Available online at www.sciencedirect.com

ScienceDirect

ELSEVIER

Journal of Combinatorial Theory, Series A 115 (2008) 547–568

Journal of Combinatorial Theory Series A

www.elsevier.com/locate/jcta

Orbits of rational n-sets of projective spaces under the action of the linear group

Ricard Martí, Enric Nart [1,2]

Universitat Autònoma de Barcelona, Departament de Matemàtiques, 08193 Bellaterra, Barcelona, Spain

Received 19 January 2007

Available online 6 September 2007

Communicated by Bernd Sturmfels

Abstract

Let $k = \mathbb{F}_q$ be a finite field. We enumerate k-rational n-sets of (unordered) points in a projective space $\mathbb{P}^N$ over k, and we compute the generating function for the numbers of $\mathrm{PGL}_{N+1}(k)$-orbits of these n-sets. For $N = 1, 2$ we obtain a formula for these numbers of orbits as a polynomial in q with integer coefficients.
© 2007 Elsevier Inc. All rights reserved.

Keywords: Finite field; Rational n-set; Projective space; Projective linear group; Generating function; Zeta function; Finite poset

0. Introduction

Deep properties of geometric objects often rely on combinatorial properties of unordered structures. For example, at the beginning of the last century Coble and others studied geometric structures related to n-sets of points in projective spaces. A revision of this work in modern language can be found in the book [4] of Dolgachev and Ortland.

From an arithmetic perspective we are led to consider n-sets that are rational over the ground field k we are interested in. Let $\bar{k}$ be an algebraic closure of the field k; an n-set $S = \{P_1, \dots, P_n\}$

E-mail address: nart@mat.uab.cat (E. Nart).

[1] Fax: +34 935812790.

[2] Supported by the project MTM2006-11391 from the Spanish MEC.

0097-3165/$ – see front matter © 2007 Elsevier Inc. All rights reserved.
doi:10.1016/j.jcta.2007.08.002

of a projective space $\mathbb{P}^N(\bar{k})$ is *rational* if S is invariant under the action of the absolute Galois group $\mathrm{Gal}(\bar{k}/k)$, i.e.

$$\{\sigma(P_1),\dots,\sigma(P_n)\} = \{P_1,\dots,P_n\}, \quad \forall\sigma\in\mathrm{Gal}(\bar{k}/k).$$

We denote by $\binom{\mathbb{P}^N}{n}(k)$ the set of all k-rational n-sets. Similarly, $\left(\!\binom{\mathbb{P}^N}{n}\!\right)(k)$ denotes the set of all k-rational n-multisets of $\mathbb{P}^N(\bar{k})$. We have a natural action of $\mathrm{PGL}_{N+1}(k)$ on each of these sets.

In this paper we count the number of $\mathrm{PGL}_{N+1}(k)$-orbits of rational n-sets and multisets for k a finite field, giving closed formulas for the numbers:

$$t_N(n) := \left|\mathrm{PGL}_{N+1}(k)\Big\backslash\binom{\mathbb{P}^N}{n}(k)\right|, \qquad \bar{t}_N(n) := \left|\mathrm{PGL}_{N+1}(k)\Big\backslash\left(\!\!\binom{\mathbb{P}^N}{n}\!\!\right)(k)\right|.$$

There is an extensive literature on the enumeration of orbits of *pointwise rational* n-sets; that is, n-sets $S=\{P_1,\dots,P_n\}$ such that $P_i\in\mathbb{P}^N(k)$ for all i. This is due to the fact that these orbits are in bijective correspondence with isometry classes of certain linear codes [2,5,7,9,10]. However, to our knowledge, the enumeration of rational n-sets has been considered so far only in dimension 1; for instance in [8], where the numbers $t_1(n)$ were computed.

Let us illustrate the role of global (not pointwise) rationality with an example. A hyperelliptic curve over a field of zero or odd characteristic is a double cover of $\mathbb{P}^1$ determined by a Weierstrass equation $y^2=f(x)$, with $f(x)\in k[x]$ an arbitrary separable polynomial. The ramification locus is the rational n-set of the roots of $f(x)$ in $\bar{k}$, together with ∞ if the degree of $f(x)$ is odd. Through this association, pointwise rational n-sets of $\mathbb{P}^1$ correspond only to curves with $f(x)$ splitting completely over the field k. On the other hand, it is easy to check that rational n-sets in the same $\mathrm{PGL}_2(k)$-orbit determine k-isomorphic curves, up to hyperelliptic twist. Thus, the numbers $t_1(n)$ count k-isomorphism classes of hyperelliptic curves defined over k, up to hyperelliptic twist [8].

There are also interesting examples in higher dimension. Over any field of characteristic zero, the PGL_3-orbits of 5-sets of $\mathbb{P}^2$ classify nodal genus 5 planar curves; also, the PGL_3-orbits of 7-sets of $\mathbb{P}^2$ such that no three points lie on a line and no six points lie on a conic classify non-hyperelliptic curves of genus three with a distinguished Aronhold set of bitangents [6, Section 7]. These examples show that our enumeration results may have applications beyond the scope of the geometry of varieties over a finite field k. They might be helpful to compute the number of k-rational points of the variety, or scheme, or algebraic stack $\mathcal{M}\otimes_{\mathbb{Z}}k$, for the moduli spaces $\mathcal{M}$ of some geometric structures. It is well known that from these computations one gains cohomological information on these moduli spaces (see [1] and the references quoted there).

Our main result is the computation of the generating function of $t_N(n)$ and $\bar{t}_N(n)$ for fixed N (Theorem 3.4). The generating function of the number of orbits of pointwise rational n-sets of $\mathbb{P}^N(k)$ can be expressed in terms of the cycle index of Pólya [2, 3.2.16]. This cycle index is a multivariate polynomial that carries all information about the lengths of the cycles of all elements of $\mathrm{PGL}_{N+1}(k)$ acting as permutations of $\mathbb{P}^N(k)$. Thus, this instrument is not able to have full control on rational n-sets, made of points in $\mathbb{P}^N(\bar{k})$. We define a multivariate polynomial analogous to the cycle index, called the *G-exponent index* (G stands for "Galois")

$$\mathrm{E}_G(\mathrm{PGL}_{N+1},\mathbb{P}^N) := \sum_{\alpha\in\mathcal{S}} c_\alpha \prod_{V\in\mathcal{P}(\alpha)} z_{\alpha,V} \in \mathbb{Q}\big[\{z_{\alpha,V}\}\big],$$

where $\mathcal{S}$ is a partition of the set of conjugacy classes of $\mathrm{PGL}_{N+1}(k)$ into a disjoint union of *subtypes*, and to each subtype $\alpha\in\mathcal{S}$ we associate a coefficient $c_\alpha\in\mathbb{Q}$ and a finite poset $\mathcal{P}(\alpha)$

of Galois orbits of certain linear subvarieties of $\mathbb{P}^N(\bar{k})$. The G-exponent index yields the generating function of the $t_N(n)$ when evaluated at series $h_{\alpha,V}(x)$ corresponding to the nodes of these posets:

$$\sum_{n\in\mathbb{N}} t_N(n)x^n = \mathrm{E}_G\bigl(\mathrm{PGL}_{N+1},\mathbb{P}^N\bigr)\bigl(h_{\alpha,V}(x)\bigr). \tag{1}$$

There is a similar expression for the generating function of the numbers $\bar{t}_N(n)$.

The paper is organized as follows. In Section 1, we compute the number $a_V(n)$ of rational n-sets of a quasiprojective variety V over a finite field k. Viewed in a geometric way, we count rational points on the variety $\binom{V}{n}$, the moduli space of n unordered points in V. The generating function of these numbers is easily expressed in terms of the zeta function of V (Theorem 1.2). For certain varieties V we translate this general result into explicit formulas for $a_V(n)$ as a polynomial in $q = |k|$ with integer coefficients. In Section 2, we prove that the quotient of $\mathbb{P}^N$ by a cyclic subgroup of $\mathrm{PGL}_{N+1}(k)$ has the same zeta function as $\mathbb{P}^N$ (Theorem 2.1). In Section 3 we define the subtypes, we construct the posets $\mathcal{P}(\alpha)$ associated to each subtype, and we prove the main theorem taking for granted the basic properties of $\mathcal{P}(\alpha)$, whose proof is postponed to Section 5, where we study the structure of the poset $\mathcal{P}(\alpha)$ in more detail. In Section 4, we restrict our attention to the cases $N = 1, 2$, and we carry out an explicit computation of all the ingredients of (1) in terms of combinatorial data independent of the group structure of $\mathrm{PGL}_{N+1}(k)$ and the action of its elements as permutations of $\mathbb{P}^N(\bar{k})$. This allows one to obtain explicit expressions for the numbers $t_N(n)$, $\bar{t}_N(n)$ as polynomials in q with integer coefficients.

0.1. *Conventions and notation*

Throughout the paper we fix a finite field $k = \mathbb{F}_q$ of characteristic p, with $|k| = q$ and with algebraic closure $\bar{k}$. For any integer $d \geqslant 1$, $k_d = \mathbb{F}_{q^d}$ denotes the unique extension of k of degree d in $\bar{k}$. Finally, φ denotes Euler's totient function and $\sigma \in \mathrm{Gal}(\bar{k}/k)$ denotes the q-Frobenius automorphism of $\bar{k}$, given by $\sigma(x) = x^q$.

1. Rational *n*-sets of quasiprojective varieties

Let V be a quasiprojective variety defined over k. We define the *variety of n-multisets of V* to be the symmetric product of V with itself n times, denoted

$$\left(\!\!\binom{V}{n}\!\!\right) := (V \underbrace{\times \cdots \times}_{n} V)/\mathfrak{S}_n,$$

where $\mathfrak{S}_n$ is the symmetric group. We define the *variety of n-sets of V* to be the open subvariety $\binom{V}{n} \subseteq \left(\!\binom{V}{n}\!\right)$ formed by the unordered n-tuples of points of V without repetitions. The sets of k-rational points of these varieties are denoted

$$\binom{V}{n}(k), \qquad \left(\!\!\binom{V}{n}\!\!\right)(k),$$

and the k-rational points are respectively called *k-rational n-sets* and *k-rational n-multisets* of V. Thus, a rational n-set of V is just an unordered family $S = \{t_1, \ldots, t_n\}$ of n different points of $V(\bar{k})$ which is globally invariant under the Galois action, i.e. $S = S^\sigma$.

In this section we compute the number of rational n-sets and n-multisets of V

$$a_V(n) := \left|\binom{V}{n}(k)\right|, \qquad \bar{a}_V(n) := \left|\left(\!\!\binom{V}{n}\!\!\right)(k)\right|,$$

in terms of the zeta function of V. By convention, $a_V(0) = 1 = \bar{a}_V(0)$.

