DISCRETE ANALYSIS, 2020:4, 34 pp.
www.discreteanalysisjournal.com

On sets defining few ordinary hyperplanes

Aaron Lin Konrad Swanepoel

Received 26 April 2019; Revised 17 January 2020; Published 24 April 2020

Abstract: Let P be a set of n points in real projective d-space, not all contained in a hyperplane, such that any d points span a hyperplane. An ordinary hyperplane of P is a hyperplane containing exactly d points of P. We show that if $d \geqslant 4$, the number of ordinary hyperplanes of P is at least $\binom{n-1}{d-1} - O_d(n^{\lfloor (d-1)/2 \rfloor})$ if n is sufficiently large depending on d. This bound is tight, and given d, we can calculate the exact minimum number for sufficiently large n. This is a consequence of a structure theorem for sets with few ordinary hyperplanes: For any $d \geqslant 4$ and $K > 0$, if $n \geqslant C_d K^8$ for some constant $C_d > 0$ depending on d, and P spans at most $K\binom{n-1}{d-1}$ ordinary hyperplanes, then all but at most $O_d(K)$ points of P lie on a hyperplane, an elliptic normal curve, or a rational acnodal curve. We also find the maximum number of $(d+1)$-point hyperplanes, solving a d-dimensional analogue of the orchard problem. Our proofs rely on Green and Tao's results on ordinary lines, our earlier work on the 3-dimensional case, as well as results from classical algebraic geometry.

1 Introduction

An *ordinary line* of a set of points in the plane is a line passing through exactly two points of the set. The classical Sylvester–Gallai theorem states that every finite non-collinear point set in the plane spans at least one ordinary line. In fact, for sufficiently large n, an n-point non-collinear set in the plane spans at least $n/2$ ordinary lines, and this bound is tight if n is even. This was shown by Green and Tao [9] via a structure theorem characterising all finite point sets with few ordinary lines.

It is then natural to consider higher dimensional analogues. Motzkin [22] noted that there are finite non-coplanar point sets in 3-space that span no plane containing exactly three points of the set. He proposed considering instead hyperplanes Π in d-space such that all but one point contained in Π is contained in a $(d-2)$-dimensional flat of Π. The existence of such hyperplanes was shown by Motzkin [22] for 3-space and by Hansen [10] in higher dimensions.

DOI: 10.19086/da.11949

Purdy and Smith [25] considered instead finite non-coplanar point sets in 3-space with no three points collinear, and provided a lower bound on the number of planes containing exactly three points of the set. Referring to such a plane as an *ordinary plane*, Ball [1] proved a 3-dimensional analogue of Green and Tao's [9] structure theorem, and found the exact minimum number of ordinary planes spanned by sufficiently large non-coplanar point sets in real projective 3-space with no three points collinear. Using an alternative method, we [20] were able to prove a more detailed structure theorem but with a stronger condition; see Theorem 4.1 in Section 4.

Ball and Monserrat [3] made the following definition, generalising ordinary planes to higher dimensions.

Definition. An *ordinary hyperplane* of a set of points in real projective d-space, where every d points span a hyperplane, is a hyperplane passing through exactly d points of the set.

They [3] also proved bounds on the minimum number of ordinary hyperplanes spanned by such sets (see also [21]). Our first main result is a structure theorem for sets with few ordinary hyperplanes. The elliptic normal curves and rational acnodal curves mentioned in the theorem and their group structure will be described in Section 3. Our methods extend those in our earlier paper [20], and we detail them in Section 2.

Theorem 1.1. *Let $d \geqslant 4$, $K > 0$, and suppose $n \geqslant C\max\{(dK)^8, d^3 2^d K\}$ for some sufficiently large absolute constant $C > 0$. Let P be a set of n points in $\mathbb{RP}^d$ where every d points span a hyperplane. If P spans at most $K\binom{n-1}{d-1}$ ordinary hyperplanes, then P differs in at most $O(d2^d K)$ points from a configuration of one of the following types:*

(*i*) *A subset of a hyperplane;*

(*ii*) *A coset $H \oplus x$ of a subgroup H of an elliptic normal curve or the smooth points of a rational acnodal curve of degree $d+1$, for some x such that $(d+1)x \in H$.*

It is easy to show that conversely, a set of n points where every d span a hyperplane and differing from (*i*) or (*ii*) by $O(K)$ points, spans $O(K\binom{n-1}{d-1})$ ordinary hyperplanes. By [3, Theorem 2.4], if a set of n points where every d points span a hyperplane itself spans $K\binom{n-1}{d-1}$ ordinary hyperplanes, and is not contained in a hyperplane, then $K = \Omega(1/d)$. Theorem 1.2 below implies that $K \geqslant 1$ for sufficiently large n depending on d.

