consider an integer $d$ which is a multiple of the least common multiple of the $a_i$'s, say $d=k\,\mathrm{lcm}(a_0\dots a_m)$.

We consider the weighted projective space $\mathbb{P}(\mathsf{a})=\mathbb{P}(a_0,\dots,a_m)$ of dimension $m$ with weights $a_0,\dots,a_m$ over $\mathbb{F}_q$, whose definition was recalled in Section 1.1. Note that $\mathbb{P}(a_0,\dots,a_m)$ is a disjoint union of $W_0,W_1,\dots,W_m$, where for $0\le i\le m$,

$$W_i := \{(x_0:\cdots:x_m)\in\mathbb{P}(a_0,\dots,a_m) : x_0=\cdots=x_{i-1}=0,\ x_i\neq 0\}.$$

As before, let $\mathsf{S}_d$ denote the space of weighted homogeneous polynomials of degree $d$. We define the Weighted Projective Reed–Muller code of order $d$ over $\mathbb{P}(a_0,\dots,a_m)(\mathbb{F}_q)$, denoted by $\mathrm{WPRM}_q(d,m;\mathsf{a})$, as the image of the linear map

$$c\colon \mathsf{S}_d \longrightarrow \mathbb{F}_q^{p_m} \quad \text{given by} \quad c(F)=(c_x(F))_{x\in\mathbb{P}(\mathsf{a})(\mathbb{F}_q)},$$

where for $x=(x_0:x_1:\cdots:x_m)\in\mathbb{P}(\mathsf{a})(\mathbb{F}_q)$,

$$c_x(F)=\frac{F(x_0,\dots,x_m)}{x_i^{d/a_i}} \quad \text{if } x=(x_0:\cdots:x_m)\in W_i.$$

Observe that the map $c$ is well defined. Indeed, for a nonzero $\lambda\in\overline{\mathbb{F}}_q$, if $y=(\lambda^{a_0}x_0:\cdots:\lambda^{a_m}x_m)=(x_0:\cdots:x_m)=x\in W_i$, then

$$c_y(F)=\frac{F(\lambda^{a_0}x_0,\dots,\lambda^{a_m}x_m)}{(\lambda^{a_i}x_i)^{d/a_i}}=\frac{\lambda^d F(x_0,\dots,x_m)}{\lambda^d x_i^{d/a_i}}=c_x(F).$$

This argument shows also that $c_x(F)\in\mathbb{F}_q$ since every point $x$ of $\mathbb{P}(\mathsf{a})(\mathbb{F}_q)$ has weighted homogeneous coordinates $(x_0:x_1:\cdots:x_m)$ such that $x_i\in\mathbb{F}_q$ for $i=0,1,\dots,m$.

#### 1.4.2.1 Length and dimension

The length of $\mathrm{WPRM}_q(d,m;\mathsf{a})$ is clearly $p_m=q^m+\cdots+q+1$. Assume that $d\le q$. Then the linear map $c$ in injective and so the dimension of $\mathrm{WPRM}_q(d,m;\mathsf{a})$ is equal to the dimension of the $\mathbb{F}_q$-vector space $\mathsf{S}_d$, which is equal to the number of representations of $d$ as a nonnegative integer linear combination of $a_0,\dots,a_m$:

$$\left|\{(\alpha_0,\dots,\alpha_m)\in\mathbb{Z}_{\ge 0}^{m+1} : \alpha_0a_0+\cdots+\alpha_ma_m=d\}\right|.$$

Note that, using a theorem of Schur (see, e.g., [21, Thm. 3.15.2]), we have an asymptotic formula

$$\dim \mathrm{WPRM}_q(d,m;\mathsf{a}) = \frac{d^m}{m!a_0\dots a_m} + O(d^{m-1}) \quad \text{when } d \to \infty.$$

If we suppose that $a_0 = 1$, then this dimension is equal to

$$\left|\{(\alpha_1,\dots,\alpha_m) \in \mathbb{Z}_{\geq 0}^{m+1} : \alpha_1 a_1 + \cdots + \alpha_m a_m \leq d\}\right|.$$

This can be viewed as the number of integral points in an integral convex polytope and then the dimension can be obtained using Ehrhart polynomials (see the examples below in dimension 2).

#### 1.4.2.2 Minimum distance

The minimum distance of $\mathrm{WPRM}_q(d,m;\mathsf{a})$ is equal to the number of rational points on $\mathbb{P}(\mathsf{a})(\mathbb{F}_q)$ minus the maximal number of points on a hypersurface $V$ of degree $d$ of $\mathbb{P}(\mathsf{a})(\mathbb{F}_q)$. Thus we can determine it using the results of the previous sections.

First, suppose $i,j \in \{0,1,\dots,m\}$ and $d' \in \mathbb{Z}$ are such that

$$\mathrm{lcm}(a_i,a_j) = \min\{\mathrm{lcm}(a_r,a_s), r \neq s\}, \quad \text{and} \quad d' := \frac{d}{\mathrm{lcm}(a_i,a_j)}.$$

Then from Lemma 1, we see that

$$d(\mathrm{WPRM}_q(d,m;\mathsf{a})) \leq (q-d'+1)q^{m-1}.$$

Furthermore, if $a_0 = 1$ and $m = 2$ and we assume, without loss of generality that $a_1 \leq a_2$, then from Theorem 1, we see that

$$d(\mathrm{WPRM}_q(d,2;\mathsf{a})) = \left(q - \frac{d}{a_1} + 1\right) q^{m-1}. \tag{1.7}$$

#### 1.4.2.3 A particular case

Consider the particular case of the weighted projective plane $\mathbb{P}(1,1,a)$, where $a$ is a positive integer. Also let $\mathsf{a} = (1,1,a)$. Given a convex polytope $\Delta$ whose vertices have integral coordinates, the function which assigns to a nonnegative integer $k$ the number $|k\Delta \cap \mathbb{Z}^m|$ of integral points in dilates $k\Delta$ of $\Delta$ is a polynomial of degree $m$, called the Ehrhart polynomial of $\Delta$ (see, for example, [2]). For $m = 2$, this polynomial can be written in the following way:

$$\left|k\Delta \cap \mathbb{Z}^2\right| = \mathrm{Vol}(\Delta)k^2 + \frac{1}{2}\left|\partial\Delta \cap \mathbb{Z}^2\right|k + 1.$$

Hence we find that, for $d = ka$, the dimension of the code $\mathrm{WPRM}_q(d,2;\mathsf{a})$ is equal to

$$\frac{1}{2}ak^2+\frac{a+2}{2}k+1=\frac{d^2}{2a}+\frac{(a+2)d}{2a}+1=\frac{(d+a)(d+2)}{2a}.$$

Since we have $d'=d$ in our case, we find from (1.7) that the minimum distance of $\mathrm{WPRM}_q(d,2;\mathsf{a})$ is $q^2-(d-1)q$.

Thus, the code $\mathrm{WPRM}_q(d,2;\mathsf{a})$ has parameters

$$\left[p_2,\ \frac{(d+a)(d+2)}{2a},\ q^2-(d-1)q\right]$$

and we can compare it to the parameters of the code $\mathrm{PRM}_q(d,2)$, which are

$$\left[p_2,\ \frac{(d+1)(d+2)}{2},\ q^2-(d-1)q\right].$$

We find here that the weighted projective Reed–Muller code has the same length and the same minimum distance, but worse dimension than the projective Reed–Muller code.

#### 1.4.2.4 Another particular case

Let $a,b$ be positive integers with $a\leq b$ and let $\mathsf{a}=(1,a,b)$. Consider the particular case of the weighted projective plane $\mathbb{P}^2(1,a,b)$ and consider an integer $d=k\,\mathrm{lcm}(a,b)$ with $d\leq q$. Arguing as before, we can deduce the following.