Definition 1.1. For any $P \in V(\bar{k})$, we denote by $O_\sigma(P)$ the orbit of P under the action of $\mathrm{Gal}(\bar{k}/k)$. We call $O_\sigma(P)$ the *σ-orbit* of P, and we define the *degree* of P to be $\deg(P) := |O_\sigma(P)|$.

If we think a k-rational n-set or n-multiset of V as a disjoint union of σ-orbits of different length we can express $a_V(n)$, $\bar{a}_V(n)$ in terms of the numbers of σ-orbits of points of $V(\bar{k})$ of a given degree:

$$a_d := \left|\left\{O_\sigma(P) \mid \deg(P) = d\right\}\right| = \frac{1}{d}\left|\left\{P \in V(\bar{k}) \mid \deg(P) = d\right\}\right|,$$

$$a_V(n) = \sum_{s_1+2s_2+\cdots+ns_n=n} \binom{a_1}{s_1}\binom{a_2}{s_2}\cdots\binom{a_n}{s_n},$$

$$\bar{a}_V(n) = \sum_{s_1+2s_2+\cdots+ns_n=n} \left(\!\!\binom{a_1}{s_1}\!\!\right)\left(\!\!\binom{a_2}{s_2}\!\!\right)\cdots\left(\!\!\binom{a_n}{s_n}\!\!\right),$$

where s_i is the number of σ-orbits of degree i in each n-set or n-multiset, and we understand that $\binom{a_i}{s_i} = 0$ if $s_i > a_i$. These expressions yield a computation of the generating function of the numbers $a_V(n), \bar{a}_V(n)$:

$$f_V(x) := f_{V/k}(x) := \sum_{n\geqslant 0} a_V(n)x^n = \prod_{d\geqslant 1}\left(1 + x^d\right)^{a_d},$$

$$\bar{f}_V(x) := \bar{f}_{V/k}(x) := \sum_{n\geqslant 0} \bar{a}_V(n)x^n = \prod_{d\geqslant 1}\left(1 - x^d\right)^{-a_d}. \tag{2}$$

We recognize in the last expression the zeta function of V over k:

$$\mathrm{Z}(V,t) := \mathrm{Z}(V/k,t) := \exp\left(\sum_{d\geqslant 1}\frac{1}{d}\left|V(k_d)\right|t^d\right) = \prod_{d\geqslant 1}\left(1 - t^d\right)^{-a_d}.$$

In $f_V(x)$, $\bar{f}_V(x)$ and $\mathrm{Z}(V,t)$ we suppress the appearance of the ground field k when it is clear from context. Hence, we deduce from (2) the main result of this section.

Theorem 1.2. *Let V be a quasiprojective variety V over k. Then*:

$$f_V(x) = \mathrm{Z}(V,x)/\mathrm{Z}\left(V,x^2\right), \qquad \bar{f}_V(x) = \mathrm{Z}(V,x).$$

In the rest of the section, we apply this theorem to obtain explicit formulas for $a_V(n)$ for several varieties V. We are especially interested in the open subvarieties $V \subseteq \mathbb{P}^2$ that are the complement of the union of all linear subvarieties that are invariant under the action of a fixed k-automorphism of $\mathbb{P}^2$. In all cases our formulas express $a_V(n)$ as a polynomial in q with integer coefficients. These computations will be used in Section 4 to obtain explicit formulas for the numbers $t_2(n)$ of $\mathrm{PGL}_3(k)$-orbits of rational n-sets of $\mathbb{P}^2$.

We shall extensively use the fact that $f_V(x)$, $\bar{f}_V(x)$ are multiplicative with respect to disjoint unions, which is an immediate consequence of (2).

Lemma 1.3. *Let V be a quasiprojective variety over k. Let $W \subseteq V$ be any subvariety which is also defined over k, and let $U = V \setminus W$ be the complementary subvariety. Then $f_V(x) = f_W(x) f_U(x)$, $\bar{f}_V(x) = \bar{f}_W(x)\bar{f}_U(x)$.*

1.1. Explicit formulas for $a_V(n)$: subvarieties of $\mathbb{A}^N$

Since $\mathrm{Z}(\mathbb{A}^N, t) = (1 - q^N t)^{-1}$, we get immediately from Theorem 1.2:

$$f_{\mathbb{A}^N}(x) = \frac{1 - q^N x^2}{1 - q^N x} = \left(1 - q^N x^2\right) \sum_{n \geqslant 0} q^{Nn} x^n = 1 + q^N x + \left(1 - q^{-N}\right) \sum_{n \geqslant 2} q^{Nn} x^n.$$

Proposition 1.4. *For all $N \geqslant 0$, $n \geqslant 1$,*

$$a_{\mathbb{A}^N}(n) = \begin{cases} q^N, & \text{if } n = 1, \\ q^{(n-1)N}(q^N - 1), & \text{if } n \geqslant 2. \end{cases}$$

The formula for $a_{\mathbb{A}^1}(n)$ is well known (it counts the number of monic separable polynomials of degree n with coefficients in $\mathbb{F}_q$). To our knowledge, the formula for $a_{\mathbb{A}^N}(n)$, $N > 1$, is new.

If $S(1) \subseteq \mathbb{A}^N$ is the 1-set formed by a k-rational point and $L, L' \subseteq \mathbb{A}^2$ are two intersecting lines, we get by Lemma 1.3:

$$f_{\mathbb{A}^N \setminus S(1)}(x) = \frac{f_{\mathbb{A}^N}(x)}{1 + x}, \qquad f_{\mathbb{A}^2 \setminus L}(x) = \frac{f_{\mathbb{A}^2}(x)}{f_{\mathbb{A}^1}(x)}, \qquad f_{\mathbb{A}^2 \setminus (L \cup L')}(x) = \frac{f_{\mathbb{A}^2}(x)(1 + x)}{f_{\mathbb{A}^1}(x)^2},$$

since $f_{S(1)}(x) = 1 + x$, $f_L(x) = f_{\mathbb{A}^1}(x)$ and $f_{L \cup L'} = f_{\mathbb{A}^1}(x)^2 / f_{S(1)}(x)$. Expanding these rational functions as series, we obtain the following proposition.

Proposition 1.5. *For all $n \geqslant 1$,*

$$a_{\mathbb{A}^N \setminus S(1)}(n) = \left(q^N - 1\right) \frac{q^{nN} - (-1)^n}{q^N + 1}, \quad \forall N \geqslant 1.$$

$$a_{\mathbb{A}^2 \setminus L}(n) = \frac{q - 1}{q^2 + q + 1}\left(q^{2n+1} + q^{2n} - (-1)^n q^{\lceil (n+1)/2 \rceil} - \frac{1}{2}\left(1 + (-1)^n\right) q^{\lceil n/2 \rceil}\right).$$

Moreover, for n even

$$a_{\mathbb{A}^2 \setminus (L \cup L')}(n) = \frac{q^4 - 1}{(q^2 + q + 1)^2}\left(q^{2n} - q^{n/2}\left(\frac{n}{2} \frac{(q^3 - 1)(q - 1)}{q^4 - 1} + 1\right)\right),$$

whereas for n odd, the value of $a_{\mathbb{A}^2 \setminus (L \cup L')}(n)$ is:

$$\frac{q^4 - 1}{(q^2 + q + 1)^2}\left(q^{2n} + q^{(n-1)/2}\left(\frac{n-1}{2} \frac{q^3 - 1}{q^2 + 1} - \frac{(q - 1)(2q^2 + q + 1)}{q^4 - 1}\right)\right).$$

1.2. Explicit formulas for $a_V(n)$: subvarieties of $\mathbb{P}^N$

By the usual stratification $\mathbb{P}^N = \mathbb{A}^0 \cup \mathbb{A}^1 \cup \cdots \cup \mathbb{A}^N$, Lemma 1.3 shows that:

$$f_{\mathbb{P}^N}(x) = \frac{(1-x^2)(1-qx^2)\cdots(1-q^N x^2)}{(1-x)(1-qx)\cdots(1-q^N x)}. \tag{3}$$

We easily deduce from this formula the following closed expressions.

Proposition 1.6. *For all $n \geqslant 1$,*

$$a_{\mathbb{P}^1}(n) = \begin{cases} q+1, & \text{if } n=1,\\ q^2, & \text{if } n=2,\\ q^{n-2}(q^2-1), & \text{if } n \geqslant 3, \end{cases}$$

$$a_{\mathbb{P}^2}(n) = \begin{cases} q^2+q+1, & \text{if } n=1,\\ q^4+q^3+q^2, & \text{if } n=2,\\ q^6+q^5+q^4-q^2-q, & \text{if } n=3,\\ q^{2n-6}(q^4-1)(q^2+q+1), & \text{if } n \geqslant 4. \end{cases}$$

In order to obtain a general expression for $a_{\mathbb{P}^N}(n)$ we write (3) in the form

$$f_{\mathbb{P}^N}(x) = \frac{(x^2;q)_N}{(x;q)_N}, \quad (x;q)_N := (1-x)(1-qx)\cdots\bigl(1-q^N x\bigr).$$

We can derive from [12, 1.3.17] the following identities:

$$\frac{1}{(x;q)_N} = \sum_{n\geqslant 0} \binom{N+n}{n}_q x^n, \quad (x;q)_N = \sum_{n=0}^{N} (-1)^n \binom{N+1}{n}_q q^{n(n-1)/2} x^n,$$

involving the q-binomial coefficients:

$$\binom{n}{m}_q := \frac{(n)_q}{(m)_q (n-m)_q}, \quad (n)_q := (1-q)\bigl(1-q^2\bigr)\cdots\bigl(1-q^n\bigr).$$

We get $a_{\mathbb{P}^N}(n)$ by multiplying the expressions for $1/(x;q)_N$ and $(x^2;q)_N$.