For a similar structure theorem in dimension 4 but with $K = o(n^{1/7})$, see Ball and Jimenez [2], who show that P lies on the intersection of five quadrics. Theorem 1.1 proves [2, Conjecture 12], noting that elliptic normal curves and rational acnodal curves lie on $\binom{d}{2} - 1$ linearly independent quadrics [6, Proposition 5.3; 17, p. 365]. We also mention that Monserrat [21, Theorem 2.10] proved a structure theorem stating that almost all points of the set lie on the intersection of $d-1$ hypersurfaces of degree at most 3.

Our second main result is a tight bound on the minimum number of ordinary hyperplanes, proving [3, Conjecture 3]. Note that our result holds only for sufficiently large n; see [3, 14, 21] for estimates when d is small or n is not much larger than d.

Theorem 1.2. *Let $d \geqslant 4$ and let $n \geqslant Cd^3 2^d$ for some sufficiently large absolute constant $C > 0$. The minimum number of ordinary hyperplanes spanned by a set of n points in $\mathbb{RP}^d$, not contained in a hyperplane and where every d points span a hyperplane, is*

$$\binom{n-1}{d-1} - O\left(d2^{-d/2}\binom{n}{\lfloor\frac{d-1}{2}\rfloor}\right).$$

This minimum is attained by a coset of a subgroup of an elliptic normal curve or the smooth points of a rational acnodal curve of degree $d+1$, and when $d+1$ and n are coprime, by $n-1$ points in a hyperplane together with a point not in the hyperplane.

Green and Tao [9] also used their structure theorem to solve the classical orchard problem of finding the maximum number of 3-point lines spanned by a set of n points in the plane, for n sufficiently large. We solved the 3-dimensional analogue in [20]. Our third main result is the d-dimensional analogue. We define a $(d+1)$-*point hyperplane* to be a hyperplane through exactly $d+1$ points of a given set.

Theorem 1.3. *Let $d \geqslant 4$ and let $n \geqslant Cd^3 2^d$ for some sufficiently large absolute constant $C > 0$. The maximum number of $(d+1)$-point hyperplanes spanned by a set of n points in $\mathbb{RP}^d$ where every d points span a hyperplane is*

$$\frac{1}{d+1}\binom{n-1}{d} + O\left(2^{-d/2}\binom{n}{\lfloor\frac{d-1}{2}\rfloor}\right).$$

This maximum is attained by a coset of a subgroup of an elliptic normal curve or the smooth points of a rational acnodal curve of degree $d+1$.

While the bounds in Theorems 1.2 and 1.3 are asymptotic, we provide a recursive method (as part of our proofs) to calculate the exact extremal values for a given d and n sufficiently large in Section 5. In principle, the exact values can be calculated for any given d and turns out to be a quasi-polynomial in n with a period of $d+1$. We present the values for $d = 4, 5, 6$ at the end of Section 5.

Relation to previous work

The main idea in our proof of Theorem 1.1 is to induct on the dimension d, with the base case $d = 3$ being our earlier structure theorem for sets defining few ordinary planes [20], which in turn is based on Green and Tao's Intermediate Structure Theorem for sets defining few ordinary lines [9, Proposition 5.3].

Roughly, the structure theorem in 3-space states that if a finite set of points is in general position (no three points collinear) and spans few ordinary planes, then most of the points must lie on a plane, two disjoint conics, or an elliptic or acnodal space quartic curve. In fact, we can define a group structure on these curves encoding when four points are coplanar, in which case our point set must be very close to a coset of the curve. (See Theorem 4.1 for a more precise statement.)