**Proposition 3.** *The code* $\mathrm{WPRM}_q(d,2;\mathsf{a})$ *has parameters*

$$\left[p_2,\ \frac{(d+2a)(d+b)+(\gcd(a,b)-a)d}{2ab},\ q^2-\left(\frac{d}{a}-1\right)q\right].$$

In particular, if $a=2$ and $b\geq 2$, we see that the minimum distance of the code $\mathrm{WPRM}_q(d,2;(1,2,b))$ is always better than the minimum distance of $\mathrm{PRM}_q(d,2)$, but the dimension of $\mathrm{WPRM}_q(d,2;(1,2,b))$ is always worse than the dimension of $\mathrm{PRM}_q(d,2)$.

#### 1.4.2.5 Relative parameters

Recall that, for any code $C$, the transmission rate $R(C)$ and the relative distance $\delta(C)$ of $C$ are defined by

$$R(C)=\frac{\dim C}{\mathrm{length}\,C}\quad\text{and}\quad\delta(C)=\frac{\mathrm{dist}\,C}{\mathrm{length}\,C}.$$

The number

$$\lambda(C)=R(C)+\delta(C)=(\dim C+\mathrm{dist}\,C)/\mathrm{length}\,C$$

is a parameter of $C$ and it is suggested in [14] that it can be taken as a measure of the performance of the code $C$.

It is proved in [14] that if $q \geq d+1$, $m \geq 2$, and $d \geq 2m/(m-1)$, then

$$\lambda(\mathrm{PRM}_q(d,m)) > \lambda(\mathrm{RM}_q(d,m)).$$

If $q$ is sufficiently large then one can show that $\mathrm{WPRM}_q(d,2;(1,2,2))$ has a greater (and thus better) performance than $\mathrm{PRM}_q(d,2)$:

**Proposition 4.** *If $q \geq \frac{3k+3}{2}$, then*

$$\lambda(\mathrm{WPRM}_q(2k,2;(1,2,2))) \geq \lambda(\mathrm{PRM}_q(2k,2)).$$

*Proof.* Since the lengths of these codes are equal (namely to $p_2$), we just have to show that the sum of the dimension and the minimum distance is greater for the first code when $q$ is sufficiently large. Applying Propositions 2 and 3 yields the desired result. □

In the same way, it is easy to see that:

**Proposition 5.** *If $q \geq \frac{7k+4}{2}$, then*

$$\lambda(\mathrm{WPRM}_q(4k,\ 2;\ (1,2,4))) \geq \lambda(\mathrm{PRM}_q(4k,2)).$$

More generally, using Propositions 2 and 3 we can show that:

**Theorem 2.** *For any nonnegative integers $a, \beta$ and $k$ with $a \geq 2$,*

$$\lambda(\mathrm{WPRM}_q(ka\beta,\ 2;\ (1,a,a\beta))) \geq \lambda(\mathrm{PRM}_q(ka\beta,2)),$$

*provided*

$$q \geq \frac{k\beta^2a^2+3\beta a-k\beta-\beta-2}{2\beta(a-1)}.$$

Let us compare the performance over $\mathbb{F}_{19}$ and in degree 16 of the generalized Reed–Muller code over $\mathbb{A}^2$, the projective Reed–Muller code over $\mathbb{P}^2$, and the weighted projective Reed–Muller codes over the five different weighted projective planes $\mathbb{P}(1,2,2)$, $\mathbb{P}(1,2,4)$, $\mathbb{P}(1,2,8)$, $\mathbb{P}(1,4,4)$ and $\mathbb{P}(1,16,16)$.

We find that $\mathrm{RM}_{19}(16,2)$ has parameters $[361,153,57]$ and the projective counterpart $\mathrm{PRM}_{19}(16,2)$ has parameters $[381,153,76]$, whereas

- $\mathrm{WPRM}_{19}(16,2;(1,2,2))$ has parameters $[381,45,228]$,
- $\mathrm{WPRM}_{19}(16,2;(1,2,4))$ has parameters $[381,25,228]$,
- $\mathrm{WPRM}_{19}(16,2;(1,2,8))$ has parameters $[381,15,228]$,
- $\mathrm{WPRM}_{19}(16,2;(1,4,4))$ has parameters $[381,15,304]$, and
- $\mathrm{WPRM}_{19}(16,2;(1,16,16))$ has parameters $[381,3,361]$.

The affine and projective Reed–Muller codes above have performances

$$\lambda(\mathrm{RM}_{19}(16,2)) = 0.581... \quad \text{and} \quad \lambda(\mathrm{PRM}_{19}(16,2)) = 0.601...,$$

whereas the performances of the above five weighted projective Reed–Muller codes are 0.716..., 0.664..., 0.637..., 0.837..., and 0.955... respectively.

## Acknowledgement

This work was initiated during a week-long IPAM workshop on Algebraic Geometry for Coding and Cryptography, that was held in UCLA during February 2016. The authors would like to thank the organizers of the workshop, namely, Everett Howe, Kristin Lauter and Judy Walker for giving them this opportunity, and the anonymous referee for various helpful comments. The second author was partially supported by the European Commission under the ICT programme with contract H2020-ICT-2014-1 645622 PQCRYPTO, and through the European Research Council under the FP7/2007-2013 programme with ERC Grant Agreement 615722 MOTMELSUM.

## References

1. Yves Aubry, *Reed–Muller codes associated to projective algebraic varieties*, Coding theory and algebraic geometry (Luminy, 1991) (H. Stichtenoth and M. A. Tsfasman, eds.), Lecture Notes in Mathematics, vol. 1518, Springer, Berlin, 1992, pp. 4–17.
2. M. Beck, J. A. De Loera, M. Develin, J. Pfeifle, and R. P. Stanley, *Coefficients and roots of Ehrhart polynomials*, Integer points in polyhedra — Geometry, number theory, algebra, optimization (A. Barvinok, M. Beck, C. Haase, B. Reznick, and V. Welker, eds.), Contemporary Mathematics, vol. 374, American Mathematical Society, Providence, RI, 2005, pp. 15–36.
3. Cícero Carvalho, Victor G. L. Neumann, and Hiram H. López, *Projective nested cartesian codes*, Bull. Braz. Math. Soc. (N.S.) (2016), 1–20.
4. Keith Conrad, *Primitive vectors and* $\mathrm{SL}_n$, http://www.math.uconn.edu/~kconrad/blurbs/ringtheory/primvector.pdf, undated.
5. Alain Couvreur, *An upper bound on the number of rational points of arbitrary projective varieties over finite fields*, Proc. Amer. Math. Soc. **144** (2016), no. 9, 3671–3685.
6. Mrinmoy Datta and Sudhir R. Ghorpade, *On a conjecture of Tsfasman and an inequality of Serre for the number of points of hypersurfac*
Mosc. Math. J. **15** (2015), no. 4, 715–725.
7. ———, *Number of solutions of systems of homogeneous polynomial equations over finite fields*, Proc. Amer. Math. Soc. **145** (2017), no. 2, 525–541.
8. Charles Delorme, *Espaces projectifs anisotropes*, Bull. Soc. Math. France **103** (1975), no. 2, 203–223.
9. P. Delsarte, J.-M. Goethals, and F. J. MacWilliams, *On generalized Reed–Muller codes and their relatives*, Information and Control **16** (1970), 403–442.
10. Igor Dolgachev, *Weighted projective varieties*, Group actions and vector fields (Vancouver, B.C., 1981) (J. B. Carrell, ed.), Lecture Notes in Mathematics, vol. 956, Springer, Berlin, 1982, pp. 34–71.
11. Frédéric A. B. Edoukou, *Codes defined by forms of degree 2 on quadric varieties in* $\mathbb{P}^4(\mathbb{F}_q)$, Arithmetic, geometry, cryptography and coding theory (G. Lachaud, C. Ritzenthaler, and