Proposition 1.7. *For all $n \geqslant 1$,*

$$a_{\mathbb{P}^N}(n) = \sum_{2i+j=n} (-1)^i \binom{N+1}{i}_q \binom{N+j}{j}_q q^{i(i-1)/2}.$$

Finally, we compute $a_V(n)$ for certain open subvarieties of the type $V = \mathbb{P}^N \setminus S(d_1^{s_1}, \ldots, d_n^{s_n})$, where $S(d_1^{s_1}, \ldots, d_n^{s_n})$ denotes any rational n-set which is the disjoint union of s_i different σ-orbits of points of degree d_i, for $i = 1, \ldots, n$. For $V = \mathbb{P}^2 \setminus S(3)$ we use the function $\delta : \mathbb{N} \to \mathbb{N}$ defined as

$$\delta(n) := \begin{cases} 0, & \text{if } n \equiv 1, 4 \pmod 6,\\ 1, & \text{if } n \equiv 2, 3 \pmod 6,\\ -1, & \text{if } n \equiv 0, 5 \pmod 6. \end{cases}$$

Proposition 1.8. *For all $n \geqslant 1$,*

$$a_{\mathbb{P}^1\setminus S(2)}(n) = \frac{q+1}{q^2+1}\bigl(q^{n+1} - q^n - (-1)^{\lceil n/2\rceil}q + (-1)^{\lceil (n-1)/2\rceil}\bigr).$$

$$a_{\mathbb{P}^2\setminus S(1)}(n) = \begin{cases} q^2+q, & \textit{if } n=1,\\ q^4+q^3-q, & \textit{if } n=2,\\ q^{2n-4}(q^3-1)(q+1), & \textit{if } n\geqslant 3.\end{cases}$$

$$a_{\mathbb{P}^2\setminus S(3)}(n) = \frac{q^2+q+1}{q^4-q^2+1}\bigl(q^{2n+2} - q^{2n} + \delta(n)q^2 + \delta(n+2)\bigr).$$

$$\begin{aligned} a_{\mathbb{P}^2\setminus S(1^3)}(n) = {} & \frac{q-1}{(q^2+1)^2}\bigl[(q^3+2q^2+2q+1)q^{2n}\\ & + (-1)^n\bigl((n-1)q^3 - (n+2)q^2 + (n-2)q - (n+1)\bigr)\bigr].\end{aligned}$$

$$\begin{aligned} a_{\mathbb{P}^2\setminus S(1,2)}(n) = {} & \frac{q+1}{q^4+1}\biggl(q^{2n+3} - q^{2n} + \frac{1}{2}\bigl((-1)^{\lfloor\frac{n-1}{2}\rfloor} + (-1)^{\lfloor\frac{n}{2}\rfloor}\bigr)q(q+1)\\ & - \frac{1}{2}\bigl((-1)^{\lfloor\frac{n+1}{2}\rfloor} + (-1)^{\lfloor\frac{n}{2}\rfloor}\bigr)(q^3-1)\biggr).\end{aligned}$$

2. Zeta function of the quotient of $\mathbb{P}^N$ by an automorphism

For any $\gamma \in \mathrm{PGL}_{N+1}(k)$, we denote by $\mathbb{P}^N/\gamma$ the quotient variety of $\mathbb{P}^N$ by the action of the finite cyclic group generated by γ. The aim of this section is to prove the following result.

Theorem 2.1. *For any $\gamma \in \mathrm{PGL}_{N+1}(k)$, we have $\mathrm{Z}(\mathbb{P}^N/\gamma, t) = \mathrm{Z}(\mathbb{P}^N, t)$.*

This theorem has two important consequences (Corollaries 2.2, 2.4), that will be crucial for the enumeration of orbits of n-sets and n-multisets:

Corollary 2.2. *Let $\gamma \in \mathrm{PGL}_{N+1}(k)$. Let $W \subseteq V$ be subvarieties of $\mathbb{P}^N$ defined over k, both expressable as a finite union of linear irreducible γ-invariant subvarieties of $\mathbb{P}^N$. Let $U = V \setminus W$ be the complementary variety. Then,*

$$f_{V/\gamma}(x) = f_V(x), \qquad f_{U/\gamma}(x) = f_U(x),$$
$$\overline{f}_{V/\gamma}(x) = \overline{f}_V(x), \qquad \overline{f}_{U/\gamma}(x) = \overline{f}_U(x).$$

Proof. If V is a linear irreducible γ-invariant subvariety of $\mathbb{P}^N$, then $V \simeq \mathbb{P}^{\dim V}$ and $\mathrm{Z}(V/\gamma, t) = \mathrm{Z}(V, t)$ by Theorem 2.1. This equality holds too for V a finite union of linear irreducible γ-invariant subvarieties, since each irreducible component of V and the intersection of any number of components are projective spaces. The corollary follows from Theorem 1.2 and Lemma 1.3. □

Definition 2.3. Let $\gamma \in \mathrm{PGL}_{N+1}(k)$. The *$\gamma$-orbit* of $P \in \mathbb{P}^N(\bar{k})$, denoted $O_\gamma(P)$, is the orbit of P under the action of the cyclic group generated by γ.

Let $V \subseteq \mathbb{P}^N$ be a subvariety over k. The sets of rational n-sets and n-multisets of V that are fixed by γ as unordered families of points of $\mathbb{P}^N(\bar{k})$ are denoted:

$$\mathrm{Fix}_\gamma(V,n) := \left\{ S \in \binom{V}{n}(k) \;\middle|\; \gamma(S) = S \right\},$$
$$\mathrm{Fix}_\gamma((V,n)) := \left\{ S \in \left(\!\!\binom{V}{n}\!\!\right)(k) \;\middle|\; \gamma(S) = S \right\}.$$

Corollary 2.4. *Let γ, V, W, U be as in Corollary* 2.2 *and suppose that all $\bar{k}$-rational points of U have γ-orbits of the same length m. Then,*

$$\left|\mathrm{Fix}_\gamma(U,mn)\right| = \left|\binom{U}{n}(k)\right|, \qquad \left|\mathrm{Fix}_\gamma((U,mn))\right| = \left|\left(\!\!\binom{U}{n}\!\!\right)(k)\right|.$$

Proof. The γ-invariant and σ-invariant mn-sets of U are in one-to-one correspondence with the σ-invariant n-sets of U/γ; thus, by Corollary 2.2

$$\left|\mathrm{Fix}_\gamma(U,mn)\right| = \left|\binom{U/\gamma}{n}(k)\right| = \left|\binom{U}{n}(k)\right|.$$

The argument for $|\mathrm{Fix}_\gamma((U,mn))|$ is analogous. □

In order to prove Theorem 2.1 we attain first a similar result for $\mathbb{A}^N$.

Proposition 2.5. *For any $\gamma \in \mathrm{GL}_N(k)$ we have $|(\mathbb{A}^N/\gamma)(k)| = |\mathbb{A}^N(k)|$.*

Proof. Our aim is to compute the cardinality of the set

$$(\mathbb{A}^N/\gamma)(k) = \left\{ O_\gamma(P),\, P \in \mathbb{A}^N(\bar{k}) \;\middle|\; \sigma\big(O_\gamma(P)\big) = O_\gamma(P) \right\}.$$

Since γ and σ commute, for any $P \in \mathbb{A}^N(\bar{k})$ we have:

$$\sigma\big(O_\gamma(P)\big) = O_\gamma(P) \quad \text{if and only if} \quad \sigma(P) \in O_\gamma(P). \tag{4}$$

For any $\rho \in \mathrm{GL}_N(k)$, let us denote by C_ρ the set $\{P \in \mathbb{A}^N(\bar{k}) \mid \sigma(P) = \rho(P)\}$. If m is the order of γ as an element of $\mathrm{GL}_N(k)$ we claim that

$$\left|(\mathbb{A}^N/\gamma)(k)\right| = \frac{1}{m} \sum_{0 \leqslant i < m} |C_{\gamma^i}|. \tag{5}$$

In fact, consider the formal disjoint union of all C_{γ^i} (which are not disjoint as subsets of $\mathbb{A}^N(\bar{k})$) and the map

$$O_\gamma : \coprod_{0 \leqslant i < m} C_{\gamma^i} \to (\mathbb{A}^N/\gamma)(k), \qquad P \mapsto O_\gamma(P).$$

By (4), $O_\gamma(P)$ is defined over k if and only if $P \in \bigcup_{0 \leqslant i < m} C_{\gamma^i}$, so that this map is well defined and onto. Thus, to prove (5) we need only to check that each $O_\gamma(P) \in (\mathbb{A}^N/\gamma)(k)$ has exactly m preimages. Let $d = |O_\gamma(P)|$; clearly $d|m$ and $P \in C_{\gamma^i}$ for a unique $0 \leqslant i < d$. Now, the d points of $O_\gamma(P)$ belong to

$$C_{\gamma^i}, C_{\gamma^{i+d}}, C_{\gamma^{i+2d}}, \ldots, C_{\gamma^{i+(\frac{m}{d}-1)d}},$$

and none of these points belongs to any other C_{γ^j}. Therefore, $O_\gamma(P)$ has exactly $d(m/d) = m$ preimages.

Finally, the proposition will be proved if we show that $|C_\rho| = q^N$ for all $\rho \in \mathrm{GL}_N(k)$. Let us check this; for any given $\rho \in \mathrm{GL}_N(k)$ let $\beta \in \mathrm{GL}_N(k)$ be such that $\beta\rho\beta^{-1}$ is a rational canonical matrix: $\beta\rho\beta^{-1} = \mathrm{diag}(A_1, \dots, A_r)$, each A_i being a cyclic component of the type:

$$A = \begin{pmatrix} 0 & & \cdots & & -a_s \\ 1 & 0 & \cdots & & -a_{s-1} \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & -a_2 \\ & & & 1 & -a_1 \end{pmatrix}, \tag{6}$$

with $x^s + a_1x^{s-1} + \cdots + a_s \in k[x]$ an invariant factor of the endomorphism ρ. We have $|C_\rho| = |C_{\beta\rho\beta^{-1}}|$ because the automorphism β of $\mathbb{A}^N(\bar{k})$ maps one set onto the other. Hence, we need only to check that $|C_A| = q^s$, for a matrix A as in (6). For $x = (x_1, \dots, x_s) \in \bar{k}^s$, the equality $\sigma(x) = A(x)$ splits into

$$\sigma(x_1) = -a_s x_s, \qquad \sigma(x_2) = x_1 - a_{s-1}x_s, \qquad \dots, \qquad \sigma(x_s) = x_{s-1} - a_1 x_s. \tag{7}$$

Thus, $x_1, \dots, x_{s-1}$ are a linear combination of x_s and its Galois conjugates:

$$x_{s-i} = a_i x_s + a_{i-1}\sigma(x_s) + \cdots + a_1\sigma^{i-1}(x_s) + \sigma^i(x_s), \quad 1 \leqslant i < s,$$

and the first equation of (7) is equivalent to

$$\sigma^s(x_s) + a_1\sigma^{s-1}(x_s) + \cdots + a_{s-1}\sigma(x_s) + a_s x_s = 0.$$

Since $a_s \neq 0$, this is a separable equation in x_s with q^s solutions in $\bar{k}$. □

We are now ready to prove Theorem 2.1, which is an immediate consequence of the following proposition.