As originally observed by Ball [1] in 3-space, the general position condition allows the use of projection to leverage Green and Tao's Intermediate Structure Theorem [9, Proposition 5.3]. This avoids having to apply their Full Structure Theorem [9, Theorem 1.5], which has a much worse lower bound on n, as it avoids the technical Section 6 of [9], dealing with the case in the plane when most of the points lie on a large, though bounded, number of lines. On the other hand, to get to the precise coset structure,

we used additive-combinatorial results from [9, Section 7], specifically [9, Propositions A.5, Lemmas 7.2, 7.4, 7.7, and Corollary 7.6]. In this paper, the only result of Green and Tao [9] we explicitly use is [9, Proposition A.5], which we extend in Proposition 4.3, while all other results are subsumed in the structure theorem in 3-space. In dimensions $d > 3$, the general position condition also allows the use of projections from a point to a hyperplane (see also Ball and Monserrat [3]). In Section 2.2 we detail various technical results about the behaviour of curves under such projections, which are extensions of 3-dimensional results in [20].

While the group structure on elliptic or singular space quartic curves are well studied (see for instance [23]), we could not find references to the group structure on singular rational curves in higher dimensions. This is our main focus in Section 3, which in a way extends [20, Section 3]. In particular, we look at Sylvester's theorem on when a binary form can be written as a sum of perfect powers, which has its roots in classical invariant theory. In extending the results of [20, Section 3], we have to consider how to generalise the catalecticant (of a binary quartic form), which leads us to the secant variety of the rational normal curve as a determinantal variety.

Green and Tao's Intermediate Structure Theorem in 2-space has a slightly different flavour to their Full Structure Theorem, the structure theorem in 3-space, and Theorem 1.1. However, this is not the only reason why we start our induction at $d = 3$. A more substantial reason is that there are no smooth rational cubic curves in 2-space; as is well known, all rational planar cubic curves are singular. Thus, both smooth and singular rational quartics in 3-space project onto rational cubics, and we need some way to tell them apart. In higher dimensions, we have Lemma 3.7 to help us, but since this is false when $d = 3$, the induction from the plane to 3-space [20] is more technical. This is despite the superficial similarity between the 2- and 3-dimensional situations where there are two almost-extremal cases while there is essentially only one case when $d > 3$.

Proving Theorem 1.1, which covers the $d > 3$ cases, is thus in some sense less complicated, since not only are we leveraging a more detailed structure theorem (Theorems 1.1 and 4.1 as opposed to [9, Proposition 5.3]), we also lose a case. However, there are complications that arise in how to generalise and extend results from 2- and 3-space to higher dimensions.

2 Notation and tools

By $A = O(B)$, we mean there exists an absolute constant $C > 0$ such that $0 \leqslant A \leqslant CB$. Thus, $A = -O(B)$ means there exists an absolute constant $C > 0$ such that $-CB \leqslant A \leqslant 0$. We also write $A = \Omega(B)$ for $B = O(A)$. None of the $O(\cdot)$ and $\Omega(\cdot)$ statements in this paper have implicit dependence on the dimension d.

We write $A \triangle B$ for the symmetric difference of the sets A and B.

Let $\mathbb{F}$ denote the field of real or complex numbers, let $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$, and let $\mathbb{FP}^d$ denote the d-dimensional projective space over $\mathbb{F}$. We denote the homogeneous coordinates of a point in d-dimensional projective space by a $(d+1)$-dimensional vector $[x_0, x_1, \ldots, x_d]$. We call a linear subspace of dimension k in $\mathbb{FP}^d$ a *k-flat*; thus a point is a 0-flat, a line is a 1-flat, a plane is a 2-flat, and a hyperplane is a $(d-1)$-flat. We denote by $Z_{\mathbb{F}}(f)$ the set of $\mathbb{F}$-points of the algebraic hypersurface defined by the vanishing of a homogeneous polynomial $f \in \mathbb{F}[x_0, x_1, \ldots, x_d]$. More generally, we consider a (closed, projective) *variety* to be any intersection of algebraic hypersurfaces. We say that a variety is pure-dimensional if each of its

irreducible components has the same dimension. We consider a *curve* of degree e in $\mathbb{CP}^d$ to be a variety δ of pure dimension 1 such that a generic hyperplane in $\mathbb{CP}^d$ intersects δ in e distinct points. More generally, the degree of a variety $X \subset \mathbb{CP}^d$ of dimension r is

$$\deg(X) := \max\{|\Pi \cap X| : \Pi \text{ is a } (d-r)\text{-flat such that } \Pi \cap X \text{ is finite}\}.$$

We say that a curve is *non-degenerate* if it is not contained in a hyperplane, and *non-planar* if it is not contained in a 2-flat. We call a curve *real* if each of its irreducible components contains infinitely many points of $\mathbb{RP}^d$. Whenever we consider a curve in $\mathbb{RP}^d$, we implicitly assume that its Zariski closure is a real curve.