M. A. Tsfasman, eds.), Contemporary Mathematics, vol. 487, American Mathematical Sociaety, Providence, RI, 2009, pp. 21–32.
12. Timothy Hosgood, *An introduction to varieties in weighted projective space*, https://thosgood.github.io/pdfs/general/introduction-to-wps.pdf, 2015.
13. Gilles Lachaud, *Projective Reed–Muller codes*, Coding theory and applications (Cachan, 1986) (G. Cohen and P. Godlewski, eds.), Lecture Notes in Computer Science, vol. 311, Springer, Berlin, 1988, pp. 125–129.
14. ———, *The parameters of projective Reed–Muller codes*, Discrete Math. **81** (1990), no. 2, 217–221.
15. Rudolf Lidl and Harald Niederreiter, *Finite fields*, Encyclopedia of Mathematics and its Applications, vol. 20, Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, 1983.
16. Marc Perret, *On the number of points of some varieties over finite fields*, Bull. London Math. Soc. **35** (2003), no. 3, 309–320.
17. Miles Reid, *Graded rings and varieties in weighted projective space*, http://homepages.warwick.ac.uk/~masda/surf/more/grad.pdf, 2002.
18. Jean-Pierre Serre, *Lettre à M. Tsfasman*, Journées Arithmétiques, 1989 (Luminy, 1989), Astérisque, vol. 198–200, 1991, pp. 351–353.
19. Anders Bjært Sørensen, *Projective Reed–Muller codes*, IEEE Trans. Inf. Theory **37** (1991), no. 6, 1567–1576.
20. ———, *Weighted Reed–Muller codes and algebraic-geometric codes*, IEEE Trans. Inf. Theory **38** (1992), no. 6, 1821–1826.
21. Herbert S. Wilf, *generatingfunctionology*, third ed., A K Peters, Ltd., Wellesley, MA, 2006.

## 1.A Appendix: Weighted projective spaces

This appendix is aimed at providing a handy reference for weighted projective spaces over arbitrary fields. While some proofs are occasionally outlined, for most part we provide complete statements of results and suitable references where proofs can be found.

### *1.A.1 Definitions of weighted projective spaces*

#### 1.A.1.1 WPS as a Proj functor

Let $k$ be a field and let $\mathsf{a} = (a_0, \ldots, a_m)$ be a sequence of strictly positive integers. The condition

$$\deg X_i = a_i, \qquad i = 0, \ldots, m$$

defines a gradation of type $\mathbb{Z}$ on the polynomial algebra $\mathsf{S} = k[X_0, \ldots, X_m]$:

$$\mathsf{S} = \bigoplus_{n \geq 0} \mathsf{S}_n$$

such that $\mathsf{S}_n = 0$ if $n < 0$. For a monomial $f = X_0^{r_0} \ldots X_m^{r_m}$, we have

$$\mathsf{a}\text{-deg}\, f = n \quad \Longleftrightarrow \quad a_0 r_0 + \cdots + a_m r_m = n.$$

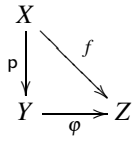
We assume that the characteristic $p$ of $k$ is coprime to all $a_i$ $(0 \leq i \leq m)$, and that $\gcd(a_0, \ldots, a_m) = 1$. The *weighted projective space* (WPS) with sequence of weights $\mathsf{a}$ over $k$ is the scheme $\mathbb{P}(\mathsf{a}) = \operatorname{Proj} \mathsf{S}(\mathsf{a})$. If $\mathsf{a} = (1, \ldots, 1)$, we recover the usual projective space:

$$\mathbb{P}(1, \ldots, 1) = \mathbb{P}^m.$$

### 1.A.1.2 Quotients

Let $G$ be an affine algebraic group over a field $k$ acting on an algebraic variety $X$ over $k$. A *categorical quotient* of $X$ by $G$, see [Do2, p. 92], [Gr, Ch. V, §1], [MFK, Def. 0.5, p. 3], is a morphism $p\colon X \longrightarrow Y$, where $Y$ is a variety over $k$, such that

1. $\mathsf{p}$ is surjective.
2. $\mathsf{p}$ is $G$-invariant, that is, $G$-equivariant, that is, $\mathsf{p}$ is constant on the orbits of $G$.
3. If $f\colon X \longrightarrow Z$ is a $k$-morphism constant on the orbits of $G$, then there exists a $k$-morphism $\varphi\colon Y \longrightarrow Z$ such that $f = \varphi \circ \mathsf{p}$.




The couple $(Y, \mathsf{p})$ is unique up to unique isomorphism. A categorical quotient is called a *geometric quotient*, see [Do2, p. 92], [MFK, Def. 0.6, p. 4], if moreover

4. $\mathsf{p}$ is open.
5. The fibres of $\mathsf{p}$ are the orbits of $G$ in $X$.

### 1.A.1.3 WPS as a quotient of the punctured affine space

The gradation $\mathsf{a}$ of $\mathsf{S}$ defines an action

$$\sigma\colon \mathbb{G}_m \times \mathbb{A}^{m+1} \longrightarrow \mathbb{A}^{m+1}$$

of $\mathbb{G}_m$ on $\mathbb{A}^{m+1}$ such that

$$\sigma(t).(x_0, \ldots, x_m) = t.(x_0, \ldots, x_m) = (t^{a_0} x_0, \ldots, t^{a_m} x_m).$$

The corresponding morphism

$$\sigma^\flat\colon \mathsf{S} \longrightarrow k[T, T^{-1}] \otimes \mathsf{S} \simeq \mathsf{S}[T, T^{-1}]$$

is such that

$$[\sigma^\flat f](T, X_0, \ldots, X_m) = f(T^{a_0} X_0, \ldots, T^{a_m} X_m).$$

The algebra $\mathsf{S}[T, T^{-1}]$ is called the algebra of *Laurent polynomials* over $\mathsf{S}$. The group $\mathbb{G}_m$ operates as well on the pointed cone

$$\mathbb{V} = \mathbb{A}^{m+1} \setminus \{0\}.$$

**Theorem 3.** *The morphism*

$$p \colon \mathbb{V} \longrightarrow \mathbb{V}/\mathbb{G}_m$$

*is a geometric quotient, and there is an isomorphism*

$$\iota \colon \mathbb{V}/\mathbb{G}_m \xrightarrow{\sim} \mathbb{P}(\mathsf{a})$$

*Proof.* [Do1, 1.21, p. 36], [Do2, Ex. 6.2, p. 96]. □

The scheme $\mathbb{P}(\mathsf{a})$ is a normal irreducible projective variety, of dimension $m$ [MFK, p. 5], [Do1, 1.3.3].

### 1.A.1.4 WPS as a finite quotient of the projective space

For any integer $n > 0$, we denote by $\boldsymbol{\mu}_n$ the finite group scheme of $n$-th roots of unity, with coordinate ring $k[X]/(X^n - 1)$. We put

$$G = G_{\mathsf{a}} = \boldsymbol{\mu}_{a_0} \times \cdots \times \boldsymbol{\mu}_{a_m}.$$

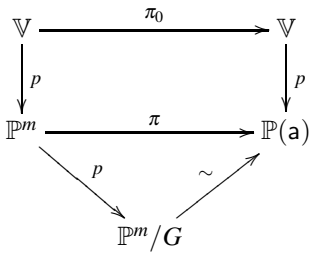
Then $|G_{\mathsf{a}}| = a$, with $a = a_0 \ldots a_m$, and $G_{\mathsf{a}} \simeq \boldsymbol{\mu}_a$ if and only if $a$ is the l.c.m. of $a_0, \ldots, a_m$, that is, if and only if $a_0, \ldots, a_m$ are pairwise coprime. There is a linear action of $G$ on $\mathbb{P}^m$ given by

$$(\zeta_0, \ldots, \zeta_m).(x_0 : \ldots : x_m) = (\zeta_0 x_0 : \ldots : \zeta_m x_m)$$

The morphism $\pi_0 \colon \mathbb{V} \to \mathbb{V}$ given by

$$\pi_0(x_0, \ldots, x_m) = (x_0^{a_0}, \ldots, x_m^{a_m})$$

induces a diagram




Let $G$ be an affine algebraic group over a field $k$ acting on an algebraic variety $X$ over $k$. For the definition of a *good geometric quotient* of $X$ by $G$, see [Do2, p. 92]. We denote by $G(x)$ the *stabilizer* or *isotropy group* of $X$. The action is *free* at $x$ if $G(x)$ is trivial.