Proposition 2.6. *For any $\gamma \in \mathrm{PGL}_{N+1}(k)$ we have $|(\mathbb{P}^N/\gamma)(k)| = |\mathbb{P}^N(k)|$.*

Proof. We choose a representative of γ in $\mathrm{GL}_{N+1}(k)$, which we still denote by γ. We identify an affine point $P \in \mathbb{A}^{N+1}(\bar{k})$ with its image $P \in \mathbb{P}^N(\bar{k})$ under the natural morphism $\pi : \mathbb{A}^{N+1} \setminus \{0\} \to \mathbb{P}^N$. However, in order to avoid confusion we shall denote by $O_\gamma(P)$ the affine γ-orbit of P and by $O_\gamma^{\mathrm{pr}}(P)$ the projective orbit. Clearly $\pi(O_\gamma(P)) = O_\gamma^{\mathrm{pr}}(P)$ and π induces a natural map

$$\pi : \big(\mathbb{A}^{N+1}/\gamma\big)(k) \setminus \{0\} \to \big(\mathbb{P}^N/\gamma\big)(k).$$

By Proposition 2.5, we need only to show that π is onto and each element of $(\mathbb{P}^N/\gamma)(k)$ has $q-1$ preimages. Let $O_\gamma^{\mathrm{pr}}(P) \in (\mathbb{P}^N/\gamma)(k)$ be given; for $Q \in \mathbb{A}^{N+1}(\bar{k})$ the condition $\pi(O_\gamma(Q)) = O_\gamma^{\mathrm{pr}}(P)$ is equivalent to $O_\gamma(Q) = O_\gamma(\mu P)$ for some $\mu \in \bar{k}^*$. Thus, we want to see that exactly $q-1$ of the orbits $O_\gamma(\mu P)$, $\mu \in \bar{k}^*$, are k-rational. To check this, consider the multiplicative subgroup $\Lambda_P := \{\lambda \in \bar{k}^* \mid \lambda O_\gamma(P) = O_\gamma(P)\} \subseteq \bar{k}^*$, and let $e = |\Lambda_P|$. For any $\mu \in \bar{k}^*$,

$$\sigma\big(O_\gamma(\mu P)\big) = \sigma\big(\mu O_\gamma(P)\big) = \sigma(\mu)\sigma\big(O_\gamma(P)\big) = \sigma(\mu)O_\gamma(P).$$

Thus, $O_\gamma(\mu P)$ is k-rational if and only if $\sigma(\mu)\mu^{-1}O_\gamma(P) = O_\gamma(P)$, or equivalently $\mu^{q-1} \in \Lambda_P$. On the other hand, for any $\mu \in \bar{k}^*$ there are e values $\mu' \in \bar{k}^*$ providing the same γ-orbit:

$$O_\gamma(\mu P) = O_\gamma(\mu' P) \quad \Leftrightarrow \quad \mu'\mu^{-1} \in \Lambda_P \quad \Leftrightarrow \quad \mu' \in \mu\Lambda_P.$$

Hence, the $e(q-1)$ values of $\mu \in \bar{k}^*$ such that $O_\gamma(\mu P)$ is k-rational determine exactly $q-1$ different γ-orbits. □

3. *G*-exponent index and generating functions

Let Γ be a finite group acting on a finite set X. The number of orbits of this action can be counted as the average number of fixed points:

$$|\Gamma\backslash X| = \frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}\left|\mathrm{Fix}_\gamma(X)\right| = \sum_{\gamma\in\mathcal{C}}\frac{|\operatorname{Fix}_\gamma(X)|}{|\Gamma_\gamma|}, \tag{8}$$

where $\mathcal{C}$ is a set of representatives of conjugacy classes of elements of Γ and

$$\mathrm{Fix}_\gamma(X) := \left\{x \in X \mid \gamma(x) = x\right\}, \qquad \Gamma_\gamma := \left\{\rho \in \Gamma \mid \rho\gamma\rho^{-1} = \gamma\right\}.$$

The formula (8) is usually called Burnside's theorem, or more accurately the Cauchy–Frobenius theorem [2, 3.1.6]. In this section we apply this formula to compute the generating function of

$$t_N(n) := \left|\Gamma\Big\backslash\binom{\mathbb{P}^N}{n}(k)\right|, \qquad \bar{t}_N(n) := \left|\Gamma\Big\backslash\left(\!\!\binom{\mathbb{P}^N}{n}\!\!\right)(k)\right|,$$

for $\Gamma := \mathrm{PGL}_{N+1}(k)$. The crucial step is the computation of $|\operatorname{Fix}_\gamma(\mathbb{P}^N, n)|$, $|\operatorname{Fix}_\gamma((\mathbb{P}^N, n))|$ (cf. Definition 2.3), and the ingredients for this computation are Corollary 2.4 and a weighted finite poset $\mathcal{P}(\gamma)$ that we introduce now.

3.1. *Proper linear arrangements in projective spaces*

We fix throughout this paragraph an automorphism $\gamma \in \mathrm{PGL}_{N+1}(k)$ of $\mathbb{P}^N$.

For any variety $V \subseteq \mathbb{P}^N(\bar{k})$, we define the *degree* of V, denoted $\deg V$, to be the least exponent r such that $\sigma^r(V) = V$ (i.e. V is defined over k_r). This arithmetic invariant of V should not be confused with the geometric concept of degree as an embedded subvariety of the projective space.

Let $V \subseteq \mathbb{P}^N(\bar{k})$ be a γ-invariant variety. We define the *exponent* of V, denoted $\exp V$, to be the order of γ as an automorphism of V. Note that $W \subseteq V$ implies $\exp W \mid \exp V$.

We define a *G-linear arrangement* to be a linear arrangement of the type

$$V = L \cup \sigma(L) \cup \cdots \cup \sigma^{r-1}(L), \quad r = \deg L,$$

where $L \subseteq \mathbb{P}^N(\bar{k})$ is a γ-invariant irreducible linear variety. We denote by $\mathcal{L}_G = \mathcal{L}_G(\gamma)$ the set of all G-linear arrangements. Each $V \in \mathcal{L}_G$ has a 3-dimensional weight given by three invariants *dimension*, *exponent* and *G-degree*:

$$(\dim V, \exp V, \mathrm{d}_G\, V) := (\dim L, \exp L, \deg L)$$

where L is any of the irreducible components of V. Note that $\dim V$ and $\exp V$ are the dimension and exponent of V as a variety, but the G-degree $\mathrm{d}_G\, V$ should not be confused with the degree of V as a variety, which is $\deg V = 1$.

Definition 3.1. A G-linear arrangement $V \in \mathcal{L}_G$ is said to be *proper* if it is maximal among all other G-linear arrangements with the same exponent:

$$\exp V < \exp W, \quad \forall W \in \mathcal{L}_G \text{ such that } V \subsetneq W.$$

We denote by $\mathcal{P} = \mathcal{P}(\gamma)$ the poset formed by the proper G-linear arrangements ordered by inclusion.

For instance, $\mathbb{P}^N$ is a proper G-linear arrangement with weight $(N, \operatorname{ord}(\gamma), 1)$. For any $V \in \mathcal{P}$ we define

$$V^0 := V \Big\backslash \Big(\bigcup_{W \in \mathcal{P},\, W < V} W \Big).$$

Theorem 3.2.

(1) *The poset $\mathcal{P}$ is a finite lattice.*
(2) *For any $V \in \mathcal{P}$ and any $P \in V^0$, the γ-orbit of P has* $\exp V$ *elements.*
(3) *For any $V \in \mathcal{P}$ of dimension d and* $\mathrm{d}_G\, V = r$ *we have $f_V(x) = f_{\mathbb{P}^d/k_r}(x^r)$.*

This result summarizes the properties of the poset $\mathcal{P}$ that we need for the proof of the main theorem. The proof of Theorem 3.2 is postponed to Section 5, where we shall study in more detail the structure of the poset $\mathcal{P}$.

3.2. The main theorem

Let $\gamma \in \mathrm{PGL}_{N+1}(k)$ be a fixed automorphism of $\mathbb{P}^N$ and consider the stratification $\mathbb{P}^N(\bar{k}) = \coprod_{V \in \mathcal{P}} V^0$, determined by the proper G-linear arrangements with respect to γ. For any rational n-set $S \in \operatorname{Fix}_\gamma(\mathbb{P}^N, n)$ let the distribution of the n points of S among these strata be

$$S = \coprod_{V \in \mathcal{P}} S_V, \quad S_V := S \cap V^0.$$

Since S and V^0 are γ-invariant and σ-invariant, each S_V is also γ-invariant and σ-invariant; in other words, $S_V \in \operatorname{Fix}_\gamma(V^0, |S_V|)$. Thus, we can count the number of possibilities for S just by considering all possible numerical distributions of n points among the strata V^0, and then counting, for each numerical distribution, the number of possibilities for S_V. By (2) of Theorem 3.2, $|S_V| = n_V \exp V$ for some non-negative integer n_V, and

$$\begin{aligned} \big|\operatorname{Fix}_\gamma\big(\mathbb{P}^N, n\big)\big| &= \sum_{\sum_{V \in \mathcal{P}} n_V \exp V = n} \Big(\prod_{V \in \mathcal{P}} \big|\operatorname{Fix}_\gamma\big(V^0, n_V \exp V\big)\big| \Big) \\ &= \sum_{\sum_{V \in \mathcal{P}} n_V \exp V = n} \Big(\prod_{V \in \mathcal{P}} \Big| \binom{V^0}{n_V}(k) \Big| \Big), \end{aligned}$$

the last equality by Corollary 2.4. Therefore,

$$\sum_{n \geqslant 0} \big|\operatorname{Fix}_\gamma\big(\mathbb{P}^N, n\big)\big| x^n = \prod_{V \in \mathcal{P}} f_{V^0}\big(x^{\exp V}\big).$$

An application of the Cauchy–Frobenius formula leads to a first computation of the generating function we are interested in:

$$\sum_{n \geqslant 0} t_N(n) x^n = \sum_{\gamma \in \mathcal{C}} |\Gamma_\gamma|^{-1} \prod_{V \in \mathcal{P}(\gamma)} f_{V^0}\big(x^{\exp V}\big). \tag{9}$$

We can compute $f_{V^0}(x)$ by Möbius inversion in the poset $\mathcal{P}(\gamma)$ [12, 3.7]:

$$f_{V^0}(x) = \prod_{W \leqslant V} f_W(x)^{\mu(W,V)} = \prod_{W \leqslant V} f_{\mathbb{P}^{\dim W}/k_{\mathrm{d}_G W}}\big(x^{\mathrm{d}_G\, W}\big)^{\mu(W,V)},$$

the last equality by (3) of Theorem 3.2. Hence, the term $\prod_{V\in\mathcal{P}(\gamma)} f_{V^0}(x^{\exp V})$ depends only on the structure of the weighted poset $\mathcal{P}(\gamma)$. This allows us to refine (9) by grouping together all elements $\gamma\in\mathcal{C}$ with a common value of $\prod_{V\in\mathcal{P}(\gamma)} f_{V^0}(x^{\exp V})$.