We denote the Zariski closure of a set $S \subseteq \mathbb{CP}^d$ by $\overline{S}$. We will use the *secant variety* $\mathrm{Sec}_{\mathbb{C}}(\delta)$ of a curve δ, which is the Zariski closure of the set of points in $\mathbb{CP}^d$ that lie on a line through some two points of δ.

2.1 Bézout's theorem

Bézout's theorem gives the degree of an intersection of varieties. While it is often formulated as an equality, in this paper we only need the weaker form that ignores multiplicity and gives an upper bound. The (set-theoretical) intersection $X \cap Y$ of two varieties is just the variety defined by $P_X \cup P_Y$, where X and Y are defined by the collections of homogeneous polynomials P_X and P_Y respectively.

Theorem 2.1 (Bézout [7, Section 2.3])**.** *Let X and Y be varieties in $\mathbb{CP}^d$ with no common irreducible component. Then* $\deg(X \cap Y) \leqslant \deg(X)\deg(Y)$.

2.2 Projections

Given $p \in \mathbb{FP}^d$, the *projection from p*, $\pi_p \colon \mathbb{FP}^d \setminus \{p\} \to \mathbb{FP}^{d-1}$, is defined by identifying $\mathbb{FP}^{d-1}$ with any hyperplane Π of $\mathbb{FP}^d$ not passing through p, and then letting $\pi_p(x)$ be the point where the line px intersects Π [11, Example 3.4]. Equivalently, π_p is induced by a surjective linear transformation $\mathbb{F}^{d+1} \to \mathbb{F}^d$ where the kernel is spanned by the vector p.

As in our previous paper [20], we have to consider projections of curves where we do not have complete freedom in choosing a generic projection point p.

Let $\delta \subset \mathbb{CP}^d$ be an irreducible non-planar curve of degree e, and let p be a point in $\mathbb{CP}^d$. We call π_p *generically one-to-one on* δ if there is a finite subset S of δ such that π_p restricted to $\delta \setminus S$ is one-to-one. (This is equivalent to the birationality of π_p restricted to $\delta \setminus \{p\}$ [11, p. 77].) If π_p is generically one-to-one, the degree of the curve $\overline{\pi_p(\delta \setminus \{p\})}$ is $e-1$ if p is a smooth point on δ, and is e if p does not lie on δ; if π_p is not generically one-to-one, then the degree of $\overline{\pi_p(\delta \setminus \{p\})}$ is at most $(e-1)/2$ if p lies on δ, and is at most $e/2$ if p does not lie on δ [11, Example 18.16], [18, Section 1.15].

The following three lemmas on projections are proved in [20] in the case $d = 3$. They all state that most projections behave well and can be considered to be quantitative versions of the trisecant lemma [15]. The proofs of Lemmas 2.3 and 2.4 are almost word-for-word the same as the proofs of the 3-dimensional cases in [20]. All three lemmas can also be proved by induction on the dimension $d \geqslant 3$ from the 3-dimensional case. We illustrate this by proving Lemma 2.2.

Lemma 2.2. *Let δ be an irreducible non-planar curve of degree e in $\mathbb{CP}^d$, $d \geqslant 3$. Then there are at most $O(e^4)$ points p on δ such that π_p restricted to $\delta \setminus \{p\}$ is not generically one-to-one.*