**Proposition 6.** *The morphism* $\pi\colon \mathbb{P}^m \longrightarrow \mathbb{P}(\mathsf{a})$ *given by*

$$\pi(x_0 : \ldots : x_m) = (x_0^{a_0} : \ldots : x_m^{a_m})$$

*is a good geometric quotient of $X$ by $G$, and therefore enjoys the following properties:*

1. *$\pi$ is surjective, finite and submersive.*
2. *The fibres of $\pi$ are the orbits of $G$ in $\mathbb{P}^m$.*
3. *If $x \in \mathbb{P}^m$ and $y = \pi(x) \in \mathbb{P}(\mathsf{a})$, the residual field $\kappa(x)$ is a Galois extension of $\kappa(y)$ and the canonical homomorphism of $G(x)$ in the group $\mathrm{Gal}(\kappa(x)/\kappa(y))$ of $\kappa(y)$-automorphisms of $\kappa(x)$ is surjective.*

*Proof.* See [Se, Ch. III, Prop. 19], [Gr, Ch. V, Props. 1.3 and 1.8], [Do2, Ex. 6.1, p. 95]. □

Notice that $\deg \pi = a_0 \ldots a_m$. The Jacobian matrix of $\pi$ is

$$d\pi(x) = \mathrm{Diag}(a_0 x_0^{a_0-1}, \ldots, a_m x_m^{a_m-1}),$$

and

$$\det d\pi(x) = (a_0 \ldots a_m) x_0^{a_0-1} \ldots x_m^{a_m-1}$$

If we denote by $H_i$ the hyperplane $x_i = 0$, the ramification locus is

$$R = \bigcup_{a_i>1} H_i.$$

Then $\pi$ is étale outside $R$, which clearly contains the singular set.

**Proposition 7.** *The scheme $\mathbb{P}(\mathsf{a})$ is Cohen–Macaulay.*

*Proof.* Cf. [BR, Th. 3A.1]. □

### *1.A.2 The singular locus*

We say that the sequence of weights $\mathsf{a}$ is *normalized* [Di, p. 185] or *well formed* [Ho, Def. 3.3.4] if

$$\gcd(a_0,\dots,\widehat{a_i},\dots,a_m) = 1 \quad \text{for every } 0 \le i \le m.$$

Any weighted projective space is isomorphic to a well-formed weighted projective space [*loc. cit*]. If $p$ is a prime number, we put

$$I(p) = \{i \in \{1,\dots,m\} \,:\, p \text{ divides } a_i\}\,.$$

The set $\Sigma = \Sigma(\mathsf{a})$ of prime numbers such that $I(p) \neq \emptyset$ is finite, and $\mathsf{a}$ is *normalized* if and only if $|I(p)| \le m-1$ for every $p$. The space

$$S(p) = \{x \in \mathbb{P}(\mathsf{a}) \,:\, x_i = 0 \text{ if } i \notin I(p)\}$$

is a weighted projective space of dimension $|I(p)|$.

**Proposition 8.** *Assume that* $\mathsf{a}$ *is normalized.*

1. *The decomposition of* $\operatorname{Sing}\mathbb{P}(\mathsf{a})$ *into irreducible components is*

$$\operatorname{Sing}\mathbb{P}(\mathsf{a}) = \bigcup_{p\in\Sigma} S(p).$$

2. *Moreover*

$$\operatorname{Sing}\mathbb{P}(\mathsf{a}) = \{x \in \operatorname{Sing}\mathbb{P}(\mathsf{a}) \,:\, G_x \neq \{1\}\}\,.$$

*Proof.* See Dimca [Di, p. 185]. □

Notice that $\dim \operatorname{Sing}\mathbb{P}(\mathsf{a}) \le m-2$, that is, $\mathbb{P}(\mathsf{a})$ is regular in codimension one, as it already follows from normality.

**Corollary 1.** *Assume that* $\mathsf{a}$ *is normalized.*

1. *If* $(x_0 : \dots : x_m) \in \operatorname{Sing}\mathbb{P}(\mathsf{a})$, *then* $x_i = 0$ *for at least one* $i$.
2. *If*

$$\gcd(a_j, a_j) = 1 \quad \textit{for every couple } (i,j) \textit{ with } j \neq i,$$

*then*

$$\operatorname{Sing}\mathbb{P}(\mathsf{a}) = \{P_0,\dots,P_m\},$$

*where* $P_i$ *are the* $m+1$ *vertices* $(0 : \dots : 1 : \dots : 0)$.

*Proof.* From Proposition 8 we deduce that if $x \in \operatorname{Sing}\mathbb{P}(\mathsf{a})$, then $x \in S(p)$ for some $p \in \Sigma$, hence, $x_i = 0$ for at least one $i$. This proves (1). If $a_0,\dots,a_m$ are pairwise coprime, then $I(p)$ has only one element $i$, and $S(p) = \{P_i\}$. This proves (2). □

## *1.A.3 Affine parts*

### 1.A.3.1 Quotient of the affine space by a cyclic group

We shall define an action of the cyclic group $\boldsymbol{\mu}_{a_i}$ on $\mathbb{A}^m$, which is called *the action of type*

$$\frac{1}{a_i}(a_0,\dots,\widehat{a_i},\dots,a_m).$$

Let $\mathbb{A}^m_{\{i\}}$ the affine hypersurface of $\mathbb{V}$ with equation $X_i = 1$. Our action is defined by

$$\zeta.(x_0,\dots,1,\dots,x_m) = (\zeta^{a_0}x_0,\dots,1,\dots,\zeta^{a_m}x_m), \quad \zeta \in \boldsymbol{\mu}_{a_i},$$

and we get a finite quotient

$$p\colon \mathbb{A}^m_{\{i\}} \longrightarrow \mathbb{A}^m_{\{i\}}/\boldsymbol{\mu}_{a_i}.$$

We have

$$k[\mathbb{A}^m_{\{i\}}] = \mathsf{S}/(X_i - 1) = k[X_0,\dots,\widehat{X_i},\dots,X_m].$$

If

$$k[\mathbb{A}^m_{\{i\}}]^{\mathrm{inv}} = k[\mathbb{A}^m_{\{i\}}/\boldsymbol{\mu}_{a_i}] = k[\mathbb{A}^m_{\{i\}}]^{\boldsymbol{\mu}_{a_i}},$$

then [BR, Lem. 2.5, p. 11]

$$k[\mathbb{A}^m_{\{i\}}]^{\mathrm{inv}} = \bigoplus k[\mathbb{A}^m_{\{i\}}]_{na_i}.$$

If $\gcd(a_j,a_i) = 1$ for $j \neq i$, then the only point $x \in \mathbb{A}^m$ with non-trivial isotropy subgroup is $x = 0$, and the projection $\mathbb{A}^m_{\{i\}} \to \mathbb{A}^m_{\{i\}}/\boldsymbol{\mu}_{a_i}$ is étale outside 0.