Definition 3.3. Two elements $\gamma,\gamma'\in\mathcal{C}$ have the same *subtype* if there exists a poset isomorphism $\mathcal{P}(\gamma)\xrightarrow{\sim}\mathcal{P}(\gamma')$, preserving the weight $(\dim V, \exp V, \mathrm{d}_G V)$ of each node V. We denote by $\mathcal{S}$ the quotient set of $\mathcal{C}$ by this equivalence relation. For each subtype $\alpha\in\mathcal{S}$ we denote by $\mathcal{P}(\alpha)$ the poset $\mathcal{P}(\gamma)$ for any choice of γ in α, and we consider the weighted sum: $c_\alpha := \sum_{\gamma\in\alpha}|\Gamma_\gamma|^{-1}$.

Our main theorem is a rewriting of (9) after grouping together all $\gamma\in\mathcal{C}$ in the same subtype. We include in the theorem the similar statement for n-multisets, which is obtained by completely analogous arguments.

Theorem 3.4. *For a fixed value of $N\geqslant 1$, the generating functions of the numbers $t_N(n)$, $\bar{t}_N(n)$ are given by*

$$\sum_{n\geqslant 0} t_N(n)x^n = \sum_{\alpha\in\mathcal{S}} c_\alpha \prod_{V\in\mathcal{P}(\alpha)} h_{\alpha,V}(x), \qquad \sum_{n\geqslant 0} \bar{t}_N(n)x^n = \sum_{\alpha\in\mathcal{S}} c_\alpha \prod_{V\in\mathcal{P}(\alpha)} \bar{h}_{\alpha,V}(x),$$

where $h_{\alpha,V}(x)$ is the series

$$h_{\alpha,V}(x) := f_{V^0}\bigl(x^{\exp V}\bigr) = \prod_{W\leqslant V} f_{\mathbb{P}^{\dim W}/k_{\mathrm{d}_G W}}\bigl(x^{\exp V\,\mathrm{d}_G W}\bigr)^{\mu(W,V)}$$

and $\bar{h}_{\alpha,V}(x)$ has a similar expression replacing f by $\bar{f}$.

This formula is suitable of an effective implementation. In this regard one needs only to carry out the following tasks:

(1) Find an intrinsic description of the set $\mathcal{S}$ of subtypes.
(2) For each $\alpha\in\mathcal{S}$ find an intrinsic description of the weighted poset $\mathcal{P}(\alpha)$ and its Möbius function.
(3) For each $\alpha\in\mathcal{S}$ find an explicit formula for the universal coefficients c_α.

This will be fulfilled in Section 4 for the cases $N=1,2$. As a consequence, we shall obtain explicit formulas for $t_2(n)$, $\bar{t}_2(n)$ as polynomials with integer coefficients in the cardinality q of the ground field. Similar formulas for $t_1(n)$, $\bar{t}_1(n)$ had been obtained in [8].

In practice we often find problems leading to the computation of numbers, say $x(n)$, counting $\mathrm{PGL}_{N+1}(k)$-orbits of rational n-sets of projective spaces that satisfy certain conditions: no three points on a line, no six points on a conic, general position, etc. In these cases it is usually difficult to obtain a description of the generating function of the $x(n)$ in the spirit of Theorem 3.4, but it is still possible to apply the techniques of this paper to obtain explicit formulas for the $x(n)$. In fact, suppose that $x(n)=|\mathrm{PGL}_{N+1}(k)\backslash X|$, where $X\subseteq\binom{\mathbb{P}^N}{n}(k)$ is stable under the action of $\mathrm{PGL}_{N+1}(k)$ and, moreover, $|\mathrm{Fix}_\gamma(X)|$ depends only on the subtype of γ, for any automorphism γ of $\mathbb{P}^N$. Then, by the Cauchy–Frobenius formula:

$$\bigl|\mathrm{PGL}_{N+1}(k)\backslash X\bigr| = \sum_{\alpha\in\mathcal{S}} c_\alpha\bigl|\mathrm{Fix}_\gamma(X)\bigr|,$$

and the computation of $x(n)$ is reduced to the computation of $|\mathrm{Fix}_\gamma(X)|$ for one representative γ of each subtype. Often, this computation can be deduced too, from Corollary 2.4 and the formulas of Section 1 if one is able to control the behavior of the conditions defining X under the quotient maps $\mathbb{P}^N \to \mathbb{P}^N/\gamma$. Since the constants c_α do not depend on X we occasionally call them "universal coefficients."

For instance, this technique has been used in the papers [3] and [11] to count, for any given value of the genus $g > 1$, the number of k-isomorphism classes of hyperelliptic curves, of pointed hyperelliptic curves, and of hyperelliptic curves having a rational Weierstrass point.

4. Explicit formulas for dimension $N = 1, 2$

The description of the subtypes of conjugacy classes of $\mathrm{PGL}_{N+1}(k)$ and the computation of the coefficients c_α can be deduced from [7, Proposition 2.3, Lemma 2.4] for $N = 1$ and from [9, Sections 1–2] for $N = 2$.

The conjugacy classes are first distributed into *types* according to the rational canonical form of the matrices. Then, the conjugacy classes of each type are distributed into subtypes. For $N = 1, 2$ two conjugacy classes are in the same subtype if and only if they have the same cycle decomposition as a permutation of $\mathbb{P}^N(k)$. This is not true anymore for $N \geqslant 3$.

4.1. Types and subtypes in dimension $N = 1$

The conjugacy classes of $\mathrm{PGL}_2(k)$ are distributed into four types:

A. The identity, $\gamma = 1$, has order 1 and $|\Gamma_\gamma| = |\mathrm{PGL}_2(k)| = q(q^2 - 1)$.

B. The class of the translation $\gamma_0 = \left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$. It has only one fixed point (the point at infinity), order p and $|\Gamma_{\gamma_0}| = q$.

C. The classes of $\gamma = \mathrm{diag}(\lambda, 1)$, $\lambda \in k^*$, $\lambda \neq 1$. They have two fixed points, lying in $\mathbb{P}^1(k)$, and order $d = \mathrm{ord}_{k^*}(\lambda)$ which is a divisor of $q - 1$.

The subtypes are parameterized by divisors $d > 1$ of $q - 1$, and for any such d

$$c_d = \frac{\varphi(d)}{2(q-1)}.$$

D. The classes of those γ represented by a matrix $B_2 \in \mathrm{GL}_2(k)$ with irreducible characteristic polynomial. They have two fixed points, which are quadratic conjugate in $\mathbb{P}^1(k_2)$. If $\alpha \in k_2 \setminus k$ is an eigenvalue of B_2, the order of γ is the least positive integer d such that $\alpha^d \in k$, and it is a divisor of $q + 1$.

The subtypes are parameterized by divisors $d > 1$ of $q + 1$, and for any such d

$$c_d = \frac{\varphi(d)}{2(q+1)}.$$

4.2. Types and subtypes in dimension $N = 2$

Denote by $P_1 = (1, 0, 0)$, $P_2 = (0, 1, 0)$, $P_3 = (0, 0, 1)$ the three fundamental points of $\mathbb{P}^2$, and by $L_1 = \overline{P_2P_3}$, $L_2 = \overline{P_1P_3}$, $L_3 = \overline{P_1P_2}$ the three fundamental lines. The conjugacy classes of $\mathrm{PGL}_3(k)$ are distributed into eight types:

A. The identity, $\gamma = 1$, has order 1 and $|\Gamma_\gamma| = |\mathrm{PGL}_3(k)| = q^3(q^2 - 1)(q^3 - 1)$.

B. The class of the translation $\gamma_0=\operatorname{diag}\left(\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right),1\right)$. It has order p and the γ_0-invariant lines are all lines through P_1; the line L_2 has exponent 1 and all other invariant lines have exponent p. Moreover, $|\Gamma_{\gamma_0}|=q^3(q-1)$.

C. The class of $\gamma_0'=\left(\begin{smallmatrix}1&1&0\\0&1&1\\0&0&1\end{smallmatrix}\right)$. It has only one invariant line, L_3, of exponent p, and only one fixed point, P_1. It has order p if $p>2$, and order 4 if $p=2$. Moreover, $|\Gamma_{\gamma_0'}|=q^2$.

D. The classes of $\gamma=\operatorname{diag}\left(\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right),\lambda\right)$, $\lambda\in k^*$, $\lambda\ne 1$. They have order pd, with $d=\operatorname{ord}_{k^*}(\lambda)$. The fixed points are P_1, P_3 and the invariant lines are L_2 (of exponent d) and L_3 (of exponent p).

The subtypes are parameterized by divisors $d>1$ of $q-1$, and for any such d

$$c_d=\frac{\varphi(d)}{q(q-1)}.$$

E. The classes of $\gamma=\operatorname{diag}(\lambda,1,1)$, $\lambda\in k^*$, $\lambda\ne 1$. They have order $d=\operatorname{ord}_{k^*}(\lambda)$. The fixed points are P_1 and the whole line L_1; the invariant lines are L_1 (of exponent 1) and every line through P_1 (of exponent d).

The subtypes are parameterized by divisors $d>1$ of $q-1$, and for any such d

$$c_d=\frac{\varphi(d)}{q(q-1)(q^2-1)}.$$

F. The classes of $\gamma=\operatorname{diag}(\lambda,\mu,1)$, $\lambda,\mu\in k^*\setminus\{1\}$, $\lambda\ne\mu$. They have three fixed points P_1,P_2,P_3 and three invariant lines L_1,L_2,L_3 of respective exponent $d=\operatorname{ord}_{k^*}(\mu)$, $e=\operatorname{ord}_{k^*}(\lambda)$, $f=\operatorname{ord}_{k^*}(\lambda/\mu)$. The order of γ is $m=\operatorname{lcm}(d,e)=\operatorname{lcm}(d,f)=\operatorname{lcm}(e,f)$.