Proof. The case $d = 3$ was shown in [20], based on the work of Furukawa [8]. We next assume that $d \geqslant 4$ and that the lemma holds in dimension $d-1$. Since $d > 3$ and the dimension of $\mathrm{Sec}_{\mathbb{C}}(\delta)$ is at most 3 [11, Proposition 11.24], there exists a point $p \in \mathbb{CP}^d$ such that all lines through p have intersection multiplicity at most 1 with δ. It follows that the projection $\delta' := \overline{\pi_p(\delta)}$ of δ is a non-planar curve of degree e in $\mathbb{CP}^{d-1}$. Consider any line ℓ not through p that intersects δ in at least three distinct points p_1, p_2, p_3. Then $\pi_p(\ell)$ is a line in $\mathbb{CP}^{d-1}$ that intersects δ' in three points $\pi_p(p_1), \pi_p(p_2), \pi_p(p_3)$. It follows that if $x \in \delta$ is a point such that for all but finitely many points $y \in \delta$, the line xy intersects δ in a point other than x or y, then $x' := \pi_p(x)$ is a point such that for all but finitely many points $y' := \pi_p(y) \in \delta'$, the line $x'y'$ intersects δ' in a third point. That is, if π_x restricted to δ is not generically one-to-one, then the projection map $\pi_{x'}$ in $\mathbb{CP}^{d-1}$ restricted to δ' is not generically one-to-one. By the induction hypothesis, there are at most $O(e^4)$ such points and we are done. □

Lemma 2.3. *Let δ be an irreducible non-planar curve of degree e in $\mathbb{CP}^d$, $d \geqslant 3$. Then there are at most $O(e^3)$ points $x \in \mathbb{CP}^d \setminus \delta$ such that π_x restricted to δ is not generically one-to-one.*

Lemma 2.4. *Let δ_1 and δ_2 be two irreducible non-planar curves in $\mathbb{CP}^d$, $d \geqslant 3$, of degree e_1 and e_2 respectively. Then there are at most $O(e_1 e_2)$ points p on δ_1 such that $\overline{\pi_p(\delta_1 \setminus \{p\})}$ and $\overline{\pi_p(\delta_2 \setminus \{p\})}$ coincide.*

3 Curves of degree $d+1$

In this paper, irreducible non-degenerate curves of degree $d+1$ in $\mathbb{CP}^d$ play a fundamental role. Indeed, the elliptic normal curve and rational acnodal curve mentioned in Theorem 1.1 are both such curves. In this section, we describe their properties that we need. These properties are all classical, but we did not find a reference for the group structure on singular rational curves of degree $d+1$, and therefore consider this in detail.

It is well-known in the plane that there is a group structure on any smooth cubic curve or the set of smooth points of a singular cubic. This group has the property that three points sum to the identity if and only if they are collinear. Over the complex numbers, the group on a smooth cubic is isomorphic to the torus $(\mathbb{R}/\mathbb{Z})^2$, and the group on the smooth points of a singular cubic is isomorphic to $(\mathbb{C}, +)$ or $(\mathbb{C}^*, \cdot)$ depending on whether the singularity is a cusp or a node. Over the real numbers, the group on a smooth cubic is isomorphic to $\mathbb{R}/\mathbb{Z}$ or $\mathbb{R}/\mathbb{Z} \times \mathbb{Z}_2$ depending on whether the real curve has one or two semi-algebraically connected components, and the group on the smooth points of a singular cubic is isomorphic to $(\mathbb{R}, +)$, $(\mathbb{R}, +) \times \mathbb{Z}_2$, or $\mathbb{R}/\mathbb{Z}$ depending on whether the singularity is a cusp, a crunode, or an acnode. See for instance [9] for a more detailed description.

In higher dimensions, it turns out that an irreducible non-degenerate curve of degree $d+1$ does not necessarily have a natural group structure, but if it has, the behaviour is similar to the planar case. For instance, in $\mathbb{CP}^3$, an irreducible non-degenerate quartic curve is either an elliptic quartic, with a group isomorphic to an elliptic curve such that four points on the curve are coplanar if and only if they sum to the identity, or a rational curve. There are two types, or species, of rational quartics. The rational quartic

curves of the first species are intersections of two quadrics (as are elliptic quartics), they are always singular, and there is a group on the smooth points such that four points on the curve are coplanar if and only if they sum to the identity. Those of the second species lie on a unique quadric, are smooth, and there is no natural group structure analogous to the other cases. See [20] for a more detailed account. The picture is similar in higher dimensions.

Definition (Clifford [4], Klein [17])**.** An *elliptic normal curve* is an irreducible non-degenerate smooth curve of degree $d+1$ in $\mathbb{CP}^d$ isomorphic to an elliptic curve in the plane.