### 1.A.3.2 Affine parts

For $0 \leq i \leq m$, we consider the principal open subset

$$V_i = \{x \in \mathbb{V} : x_i \neq 0\}.$$

Then $k[V_i]$ is the localization of $\mathsf{S}$ with respect to $X_i$, namely

$$k[V_i] = k\left[\frac{1}{X_i}\right] = \left\{\frac{f}{X_i^n} : f \in \mathsf{S}\right\} \subset k(\mathbb{A}^{m+1}).$$

We put

$$U_i = p(V_i) = V_i/\mathbb{G}_m = \{x = (x_0 : \dots : x_n) \in \mathbb{P}(\mathsf{a}) : x_i \neq 0\}$$

and we consider the $k$-subalgebra of degree 0 elements of $k[V_i]$:

$$k[V_i]^0 = \left\{ \frac{f}{X_i^n} \in \mathsf{S}_{[i]} \,:\, f \text{ homogeneous},\ n \geq 0,\ \deg f = na_i \right\}. \tag{1.8}$$

Then

$$k[U_i] = k[V_i]^0 = k[V_i]^{\mathbb{G}_m}.$$

**Proposition 9.** *With the preceding notation*:

1. *The projection* $p\colon \mathbb{A}^m_{\{i\}} \to U_i$ *given by*

$$p(x_0,\ldots,1,\ldots,x_m) = (x_0 : \ldots : 1 : \ldots : x_m)$$

*is surjective and induces an isomorphism*

$$\varphi\colon \mathbb{A}^m_{\{i\}}/\boldsymbol{\mu}_{a_i} \xrightarrow{\sim} U_i,$$

*with an inverse*

$$\psi\colon U_i \xrightarrow{\sim} \mathbb{A}^m_{\{i\}}/\boldsymbol{\mu}_{a_i}$$

*such that*

$$\psi(x_0 : \ldots : 1 : \ldots : x_m) = (x_0,\ldots,1,\ldots,x_m).$$

2. *The canonical homomorphism* $p^\flat\colon k[U_i] \to k[\mathbb{A}^m_{\{i\}}]$ *given by*

$$p^\flat\left(\frac{f}{X_i^n}\right) = f(X_0,\ldots,1,\ldots,X_m),$$

*for* $f$ *homogeneous,* $n \geq 0$, $\mathsf{a}\text{-}\deg f = na_i$, *is injective and induces an isomorphism*

$$\varphi^\flat\colon k[U_i] \xrightarrow{\sim} k[\mathbb{A}^m_{\{i\}}]^{\mathrm{inv}},$$

*with an inverse*

$$\psi^\flat\colon k[\mathbb{A}^m_{\{i\}}]^{\mathrm{inv}} \longrightarrow k[U_i]$$

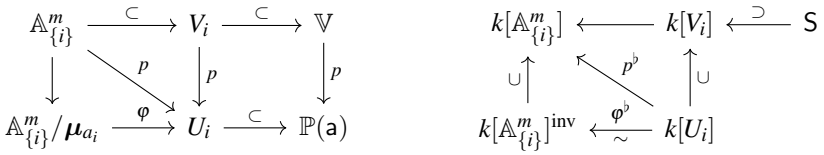
*such that*

$$\psi^\flat(f) = \frac{f}{X_i^n},$$

*for* $f \in k[\mathbb{A}^m_{\{i\}}]^{\mathrm{inv}}$, $\deg f = na_i$. *In particular*

$$\psi^\flat\left(X_j^{a_i}\right) = \frac{X_j^{a_i}}{X_i^{a_j}}.$$

Proposition 9 leads to the two diagrams




*Proof (Proof of proposition 9).*

1. See [BR, Th. 2.6.b, p. 12], [Ho, 1.2.3], and occasionally see also [Te, pp. 63–64] and [Re, pp. 4–5].

2. Let $x$ and $y$ be in $\mathbb{A}^m_{\{i\}}$. If

$$(y_0,\dots,1,\dots,y_m) = (\zeta^{a_0}x_0,\dots,1,\dots,\zeta^{a_m}x_m), \quad \zeta \in \boldsymbol{\mu}_{a_i},$$

then $p(x) = p(y)$, and the existence of $\varphi$ follows. Conversely, assume that $p(y) = p(x)$. Then we have in $\mathbb{V}$, with some $t \in \mathbb{G}_m$:

$$(v_0,\dots,1,\dots,v_m) = (t^{a_0}u_0,\dots,t^{a_i},\dots,t^{a_m}u_m)$$

This implies that $t \in \boldsymbol{\mu}_{a_i}$, hence, $p$ factors modulo $\boldsymbol{\mu}_{a_i}$, and $\varphi$ is injective.

3. Let

$$W_i = \{x = (x_0 : \dots : \xi_i : \dots : x_n) \in \mathbb{P}(a_0,\dots,1,\dots,a_m) \,:\, \xi_i \neq 0\}$$

and consider the morphisms

$$m\colon W_i \longrightarrow U_i$$

given by

$$m(x_0 : \dots : \xi_i : \dots : x_m) = (x_0 : \dots : \xi_i^{a_i} : \dots : x_m)$$

and

$$\psi_0\colon W_i \longrightarrow \mathbb{A}^m_{\{i\}}/\boldsymbol{\mu}_{a_i}$$

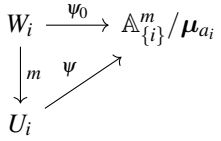
given by

$$\psi_0(x_0 : \dots : \xi_i : \dots : x_m) = (\frac{x_0}{\xi_i^{a_0}},\dots,1,\dots,\frac{x_m}{\xi_i^{a_m}}).$$

If $m(x) = m(y)$, then $\eta_i = t\xi_i$ with $t \in \boldsymbol{\mu}_{a_i}$ and $\psi_0(x) = \psi_0(y)$. Hence, there is a morphism

$$\psi\colon U_i \longrightarrow \mathbb{A}^m_{\{i\}}/\boldsymbol{\mu}_{a_i}$$

such that $\psi_0 = \psi \circ m$:



We have

$$\psi(x_0 : \ldots : 1 : \ldots : x_m) = (x_0, \ldots, 1, \ldots, x_m).$$

This implies $\psi \circ \varphi(x) = x$ if $x \in \mathbb{A}^m_{\{i\}}/\boldsymbol{\mu}_{a_i}$, and $\psi$ is surjective. On the other hand, it is easy to see that $\varphi \circ \psi \circ m(x) = m(x)$ if $x \in W_i$, hence, $\varphi \circ \psi(x) = x$ if $x \in U_i$, and $\varphi$ is surjective.

4. The corresponding homomorphisms of algebras are respectively

$$m^\flat \colon \mathsf{S}_{(i)} = k[U_i] \longrightarrow k[W_i]$$

given by

$$m^\flat(f/X_i^n) = f/\Xi_i^{na_i},$$

for $f$ homogeneous, $n \geq 0$, $\mathsf{a}\text{-deg}\, f = na_i$, and

$$\psi_0^\flat \colon k[\mathbb{A}^m_{\{i\}}]^{\mathrm{inv}} \longrightarrow k[W_i]$$

given by

$$\psi_0^\flat(f) = f/\Xi_i^{na_i},$$

for $f \in \mathsf{R}_{\{i\}}$, $\deg f = na_i$. Now the morphism

$$\psi^\flat \colon k[\mathbb{A}^m_{\{i\}}]^{\mathrm{inv}} \longrightarrow k[U_i]$$

such that

$$\psi^\flat(f) = f/X_i^n,$$

for $f \in k[\mathbb{A}^m_{\{i\}}]^{\mathrm{inv}}$, $\deg f = na_i$, satisfies $\psi_0^\flat = m^\flat \circ \psi^\flat$, and we have a diagram

$$\begin{array}{ccc} k[W_i] & \xleftarrow{\psi_0^\flat} & k[\mathbb{A}^m_{\{i\}}]^{\mathrm{inv}} \\ {\scriptstyle m^\flat}\uparrow & \swarrow_{\psi^\flat} & \\ k[U_i] & & \end{array}$$

□

*Remark 5.* Roughly speaking, we have

$$\psi(x_0 : \ldots : x_i : \ldots : x_m) = \left( \frac{x_0}{x_i^{a_0/a_i}}, \ldots, 1, \ldots, \frac{x_m}{x_i^{a_m/a_i}} \right).$$

This formula obviously makes sense if $a_i = 1$ (see below).