The subtypes are parameterized by the set $\mathcal{S}_F$ of triples (d,e,f) of divisors of $q-1$ satisfying $d\geqslant e\geqslant f>1$ and $\operatorname{lcm}(d,e)=\operatorname{lcm}(d,f)=\operatorname{lcm}(e,f)$. For any such triple

$$c_{(d,e,f)}=\frac{\varphi(m)\varphi(h)\psi(H)}{\delta_{d,e,f}(q-1)^2},$$

where $m=\operatorname{lcm}(d,e)$, $(def)/m^2=hH$ is the unique decomposition of this divisor of m into a product of positive divisors h, H satisfying respectively

$$v_\ell(h)<v_\ell(m),\qquad v_\ell(H)=v_\ell(m),$$

for any prime divisor ℓ of $(def)/m^2$; also, ψ is the multiplicative function determined by $\psi(\ell^r)=(\ell-2)\ell^{r-1}$ for any prime power and

$$\delta_{d,e,f}=\begin{cases}1, & \text{if } d>e>f,\\ 2, & \text{if } d=e>f,\\ 6, & \text{if } d=e=f.\end{cases}$$

G. The classes of $\gamma=\operatorname{diag}(B_2,1)$, where $B_2\in\mathrm{GL}_2(k)$ has irreducible characteristic polynomial. If $\alpha\in k_2\setminus k$ is an eigenvalue of B_2, the order of γ is de, where d is the least positive divisor of $q+1$ such that $\alpha^d\in k$, and $e=\operatorname{ord}_{k^*}(\alpha^d)$. The fixed points are $P_3,P,\sigma(P)$, where $P\in L_3$ has $\deg P=2$. The only invariant line is L_3 and it has exponent d.

The subtypes are parameterized by pairs (d,e) of respective positive divisors of $q+1$ and $q-1$, with $d>1$. For any such pair,

$$c_{(d,e)}=\frac{\delta_{d,e}\varphi(d)\varphi(e)}{2(q^2-1)},\qquad \delta_{d,e}=\begin{cases}1 & \text{if } d \text{ odd},\\ 0 & \text{if } d \text{ even and } e\mid(q-1)/2,\\ 2 & \text{if } d \text{ even and } e\nmid(q-1)/2.\end{cases}$$

H. The classes of $\gamma = B_3$, where $B_3 \in \mathrm{GL}_3(k)$ has irreducible characteristic polynomial. If $\alpha \in k_3 \setminus k$ is an eigenvalue of B_3, the order of γ is the least positive integer d such that $\alpha^d \in k$, which is a divisor of q^2+q+1. There are three fixed points, that form a G-linear arrangement of dimension 0, exponent 1 and G-degree 3. There are three invariant lines, that form a G-linear arrangement of dimension 1, exponent d and G-degree 3.

The subtypes are parameterized by positive divisors $d > 1$ of q^2+q+1, and for any such d

$$c_d = \frac{\varphi(d)}{3(q^2+q+1)}.$$

4.3. Explicit computations

In Tables 1, 2 we display the Hasse diagram of the poset $\mathcal{P}(\alpha)$ associated to each subtype. The subtypes are determined by the different values of the exponents of the nodes of this poset, indicated in the fourth column. The nodes of G-degree one are represented by $\bullet$ and labeled with the value of $\exp V$. The nodes with greater G-degree are represented by $\circ$ and labeled with $\exp V(\deg V)$. The value of $\dim V$ is given by the vertical level of the node (of height 0, 1 or 0, 1, 2) inside the poset; when there is some ambiguity we write the dimension of a concrete level in the left side of the poset.

We have carried out the tasks (1), (2), (3) mentioned in the last section, and this allows us to apply Theorem 3.4 to compute the generating function of $t_1(n), t_2(n), \bar{t}_1(n), \bar{t}_2(n)$. For $t_1(n), t_2(n)$ this is achieved in Theorems 4.1 and 4.2, where we split the formula of Theorem 3.4 into partial terms according to the different types of the elements of $\mathcal{C}$.

Theorem 4.1. *The numbers $t_1(n)$ split into the sum of four terms*:

$$t_1(n) = t_{1,A}(n) + t_{1,B}(n) + t_{1,C}(n) + t_{1,D}(n),$$

each term having the following generating function:

$$\sum_{n\geqslant 0} t_{1,A}(n)x^n = \frac{1}{q(q^2-1)} f_{\mathbb{P}^1}(x),$$

$$\sum_{n\geqslant 0} t_{1,B}(n)x^n = \frac{1}{q}(1+x) f_{\mathbb{A}^1}\bigl(x^p\bigr),$$

Table 1
Types, subtypes and posets $\mathcal{P}(\alpha)$ for $\gamma \in \mathrm{PGL}_2(k)$

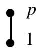
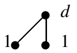
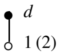
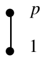
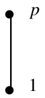
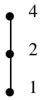
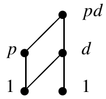
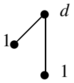
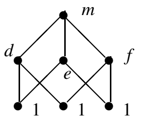
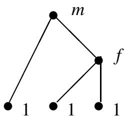
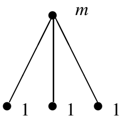
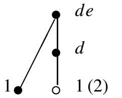
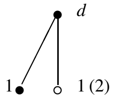
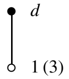
Type	γ	$\mathcal{P}(\alpha)$	Subtypes
A	1	dim 1 $\bullet$ 1	
B	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$		
C	diag(λ, 1) λ ≠ 1		$d \mid q-1,\ d > 1$
D	B_2		$d \mid q+1,\ d > 1$

Table 2
Types, subtypes and posets $\mathcal{P}(\alpha)$ for $\gamma \in \mathrm{PGL}_3(k)$

Type	γ	$\mathcal{P}(\alpha)$	Subtypes
A	1	dim 2 ● 1	
B	$\operatorname{diag}\left(\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}, 1\right)$	dim 1 	
C	$\begin{pmatrix}1 & 1 & 0\\ 0 & 1 & 1\\ 0 & 0 & 1\end{pmatrix}$	 $p>2$  $p=2$	
D	$\operatorname{diag}\left(\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}, \lambda\right)$ $\lambda \neq 1$		$d \mid q-1,\ d>1$
E	$\operatorname{diag}(\lambda, 1, 1)$ $\lambda \neq 1$		$d \mid q-1,\ d>1$
F	$\operatorname{diag}(\lambda, \mu, 1)$ $\lambda, \mu \neq 1,\ \lambda \neq \mu$	 $d>e>f$  $d=e>f$  $d=e=f$	$(d,e,f) \in \mathcal{S}_F$ $m = \operatorname{lcm}(d,e)$
G	$\operatorname{diag}(B_2, 1)$	 $e>1$  $e=1$	$d \mid q+1,\ d>1$ $e \mid q-1$
H	B_3	dim 0 	$d \mid q^2+q+1$ $d>1$

$$\sum_{n\geqslant 0} t_{1,C}(n)x^n = \frac{(1+x)^2}{2(q-1)} \sum_{d\mid q-1,\, d>1} \varphi(d) f_{\mathbb{A}^1\setminus S(1)}\bigl(x^d\bigr),$$

$$\sum_{n\geqslant 0} t_{1,D}(n)x^n = \frac{1+x^2}{2(q+1)} \sum_{d\mid q+1,\, d>1} \varphi(d) f_{\mathbb{P}^1\setminus S(2)}\bigl(x^d\bigr).$$

Theorem 4.2. *Let L, L' be two intersecting lines of $\mathbb{A}^2$. The numbers $t_2(n)$ split into the sum of eight terms*:

$$t_2(n) = t_A(n) + t_B(n) + t_C(n) + t_D(n) + t_E(n) + t_F(n) + t_G(n) + t_H(n),$$

each term having the following generating function:

$$\sum_{n\geqslant 0} t_A(n)x^n = \frac{f_{\mathbb{P}^2}(x)}{q^3(q^3-1)(q^2-1)}.$$

$$\sum_{n\geqslant 0} t_B(n)x^n = \frac{1}{q^3(q-1)} f_{\mathbb{P}^1}(x) f_{\mathbb{A}^2}\bigl(x^p\bigr).$$

According to $p>2$ or $p=2$ we have respectively

$$\sum_{n\geqslant 0} t_C(n)x^n = \frac{1+x}{q^2} f_{\mathbb{P}^2\setminus S(1)}\bigl(x^p\bigr), \quad \textit{or} \quad \sum_{n\geqslant 0} t_C(n)x^n = \frac{1+x}{q^2} f_{\mathbb{A}^1}\bigl(x^2\bigr) f_{\mathbb{A}^2}\bigl(x^4\bigr).$$

$$\sum_{n\geqslant 0} t_D(n)x^n = \frac{(1+x)^2 f_{\mathbb{A}^1}(x^p)}{q(q-1)} \sum_{d\mid q-1,\, d>1} \varphi(d) f_{\mathbb{A}^1\setminus S(1)}\bigl(x^d\bigr) f_{\mathbb{A}^2\setminus L}\bigl(x^{pd}\bigr).$$

$$\sum_{n\geqslant 0} t_E(n)x^n = \frac{(1+x) f_{\mathbb{P}^1}(x)}{q(q^2-1)(q-1)} \sum_{d\mid q-1,\, d>1} \varphi(d) f_{\mathbb{A}^2\setminus S(1)}\bigl(x^d\bigr).$$

$$\begin{aligned}\sum_{n\geqslant 0} t_F(n)x^n = \frac{(1+x)^3}{(q-1)^2}\Biggl(&\sum_{(d,e,f)\in\mathcal{S}_F,\, d>e>f} \varphi(m)\varphi(h)\psi(H) \\ &\cdot f_{\mathbb{A}^1\setminus S(1)}\bigl(x^d\bigr) f_{\mathbb{A}^1\setminus S(1)}\bigl(x^e\bigr) f_{\mathbb{A}^1\setminus S(1)}\bigl(x^f\bigr) f_{\mathbb{A}^2\setminus (L\cup L')}\bigl(x^m\bigr) \\ &+ \sum_{(d,e,f)\in\mathcal{S}_F,\, d=e>f} \frac{1}{2}\varphi(m)\varphi(h)\psi(H) f_{\mathbb{A}^1\setminus S(1)}\bigl(x^f\bigr) f_{\mathbb{A}^2\setminus S(1)}\bigl(x^m\bigr) \\ &+ \sum_{(d,e,f)\in\mathcal{S}_F,\, d=e=f} \frac{1}{6}\varphi(m)\psi(m) f_{\mathbb{P}^2\setminus S(1^3)}\bigl(x^m\bigr)\Biggr).\end{aligned}$$

$$\begin{aligned}\sum_{n\geqslant 0} t_G(n)x^n = \frac{(1+x)(1+x^2)}{2(q^2-1)}\Biggl(&\sum_{d\mid q+1,\, d>1,\, d\ odd} \varphi(d) f_{\mathbb{P}^2\setminus S(1,2)}\bigl(x^d\bigr) \\ &+ \sum_{d\mid q+1,\, e\mid q-1,\, d,e>1} \delta_{d,e}\varphi(d)\varphi(e) f_{\mathbb{P}^1\setminus S(2)}\bigl(x^d\bigr) f_{\mathbb{A}^2\setminus S(1)}\bigl(x^{de}\bigr)\Biggr).\end{aligned}$$

$$\sum_{n\geqslant 0} t_H(n)x^n = \frac{1+x^3}{3(q^2+q+1)} \sum_{d\mid q^2+q+1,\, d>1} \varphi(d) f_{\mathbb{P}^2\setminus S(3)}\bigl(x^d\bigr).$$

Theorems 4.1 and 4.2 yield a good general approximation to $t_1(n)$ and $t_2(n)$ as polynomials in q.

Corollary 4.3. *For $n \geqslant 6$ we have* $t_1(n) = q^{n-3} + O(q^{\lfloor \frac{n}{2}\rfloor - 1})$.

For $n \geqslant 8$ we have:

$$t_2(n) = q^{2n-8} + q^{2n-9} + 2\bigl(q^{2n-10} + q^{2n-11} + \cdots + q^{n-2}\bigr) + 3q^{n-3} + O\bigl(q^{n-4}\bigr).$$

Proof. The explicit formulas of Section 1 show that $t_{1,A}(n) = q^{n-3}$, and that $t_{1,B}(n)$, $t_{1,C}(n)$, $t_{1,D}(n)$ are polynomials in q of degree less than $q^{\lfloor \frac{n}{2}\rfloor}$.

For $N=2$ we have

$$t_A(n) = \frac{a_{\mathbb{P}^2}(n)}{q^3(q^3-1)(q^2-1)} = \frac{q^{2n-9}(q^2+1)}{q-1}.$$

Table 3
Value of $t_2(n)$ for $4 \leqslant n \leqslant 7$

n	$t_2(n)$
4	$2q+9+[2]_{3\mid q-1}+[1]_{p=3}-[8]_{p=2}$
5	$2q^2+6q+6+[4]_{3\mid q-1}+[2]_{6\mid q-1}+[6]_{4\mid q-1}+[2]_{4\mid q+1}+[4]_{5\mid q^2-1}$ $+[2]_{p=5}+[1]_{p=3}-[2]_{p=2,\,3\mid q+1}$
6	$q^4+2q^3+6q^2+8q+[3q+5]_{3\mid q-1}+[q-1]_{3\mid q+1}+[q+9]_{4\mid q-1}+[2]_{4\mid q+1}$ $+[10]_{6\mid q-1}+[2]_{6\mid q+1}+[12]_{5\mid q-1}+[4]_{5\mid q+1}+[3]_{p=5}-[2q+1]_{p=2}+[4]_{p=2,\,3\mid q-1}$
7	$q^6+q^5+3q^4+6q^3+11q^2+3q-5+[2q^2+10q+4]_{3\mid q-1}+[2q+16]_{6\mid q-1}$ $+[2]_{6\mid q+1}+[5q+9]_{4\mid q-1}+[q+3]_{4\mid q+1}+[4]_{12\mid q-1}+[20]_{5\mid q-1}+[4]_{5\mid q+1}$ $+[8]_{7\mid q-1}+[6]_{7\mid q+1}+[2]_{7\mid q^2+q+1}+[2]_{p=7}+[3]_{p=5}+[q^2+4q+1]_{p=3}$ $+[2]_{p=3,\,4\mid q-1}-[3q^2+3q-2]_{p=2}+[2q+4]_{p=2,\,3\mid q-1}$

Also, the contribution to $t_E(n)$ of the γ-invariant rational n-sets contained in the set $L_1 \cup \{P_1\}$ of fixed points of any γ of type E is

$$\frac{1}{q(q-1)(q^2-1)} \sum_{d\mid q-1,\, d>1} \varphi(d)\big(a_{\mathbb{P}^1}(n)+a_{\mathbb{P}^1}(n-1)\big) = \frac{q^{n-4}(q^2-q-2)}{q-1}.$$

The contributions of all other terms are expressed as polynomials in q of degree less than $n-3$. □

The formulas of Theorems 4.1 and 4.2 involve the functions $f_V(x)$ for several locally closed subvarieties V of $\mathbb{P}^1$ and $\mathbb{P}^2$. As mentioned in the last section, one can express all these functions in terms of $f_{\mathbb{P}^r}(x)$, $r=0,1,2$, by using the Möbius function of a certain poset. However, in our lower dimension cases, in order to find a concrete expression for $t_1(n)$, $t_2(n)$ it is better to use the explicit computations of the coefficients $a_V(n)$ of $f_V(x)$ that we found in Section 1 for these particular varieties. In Table 3 we display the exact value of $t_2(n)$ for $4 \leqslant n \leqslant 7$, obtained by this method. The computation of $t_F(n)$ requires some extra work that is left to the reader. Also, the reader will check easily that $t_2(1)=1$, $t_2(2)=2$, $t_2(3)=6$. Given a condition P and an integer $x \in \mathbb{Z}$, the expression $[x]_P$ that we use in Table 3 means:

$$[x]_P = \begin{cases} x, & \text{if } P \text{ is true,} \\ 0, & \text{otherwise.} \end{cases}$$

We end this section with a remark that might lead to further work on this topic. We showed in [9] that the numbers of $\mathrm{PGL}_3(k)$-orbits of pointwise rational n-sets of the plane can be expressed as a polynomial in q with rational coefficients. In contrast to this situation, Theorems 4.1, 4.2 and the computations of Section 1 yield formulas for $t_1(n)$, $\bar{t}_1(n)$, $t_2(n)$, $\bar{t}_2(n)$ as a polynomial in q with *integer* coefficients. One may speculate if the numbers $t_N(n)$, $\bar{t}_N(n)$ have this property for all N, n.

5. Proper linear varieties with respect to a fixed automorphism

In this section we prove Theorem 3.2. We fix once and for all a k-automorphism of $\mathbb{P}^N$, represented by some $\gamma \in \mathrm{PGL}_{N+1}(k)$.

Let $\mathcal{L} = \mathcal{L}(\gamma)$ be the poset of γ-invariant irreducible linear subvarieties of $\mathbb{P}^N(\bar{k})$, ordered by inclusion. This poset is not locally finite. For instance, if L is a plane of fixed points of γ

and $P \in L$, the interval $[P, L]$ is not finite. For the basic concepts and notations about posets we address the reader to [12].

Definition 5.1. A node $L \in \mathcal{L}$ is said to be *proper* if it is maximal among all nodes with the same exponent:

$$\exp L < \exp M, \quad \forall M \in \mathcal{L} \text{ such that } L < M.$$

We denote by $\mathcal{L}^{\mathrm{pr}}$ the subposet of $\mathcal{L}$ formed by the proper nodes.

Note that $\mathbb{P}^N$ is always proper. In our example above, the points P and lines M of a plane L of fixed points of γ are not proper, because they have the same exponent as L: $\exp P = \exp M = \exp L = 1$.

Our first aim is to show that $\mathcal{L}^{\mathrm{pr}}$ is a finite poset. To this end we introduce some terminology. We fix a representative of γ in $\mathrm{GL}_{N+1}(k)$, which we still denote by γ, and we use the same notation for γ-invariant subvarieties of $\mathbb{P}^N(\bar{k})$ and their affine cones, which are γ-invariant linear subspaces of $\mathbb{A}^{N+1}(\bar{k})$.

Let $\mathrm{EV} = \{\lambda_1, \dots, \lambda_s\}$ be the set of eigenvalues of γ. Recall the decomposition

$$\mathbb{A}^{N+1}(\bar{k}) = L_1 \oplus \cdots \oplus L_s, \quad L_i = \mathrm{Ker}(\gamma - \lambda_i)^{m_i}, \ i = 1, \dots, s,$$

where m_i is the maximum exponent such that $(x - \lambda_i)^{m_i}$ divides the minimal polynomial of γ. Each L_i is γ-invariant and $\exp L_i = p^{\delta_i}$, with $\delta_i = \lceil \log_p(m_i) \rceil$.

Let $\mathbf{D}_{\mathbb{N}}$ be the poset of positive integers ordered by divisibility. Let $\mathbf{B}$ be the poset of non-empty subsets of EV ordered by inclusion. For each $\Lambda \in \mathbf{B}$ we define two invariants, $\delta(\Lambda)$, $D(\Lambda)$, in the form of two morphisms of posets

$$\begin{aligned} &\delta : \mathbf{B} \to \mathbb{N}, \qquad D : \mathbf{B} \to \mathbf{D}_{\mathbb{N}}, \\ &\delta(\Lambda) := \max\bigl\{\bigl\lceil \log_p(m_i) \bigr\rceil \bigm| \lambda_i \in \Lambda\bigr\} = \max\{\delta_i \mid \lambda_i \in \Lambda\}, \\ &D\bigl(\{\lambda_{i_1}, \dots, \lambda_{i_t}\}\bigr) := \mathrm{ord}\bigl(\mathrm{diag}(\lambda_{i_1}, \dots, \lambda_{i_t})\bigr) = \min\bigl\{d \bigm| \lambda_{i_1}^d = \lambda_{i_2}^d = \cdots = \lambda_{i_t}^d\bigr\}. \end{aligned} \tag{10}$$

Note that $D(\Lambda)$ is always prime to p.

Definition 5.2. We say that $\Lambda \in \mathbf{B}$ is *D-proper* if Λ is maximal among all nodes with the same value of D:

$$D(\Lambda) < D(\Delta), \quad \forall \Delta \in \mathbf{B} \text{ such that } \Lambda < \Delta.$$

We denote by $\mathbf{B}^{\mathrm{pr}}$ the subposet of the D-proper nodes of $\mathbf{B}$.

The following remark is obvious.

Lemma 5.3. *The γ-invariant linear spaces of $\mathbb{A}^{N+1}(\bar{k})$ are all of the form $M = M_1 \oplus \cdots \oplus M_s$, with $M_i \subseteq L_i$ γ-invariant. If each M_i has exponent $\exp M_i = p^{\epsilon_i}$, $\epsilon_i \leqslant \delta_i$, then $\exp M = p^{\epsilon} D(\Lambda_M)$, where $\epsilon = \max\{\epsilon_i\}$ and $\Lambda_M := \{\lambda_i \in \mathrm{EV} \mid M_i \neq 0\}$.*

For any $0 \leqslant \nu \leqslant \delta_i$ the subspace $\mathrm{Ker}(\gamma - \lambda_i)^{p^\nu}$ is the maximum γ-invariant subspace of L_i with exponent p^ν. The following result follows immediately.