From Proposition 9 we get, see also [Ko, p. 81] and [Do1, Prop. 1.3.3(ii)]:

**Corollary 2.** *The space $\mathbb{P}(\mathsf{a})$ has cyclic quotient singularities.*

Similarly, if $k = \mathbb{R}$, the space $\mathbb{P}(\mathsf{a})$ is an orbifold (or *V-variety*) [Do1, Th. 3.1.6].

### 1.A.3.3 A special case

The complement of the open set $U_i$ is the hyperplane $P_i$ of $\mathbb{P}(\mathsf{a})$ with equation $x_i = 0$. Then $P_i$ is the weighted projective space $\mathbb{P}(\mathsf{a}')$ of dimension $m-1$, with $\mathsf{a}' = (a_0, \ldots, \widehat{a_i}, \ldots, a_m)$, and we have the standard "motivic" decomposition

$$\mathbb{P}(\mathsf{a}) = U_i \sqcup P_i. \tag{1.9}$$

If we assume $\mathsf{a} = (a_0, \ldots, 1, \ldots, a_m)$, with $a_i = 1$, the set $U_i$ is affine, since $k[U_i] = k[Y_1, \ldots, Y_m]$, with

$$Y_1 = \frac{X_0}{X_i^{a_0}}, \quad \ldots, \quad Y_m = \frac{X_m}{X_i^{a_m}}$$

and $U_i$ is isomorphic to $\mathbb{A}^m$. The morphism

$$\varphi \colon \mathbb{A}^m_{\{i\}} \xrightarrow{\sim} U_i,$$

is an isomorphism, with an inverse

$$\psi \colon U_i \xrightarrow{\sim} \mathbb{A}^m_{\{i\}}$$

given by

$$\psi(x_0 : \ldots : x_i : \ldots : x_m) = \left(\frac{x_0}{x_i^{a_0}}, \ldots, 1, \ldots, \frac{x_m}{x_i^{a_m}}\right).$$

Since $U_i$ is isomorphic to $\mathbb{A}^m$, the space $\mathbb{P}(\mathsf{a})$ is a compactification of the affine space $\mathbb{A}^m$.

### 1.A.3.4 Action of $\mathbb{G}_m$

The action

$$\sigma \colon \mathbb{G}_m \times \mathbb{A}^m_{\{i\}} \longrightarrow V_i$$

is given by

$$\sigma(t).(x_0, \ldots, 1, \ldots x_m) = (t^{a_0} x_0, \ldots, t^{a_i}, \ldots, t^{a_m} x_m).$$

Let $x = (x_0, \ldots, x_m)$ and similarly for $x'$. If $\sigma(t').x' = \sigma(t).x$, then $(t')^{a_i} = t^{a_i}$ and $t' = \zeta^{-1} t$ with $\zeta \in \boldsymbol{\mu}_{a_i}$. We thus have $(x'_0, \ldots, x'_m) = (\zeta^{a_0} x_0, \ldots, \zeta^{a_m} x_m)$ and

$$\sigma(t').x' = \sigma(t).x \quad \Longleftrightarrow \quad t' = \zeta^{-1} t \text{ and } x' = \zeta.x, \quad \zeta \in \boldsymbol{\mu}_{a_i}.$$

Hence, the action $\sigma$ factors through

$$(\mathbb{G}_m \times \mathbb{A}^m_{\{i\}})/\boldsymbol{\mu}_{a_i}$$

with the action $\zeta.(t,x) = (\zeta^{-1}t, \zeta.x)$. The canonical homomorphism

$$\sigma^\flat : k[V_i] \longrightarrow k[\mathbb{A}^m_{\{i\}}][T,T^{-1}]$$

is equal, for $f$ a-homogeneous, to

$$\sigma^\flat\left(\frac{f}{X_i^n}\right) = f(X_0,\dots,1,\dots,X_m)\cdot T^{\deg f - na_i}$$

which is injective, with image equal to $k[\mathbb{A}^m_{\{i\}}][T,T^{-1}]^{\boldsymbol{\mu}_{a_i}}$. Then:

**Proposition 10.** *The action $\sigma$ induces isomorphisms*

$$(\mathbb{G}_m \times \mathbb{A}^m_{\{i\}})/\boldsymbol{\mu}_{a_i} \xrightarrow{\sim} V_i, \qquad k[V_i] \xrightarrow{\sim} k[\mathbb{A}^m_{\{i\}}][T,T^{-1}]^{\boldsymbol{\mu}_{a_i}},$$

*and $\sigma$ is an étale morphism.*

*Proof.* See [BR, Th. 2.6.c, p. 12]. □

**Warning.** These isomorphisms are not surjective on the sets of rational points: think of the covering $\mathbb{A}^1 \to \mathbb{A}^1$ given by $z \mapsto z^2$ !

### *1.A.4 Rationality*

Let $k$ be a field. A point $y \in \mathbb{P}(\mathsf{a})$ is rational if and only if $p^{-1}(y)$ is invariant under the Galois group $\Gamma = \mathrm{Gal}(\bar{k}/k)$. We denote as usual the subset of rational points of $\mathbb{P}(\mathsf{a})$ by $\mathbb{P}(\mathsf{a})(k)$. The orbit of $x = (x_0,\dots,x_m) \in \mathbb{V}(\bar{k})$ with image $p(x) = y$ is the rational curve

$$C(x) = p^{-1}(y) = \sigma(\bar{k}^\times).x = \left\{(\lambda^{a_0}x_0,\dots,\lambda^{a_m}x_m) : \lambda \in \bar{k}^\times\right\} \subset \mathbb{V}(\bar{k}).$$

**Lemma 5.** *Let $k$ be any field.*

1. *Let $x \in \mathbb{V}$. Then*

$$p(x) \in \mathbb{P}(\mathsf{a})(k) \iff C(x) \cap \mathbb{V}(k) \neq \emptyset.$$

   *In other words, the map $p : \mathbb{V}(k) \longrightarrow \mathbb{P}(\mathsf{a})(k)$ is surjective.*

2. *The map $p$ induces a bijection $\mathbb{V}(k)/R \xrightarrow{\sim} \mathbb{P}(\mathsf{a})(k)$ where $R$ is the equivalence relation whose classes are the subsets $C(x) \cap \mathbb{V}(k)$.*

*Proof.* It is sufficient to prove the first assertion. See [Pe, Lem. 6] and [Go, Lemma 1.2]. □

**Lemma 6.** *Assume $k = \mathbb{F}_q$. Recall that $p$ is prime to all $a_i$.*

1. *If $x \in \mathbb{V}(k)$, then $\big|C(x) \cap \mathbb{V}(\mathbb{F}_q)\big| = \sigma(k^\times).x$ and*

$$\big|C(x) \cap \mathbb{V}(\mathbb{F}_q)\big| = q - 1.$$

2. *The map $p$ induces a bijection*

$$\mathbb{V}(k)/\sigma(k^\times) \xrightarrow{\sim} \mathbb{P}(\mathsf{a})(k)$$

3. *We have*

$$\big|\mathbb{P}(\mathsf{a})(\mathbb{F}_q)\big| = \pi_m, \quad \textit{with} \quad \pi_m = \big|\mathbb{P}^m(\mathbb{F}_q)\big| = \frac{q^{m+1}-1}{q-1}.$$

*Proof.* (1): See Goto [Go, Prop. 1.3] and Perret [Pe, Lem. 7]. Then (2) follows from (1) and Lemma 5(2), whereas (3) follows from (2). □

**Corollary 3.** *Let $X$ be a hypersurface in a weighted projective space of dimension $m$ over $\mathbb{F}_q$. Write $\big|X(\mathbb{F}_q)\big|$ for the number of $\mathbb{F}_q$-rational points on $X$ and $\big|(\mathrm{Cone}X)(\mathbb{F}_q)\big|$ for the number of affine solutions for the defining equation of $X$ in $\mathbb{A}^{m+1}$. Then*

$$\big|(\mathrm{Cone}X)(\mathbb{F}_q)\big| = (q-1)\big|X(\mathbb{F}_q)\big| + 1.$$

*Proof.* See [Go, Cor. 1.4]. □

If $X$ is a hypersurface of degree $d$ over $\mathbb{F}_q$ in $\mathbb{P}^m$ with $m \geq 1$, then Serre's inequality is

$$\big|X(\mathbb{F}_q)\big| \leq dq^{m-1} + \pi_{m-2}$$

(recall that $\pi_{m-2} = 0$), and hence,

$$\big|(\mathrm{Cone}X)(\mathbb{F}_q)\big| \leq dq^m - (d-1)q^{m-1}.$$

The following result is a bit amazing:

**Corollary 4.** *Let $\mathbb{A}^m_{\{i\}}$ the affine hypersurface of $\mathbb{V}$ with equation $X_i = 1$, and*

$$p\colon \mathbb{A}^m_{\{i\}} \longrightarrow \mathbb{A}^m_{\{i\}}/\boldsymbol{\mu}_{a_i}$$

*the quotient map under the action of type*

$$\frac{1}{a_i}(a_0, \ldots, \widehat{a_i}, \ldots, a_m).$$

*Let $Z_i$ be the scheme $\mathbb{A}^m_{\{i\}}/\boldsymbol{\mu}_{a_i}$. Then*

$$\big|Z_i(\mathbb{F}_q)\big| = q^m.$$

*Proof.* This is a consequence of (1.9) and of Lemma 6(3). □

To be less amazed, observe that if $q$ is odd and $Z = \mathbb{A}^1/\boldsymbol{\mu}_2$, then $\left|Z(\mathbb{F}_q)\right| = q$.

## *1.A.5 Weighted forms*

### 1.A.5.1 Definition

Since the natural homomorphism $\pi^*$ defines an isomorphism

$$\mathscr{O}_{\mathbb{P}(\mathsf{a})}(U) \xrightarrow{\sim} \pi_*(\mathscr{O}_{\mathbb{P}^m})^G(U) = \mathscr{O}_{\mathbb{P}^m}(\pi^{-1}(U))^G,$$

for any open set $U \subset \mathbb{P}(\mathsf{a})$, we have a homomorphism of graded rings

$$\pi^\flat \colon k[X_0,\dots,X_m] \longrightarrow k[X_0^{a_0},\dots,X_m^{a_m}]$$

such that $\pi^\flat(X_i) = X_i^{a_i}$. This leads to the isomorphism

$$S(\mathsf{a}) \xrightarrow{\sim} k[X_0^{a_0},\dots,X_m^{a_m}] = k[X_0,\dots,X_m]^G,$$

see [Do1, p. 37] and [Ho, Lemma 4.2.1].

Henceforth we write $X = (X_0,\dots,X_m)$ and denote by $k[X]$ the algebra of polynomials in $(X_0,\dots,X_m)$. A polynomial $f \in k[X]$ is *quasi-homogeneous* (or *weighted homogeneous*, or a *weighted form*) of $\mathsf{a}$-degree $d$ (or of degree $d$ w.r.t. $\mathsf{a}$) if

$$f(\lambda^{a_0}X_0,\dots,\lambda^{a_m}X_m) = \lambda^d(X_0,\dots,X_m).$$

We denote by $k[X]_d$ the vector space of homogeneous polynomials of degree $d$, and by $k^{\mathsf{a}}[X]_d$ the vector space of quasi-homogeneous polynomials of $\mathsf{a}$-degree $d$. Now

$$f \in k^{\mathsf{a}}[X]_d \quad \Longrightarrow \quad \pi^* f \in k[X]_d.$$

For a monomial $m = X_0^{r_0}\dots X_m^{r_m}$, we have

$$m(\lambda^{a_0}X_0,\dots,\lambda^{a_m}X_m) = \lambda^{a_0r_0}X_0^{r_0}\dots\lambda^{a_mr_m}X_m^{r_m}$$

hence, $m \in k^{\mathsf{a}}[X]_d$ with

$$a_0r_0 + \dots + a_mr_m = d,$$

and the dimension of $k^{\mathsf{a}}[X_0,\dots,X_m]_d$ is equal to

$$\{(r_0,\dots,r_m) \in \mathbb{N}^m \,:\, a_0r_0 + \dots + a_mr_m = d\}.$$

This number can be calculated with the help of Ehrhart polynomials (see [Be]).

Every $f \in k^{\mathsf{a}}[X]_d$ defines a hypersurface

$$Y = Y_f = \{(x_0 : \ldots : x_m) \in \mathbb{P}(\mathsf{a}) \,:\, f(x_0,\ldots,x_m) = 0\},$$

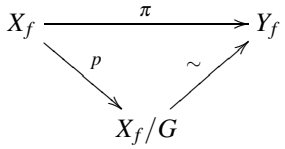
and we associate also to $f$ the projective hypersurface of degree $d$:

$$X = X_f = \{(x_0 : \ldots : x_m) \in \mathbb{P}^m \,:\, \pi^* f(x_0,\ldots,x_m) = 0\},$$

and the morphism $\pi\colon \mathbb{P}^m \longrightarrow \mathbb{P}(\mathsf{a})$ induces a morphism

$$\pi\colon X_f \longrightarrow Y_f$$

providing a diagram




and the morphism $\pi$ enjoys the properties of Proposition 6.

### 1.A.5.2 Weighted binary forms

Let $\mathsf{a} = (a_0, a_1)$ and assume $a_1 > 1$. We work with the weighted projective line $\mathbb{P}(a_0, a_1)$. It is known that $\mathbb{P}(a_0, a_1) \simeq \mathbb{P}^1$, see [Do1, p. 38]. If $P_0 = (0 : 1)$ then $\mathbb{P}(a_0, a_1) = D_0 \cup \{P_0\}$.

**Proposition 11 (D'Alembert's theorem for weighted binary forms).** *Let* $\mathsf{a} = (1, a_1)$. *Let* $f \in k[X_0, X_1]$ *be a binary weighted form with weighted degree d, where* $a_1 \mid d$. *Then the finite set*

$$X_f = \{(x_0, x_1) \in \mathbb{P}(1, a_1) \,:\, f(x_0, x_1) = 0\}$$

*satisfies*

$$\left|X_f\right| \leq \frac{d}{a_1}.$$

*Proof.* Let $\mathsf{a} = (a_0, a_1)$, and assume $a_0 a_1 \mid d$. We have

$$f(x_0, x_1) = \sum_{r_0, r_1} c_{r_0, r_1} x_0^{r_0} x_1^{r_1} \quad (a_0 r_0 + a_1 r_1 = d)$$

and in decreasing powers of $x_1$:

$$f(x_0, x_1) = c_{0, d/a_1} x_1^{d/a_1} + \cdots + c_{r_0, r_1} x_0^{r_0} x_1^{r_1} + \cdots + c_{d/a_0, 0} x_0^{d/a_0}.$$

Notice that $a_0$ divides every index $r_1$. If $x_0 = 0$ the equation reduces to

$$c_{0, d/a_1} x_1^{d/a_1} = 0$$

and the equation has exactly one solution if $c_{0,d/a_1} = 0$, namely $P_0$, and none otherwise. In $D_0$, we have as well

$$\begin{aligned}\frac{f(x_0,x_1)}{x_0^{d/a_0}} &= c_{0,d/a_1}\frac{x_1^{d/a_1}}{x_0^{d/a_0}} + \cdots + c_{r_0,r_1}\frac{x_1^{r_1}}{x_0^{a_1 r_1/a_0}} + \cdots + c_{d/a_0,0} \\ &= c_{0,d/a_1}\left(\frac{x_1^{a_0}}{x_0^{a_1}}\right)^{d/a_0 a_1} + \cdots + c_{r_0,r_1}\left(\frac{x_1^{a_0}}{x_0^{a_1}}\right)^{r_1/a_0} + \cdots + c_{d/a_0,0} \\ &= f_0(u),\end{aligned}$$

with $u = x_1^{a_0}/x_0^{a_1}$, and

$$f_0(u) = c_{0,d/a_1}u^{d/a_0a_1} + \cdots + c_{r_0,r_1}u^{r_1/a_0} + \cdots + c_{d/a_0,0}.$$