Lemma 5.4. *For each pair (Λ, ν) with $\Lambda \in \mathbf{B}$ and $0 \leqslant \nu \leqslant \delta(\Lambda)$, consider the γ-invariant linear subvariety of $\mathbb{P}^N(\bar{k})$:*

$$L_\Lambda^{(\nu)} := \bigoplus_{\lambda \in \Lambda} \operatorname{Ker}(\gamma - \lambda)^{p^\nu}.$$

Then $\exp(L_\Lambda^{(\nu)}) = p^\nu D(\Lambda)$, and this subvariety $L_\Lambda^{(\nu)}$ contains all γ-invariant subvarieties M such that $\Lambda_M \subseteq \Lambda$ and $v_p(\exp M) \leqslant \nu$.

Note that for any $\Lambda \in \mathbf{B}$ with invariants $D = D(\Lambda)$, $\delta = \delta(\Lambda)$, we have a chain of nodes of the poset $\mathcal{L}$ with respective exponents $D, pD, \dots, p^\delta D$:

$$L_\Lambda^{(0)} < L_\Lambda^{(1)} < \cdots < L_\Lambda^{(\delta)}.$$

Theorem 5.5. *A node $L \in \mathcal{L}$ is proper if and only if $L = L_\Lambda^{(\nu)}$ for some $\Lambda \in \mathbf{B}$ which is D-proper, and some $0 \leqslant \nu \leqslant \delta(\Lambda)$.*

Proof. Suppose Λ is D-proper and let us show that $L_\Lambda^{(\nu)}$ is proper. Suppose that $L_\Lambda^{(\nu)} \subseteq M$ for some $M \in \mathcal{L}$ with $\exp(L_\Lambda^{(\nu)}) = \exp(M)$. In particular $D(\Lambda) = D(\Lambda_M)$ and this implies $\Lambda = \Lambda_M$ because Λ is D-proper. Hence, $M = L_\Lambda^{(\nu)}$ by Lemma 5.4.

Conversely, suppose M proper with $\exp M = p^\epsilon D(\Lambda_M)$. By Lemma 5.4 we have $M \subseteq L_{\Lambda_M}^{(\epsilon)}$ and this implies $M = L_{\Lambda_M}^{(\epsilon)}$ because M is proper. Finally, Λ_M is proper because $\Lambda_M \subsetneq \Lambda$, with $D(\Lambda_M) = D(\Lambda)$ would lead to $M = L_{\Lambda_M}^{(\epsilon)} \subsetneq L_\Lambda^{(\epsilon)}$ and M would not be proper. □

Corollary 5.6. *Let $\delta = \delta(\mathrm{EV})$ and let $[0, \delta]$ be the poset of integers $0 \leqslant \nu \leqslant \delta$ ordered by size. We have a natural identification:*

$$\mathcal{L}^{\mathrm{pr}} \hookrightarrow [0, \delta] \times \mathbf{B}^{\mathrm{pr}},$$

with image the subposet containing the nodes (ν, Λ) with $\nu \leqslant \delta(\Lambda)$. In particular, $\mathcal{L}^{\mathrm{pr}}$ is a finite poset. Moreover, $\mathcal{L}^{\mathrm{pr}}$ is a lattice.

Proof. The first statement is an immediate consequence of Theorem 5.5. In order to prove that $\mathcal{L}^{\mathrm{pr}}$ is a lattice it is sufficient to check that the subposet $\mathbf{B}^{\mathrm{pr}}$ is a lattice. The total set $\hat{1}$ is always proper; hence, by [12, 3.3.1] it is sufficient to check that the intersection of two D-proper elements is D-proper. Consider pairwise disjoint sets $\Lambda_0, \Lambda_1, \Lambda_2 \in \mathbf{B}$, such that $\Lambda_0 \cup \Lambda_1$ and $\Lambda_0 \cup \Lambda_2$ are D-proper. Let us show that Λ_0 is D-proper. If $D(\Lambda_0 \cup \{\lambda\}) = D(\Lambda_0)$, then

$$D(\Lambda_0 \cup \Lambda_1 \cup \{\lambda\}) = D(\Lambda_0 \cup \Lambda_1), \qquad D(\Lambda_0 \cup \Lambda_2 \cup \{\lambda\}) = D(\Lambda_0 \cup \Lambda_2).$$

Since these sets are D-proper we have $\lambda \in (\Lambda_0 \cup \Lambda_1) \cap (\Lambda_0 \cup \Lambda_2) = \Lambda_0$. □

We finish our study of the poset $\mathcal{L}^{\mathrm{pr}}$ with two basic properties of the proper linear varieties.

Lemma 5.7. *Two proper varieties of the same exponent are either disjoint or coincident.*

Proof. Suppose that $L, M \in \mathcal{L}^{\mathrm{pr}}$ have both exponent d, and $L \cap M \neq \emptyset$. The linear irreducible subvariety generated by L and M is γ-invariant; if we check that it has still exponent d we shall have necessarily $L = M$ by the properness of L and M. Now, all non-zero vectors of the affine cone of L are eigenvalues of the linear mapping γ^d; this implies that $\gamma^d(x) = \lambda x$ on this affine cone, for some uniform $\lambda \in \bar{k}$. Similarly, $\gamma^d(y) = \mu y$ on the affine cone of M for some $\mu \in \bar{k}$. Since these two cones have some non-zero vector in common we have necessarily $\lambda = \mu$ and γ^d is the identity on the linear irreducible subvariety generated by L and M. □

Lemma 5.8. *Let $L \in \mathcal{L}^{\mathrm{pr}}$ and suppose that for some point $P \in L$ the γ-orbit of P has e elements, with $e < \exp L$. Then, there is a proper linear variety $M \in \mathcal{L}^{\mathrm{pr}}$ with exponent e such that $P \in M \subsetneq L$.*

Proof. The positive integer e is the minimum exponent such that P is a fixed point of γ^e. Now, the linear irreducible subvariety M generated by $O_\gamma(P)$ is γ-invariant and it is pointwise fixed by γ^e. Hence, $e = \operatorname{ord}(\gamma_{|M}) = \exp M$.

Embed M in a (unique) proper subvariety with the same exponent:

$$M \subseteq M', \quad \exp M' = e, \quad M' \in \mathcal{L}^{\mathrm{pr}}.$$

Since L is proper and $\mathcal{L}^{\mathrm{pr}}$ is a lattice, we have necessarily $M' \subseteq L$. □

We are ready to prove Theorem 3.2. The poset $\mathcal{L}_G$ of G-linear arrangements (cf. Section 3.1) can be identified to the quotient poset of $\mathcal{L}$ under the Galois action. More precisely, we have an onto morphism of posets

$$\mathcal{L} \to \mathcal{L}_G, \qquad L \mapsto L \cup \sigma(L) \cup \cdots \cup \sigma^{r-1}(L), \quad r = \deg L.$$

Moreover, it follows easily from Lemma 5.7 that a node $V \in \mathcal{L}_G$ is proper in $\mathcal{L}_G$ if and only if one (actually all) of the irreducible components L is proper in $\mathcal{L}$. Hence, we have an induced onto morphism of posets $\mathcal{L}^{\mathrm{pr}} \to \mathcal{P}$ and we deduce from Corollary 5.6 that $\mathcal{P}$ is a finite lattice; this proves item (1) of Theorem 3.2.

Item (2) of Theorem 3.2 is a consequence of Lemma 5.8 and item (3) is a consequence of Theorem 1.2 and the following proposition.

Proposition 5.9. *Let V be a proper G-linear arrangement of G-degree r and let L be one of its irreducible components. Then, $\mathrm{Z}(V/k, t) = \mathrm{Z}(L/k_r, t^r)$.*

Proof. We want to prove the identity of formal series:

$$\sum_{m \geqslant 1} \frac{|V(k_m)|}{m} t^m = \sum_{n \geqslant 1} \frac{|L(k_{rn})|}{n} t^{rn}. \tag{11}$$

By Lemma 5.7 the varieties $\sigma^i(L)$ are pairwise disjoint, because they are all proper and have the same exponent. Since,

$$P \in V(k_m) \quad \Rightarrow \quad P \in \sigma^i(L), \qquad \sigma^m(P) = P \quad \Rightarrow \quad P \in \sigma^i(L) \cap \sigma^{i+m}(L),$$

we deduce that $V(k_m) = \emptyset$ if $r \nmid m$; hence, we can change m to rn in the left side of (11), and the equality holds because $|V(k_{rn})| = r|L(k_{rn})|$. □

Acknowledgments

We thank the referees for their accurate reports, that led to a substantial improvement in the presentation of the results. In particular, the elegant formulation and proof of Proposition 1.7 was suggested by one of the referees.

References

[1] J. Bergström, Point counts and the cohomology of moduli spaces of curves, Doctoral Thesis in Mathematics, Stockholm, Sweden, 2006.

[2] A. Betten, H. Fripertinger, A. Kerber, A. Wassermann, K.-H. Zimmermann, Codierungstheorie, Springer-Verlag, Berlin, 1998.

[3] C. Demirkiran, E. Nart, Counting hyperelliptic curves that admit a Koblitz model, http://www.arxiv.org/math.NT/07051423.

[4] I. Dolgachev, D. Ortland, Point sets in projective spaces and theta functions, Astérisque 188 (1988) (Soc. Math. of France, Paris).

[5] H. Fripertinger, Cycle indices of linear, affine and projective groups, Linear Algebra Appl. 263 (1997) 133–156.

[6] B.H. Gross, J. Harris, On some geometric constructions related to theta characteristics, in: Contributions to Automorphic Forms, Geometry and Number Theory, The Johns Hopkins University Press, 2004, pp. 279–311.

[7] A. López, E. Nart, Classification of Goppa codes of genus zero, J. Reine Angew. Math. 517 (1999) 131–144.

[8] A. López, D. Maisner, E. Nart, X. Xarles, Orbits of Galois invariant n-sets of $\mathbb{P}^1$ under the action of PGL_2, Finite Fields Appl. 8 (2002) 193–206.

[9] R. Martí, E. Nart, Isometry classes of codes arising from sets of points in the projective plane, European J. Combin. 25 (2004) 1003–1023.

[10] R. Martí, E. Nart, Enumeration of linear codes, in preparation.

[11] E. Nart, Counting hyperelliptic curves, http://www.arxiv.org/math.NT/0703549.

[12] R.P. Stanley, Enumerative Combinatorics, vol. I, Cambridge Stud. Adv. Math., vol. 62, Cambridge University Press, 1999.