This is a polynomial of degree $\leq d/a_0a_1$ with strict inequality if $c_{0,d/a_1} = 0$. If $\mathsf{a} = (1,a_1)$, the morphism $\varphi\colon U_0 \to \mathbb{A}^1$ given by

$$\varphi(x_0 : x_1) = u = \frac{x_1}{x_0^{a_1}}$$

is an isomorphism, with inverse morphism given by $u \mapsto (1 : u)$, and $\left|X_f\right| \leq d/a_1$. □

### 1.A.5.3 Weighted ternary forms

We are interested on weighted projective plane curves in the weighted projective plane $\mathbb{P}(1,a_1,a_2)$, that is, $m = 2$ and $\mathsf{a} = (1,a_1,a_2)$. We assume $1 < a_1 < a_2$. Recall the notation: the morphism

$$\psi\colon U_0 \longrightarrow \mathbb{A}_0^2$$

$$\psi(x_0 : x_1 : x_2) = (1, y_1, y_2),$$

where

$$y_1 = \frac{x_1}{x_0^{a_1}}, \quad y_2 = \frac{x_2}{x_0^{a_2}},$$

corresponds to the morphism of algebras

$$\psi^\flat\colon k[X_0,X_1,X_2] \longrightarrow k[Y_1,Y_2]$$

where

$$Y_1 = \frac{X_1}{X_0^{a_1}}, \quad Y_2 = \frac{X_2}{X_0^{a_2}}.$$

The morphism $\psi$ is an isomorphism, with inverse $\varphi\colon \mathbb{A}_0^2 \to U_0$ given by

$$\psi(1, y_1, y_2) = (1 : y_1 : y_2).$$

The complement of $U_0$ is the weighted projective line $\mathbb{P}(a_1,a_2)$, and $\mathbb{P}(1,a_1,a_2)$ is a compactification of the affine plane.

Recall that Ore's inequality (1922) for forms is the following: Let $f$ be a form in $m+1$ variables, of degree $d$, defined over $\mathbb{F}_q$. Define

$$X_f = \{x \in \mathbb{P}^m : f(x) = 0\},$$

and $(X_f)^{\text{aff}} = X_f \cap U_0$. Then

$$\left|(X_f)^{\text{aff}}(\mathbb{F}_q)\right| \leq dq^{n-1}.$$

**Proposition 12.** *Let* $\mathsf{a} = (1,a_1,a_2)$ *and* $f \in k[X_0,X_1,X_2]$ *a ternary weighted form with weighted degree* $d$*, where* $a_1a_2 \mid d$*. Define*

$$X_f = \{(x_0,x_1,x_2) \in \mathbb{P}(1,a_1,a_2) : f(x_0,x_1,x_2) = 0\}.$$

1. (*Ore's inequality for weighted ternary forms*). *Let* $(X_f)^{\text{aff}} = X_f \cap U_0$*. Then*

$$\left|(X_f)^{\text{aff}}(\mathbb{F}_q)\right| \leq \frac{d}{a_1}q.$$

2. *We have*

$$\left|X_f(\mathbb{F}_q)\right| \leq \frac{d}{a_1}q + 1.$$

*Proof.* Proof of (1): we write

$$f(X_0,X_1,X_2) = \sum c_i X_0^{p_i} X_1^{q_i} X_2^{r_i}, \quad p_i + a_1q_i + a_2r_i = d.$$

The general term of $f/X_0^d$ is

$$\frac{X_0^{p_i}X_1^{q_i}X_2^{r_i}}{X_0^{p_i+a_1q_i+a_2r_i}} = \frac{X_1^{q_i}}{X_0^{a_1q_i}} \cdot \frac{X_2^{r_i}}{X_0^{a_2r_i}} = Y_1^{q_i}Y_2^{r_i}.$$

If $p_1 = r_1 = 0$, then $q_1 = d/a_2$, if $p_2 = q_2 = 0$, then $q_2 = d/a_2$, and if $q_0 = r_0 = 0$, then $p_0 = d$. Hence,

$$f(X_0,X_1,X_2) = c_1X_1^{d/a_1} + c_2X_2^{d/a_2} + \cdots + c_0X_0^d,$$

and

$$\frac{f(X_0,X_1,X_2)}{X_0^d} = c_1Y_1^{d/a_1} + c_2Y_2^{d/a_2} + \cdots + Y_1^{q_i}Y_2^{r_i} + \cdots + c_0.$$

This is a bivariate polynomial of degree $\leq d/a_1$ in $\mathbb{A}^2$. We get the result using the usual Ore inequality. For a proof of (2), see Theorem 1 in the main text. □

## References


Be. M. Beck, J. A. De Loera, M. Develin, J. Pfeifle, and R. P. Stanley, *Coefficients and roots of Ehrhart polynomials*, Integer points in polyhedra — Geometry, number theory, algebra, optimization (A. Barvinok, M. Beck, C. Haase, B. Reznick, and V. Welker, eds.), Contemporary Mathematics, vol. 374, American Mathematical Society, Providence, RI, 2005, pp. 15–36.

BR. Mauro Beltrametti and Lorenzo Robbiano, *Introduction to the theory of weighted projective spaces*, Exposition. Math. **4** (1986), no. 2, 111–162.

Di. Alexandru Dimca, *Singularities and coverings of weighted complete intersections*, J. Reine Angew. Math. **366** (1986), 184–193.

Do1. Igor Dolgachev, *Weighted projective varieties*, Group actions and vector fields (Vancouver, B.C., 1981) (J. B. Carrell, ed.), Lecture Notes in Mathematics, vol. 956, Springer, Berlin, 1982, pp. 34–71.

Do2. ———, *Lectures on invariant theory*, London Mathematical Society Lecture Note Series, vol. 296, Cambridge University Press, Cambridge, 2003.

Go. Yasuhiro Goto, *Arithmetic of weighted diagonal surfaces over finite fields*, J. Number Theory **59** (1996), no. 1, 37–81.

Gr. Alexander Grothendieck, *Revêtements étales et groupe fondamental. Fasc. I: Exposés 1 à 5*, Séminaire de Géométrie Algébrique, vol. 1960/61, Institut des Hautes Études Scientifiques, Paris, 1963.

Ho. Timothy Hosgood, *An introduction to varieties in weighted projective space*, https://thosgood.github.io/pdfs/general/introduction-to-wps.pdf, 2015.

Ko. János Kollár, *Lectures on resolution of singularities*, Annals of Mathematics Studies, vol. 166, Princeton University Press, Princeton, NJ, 2007.

MFK. D. Mumford, J. Fogarty, and F. Kirwan, *Geometric invariant theory*, third ed., Ergebnisse der Mathematik und ihrer Grenzgebiete (2), vol. 34, Springer-Verlag, Berlin, 1994.

Pe. Marc Perret, *On the number of points of some varieties over finite fields*, Bull. London Math. Soc. **35** (2003), no. 3, 309–320.

Re. Miles Reid, *Graded rings and varieties in weighted projective space*, http://homepages.warwick.ac.uk/~masda/surf/more/grad.pdf, 2002.

Se. Jean-Pierre Serre, *Algebraic groups and class fields*, Graduate Texts in Mathematics, vol. 117, Springer-Verlag, New York, 1988.

Te. Jenia Tevelev, *Introduction to invariant theory and moduli spaces*, http://people.math.umass.edu/~tevelev/moduli797.html, undated.