Proposition 3.1 ([28, Exercise 3.11 and Corollary 5.1.1], [29, Corollary 2.3.1])**.** *An elliptic normal curve δ in $\mathbb{CP}^d$, $d \geqslant 2$, has a natural group structure such that $d+1$ points in δ lie on a hyperplane if and only if they sum to the identity. This group is isomorphic to $(\mathbb{R}/\mathbb{Z})^2$.*

If the curve is real, then the group is isomorphic to $\mathbb{R}/\mathbb{Z}$ or $\mathbb{R}/\mathbb{Z}\times\mathbb{Z}_2$ depending on whether the real curve has one or two semi-algebraically connected components.

A similar result holds for singular rational curves of degree $d+1$. Since we need to work with such curves and a description of their group structure is not easily found in the literature, we give a detailed discussion of their properties in the remainder of this section.

A *rational curve* δ in $\mathbb{FP}^d$ of degree e is a curve that can be parametrised by the projective line,

$$\delta\colon \mathbb{FP}^1 \to \mathbb{FP}^d, \quad [x,y] \mapsto [q_0(x,y),\dots,q_d(x,y)],$$

where each q_i is a homogeneous polynomial of degree e in the variables x and y. The following lemma is well known (see for example [27, p. 38, Theorem VIII]), and can be proved by induction from the planar case using projection.

Proposition 3.2. *An irreducible non-degenerate curve of degree $d+1$ in $\mathbb{CP}^d$, $d \geqslant 2$, is either an elliptic normal curve or rational.*

We next describe when an irreducible non-degenerate rational curve of degree $d+1$ in $\mathbb{CP}^d$ has a natural group structure. It turns out that this happens if and only if the curve is singular.

We write ν_{d+1} for the *rational normal curve* in $\mathbb{CP}^{d+1}$ [11, Example 1.14], which we parametrise as

$$\nu_{d+1} : [x,y] \mapsto [y^{d+1}, -xy^d, x^2y^{d-1}, \dots, (-x)^{d-1}y^2, (-x)^d y, (-x)^{d+1}].$$

Any irreducible non-degenerate rational curve δ of degree $d+1$ in $\mathbb{CP}^d$ is the projection of the rational normal curve, and we have

$$\delta[x,y] = [y^{d+1}, -xy^d, x^2y^{d-1}, \dots, (-x)^{d-1}y^2, (-x)^d y, (-x)^{d+1}]A,$$

where A is a $(d+2)\times(d+1)$ matrix of rank $d+1$ (since δ is non-degenerate) with entries derived from the coefficients of the polynomials q_i of degree $d+1$ in the parametrisation of the curve (with suitable alternating signs). Thus $\delta \subset \mathbb{CP}^d$ is the image of ν_{d+1} under the projection map π_p defined by A. In particular, the point of projection $p = [p_0, p_1, \dots, p_{d+1}] \in \mathbb{CP}^{d+1}$ is the (1-dimensional) kernel of A. If we project ν_{d+1} from a point $p \in \nu_{d+1}$, then we obtain a rational normal curve in $\mathbb{CP}^d$. However, since δ is of degree $d+1$, necessarily $p \notin \nu_{d+1}$. Conversely, it can easily be checked that for any $p \notin \nu_{d+1}$, the projection of ν_{d+1} from p is a rational curve of degree $d+1$ in $\mathbb{CP}^d$. We will use the notation δ_p for this curve. We summarise the above discussion in the following proposition that will be implicitly used in the remainder of the paper.

Proposition 3.3. *An irreducible non-degenerate rational curve of degree $d+1$ in $\mathbb{CP}^d$ is projectively equivalent to δ_p for some $p \in \mathbb{CP}^{d+1} \setminus \nu_{d+1}$.*

We use the projection point p to define a binary form and a multilinear form associated to δ_p. The *fundamental binary form* associated to δ_p is the homogeneous polynomial of degree $d+1$ in two variables $f_p(x,y) := \sum_{i=0}^{d+1} p_i \binom{d+1}{i} x^{d+1-i} y^i$. Its *polarisation* is the multilinear form $F_p \colon (\mathbb{F}^2)^{d+1} \to \mathbb{F}$ [5, Section 1.2] defined by

$$F_p(x_0,y_0,x_1,y_1,\ldots,x_d,y_d) := \frac{1}{(d+1)!} \sum_{I \subseteq \{0,1,\ldots,d\}} (-1)^{d+1-|I|} f_p\left(\sum_{i\in I} x_i, \sum_{i\in I} y_i\right).$$

Consider the multilinear form $G_p(x_0,y_0,\ldots,x_d,y_d) = \sum_{i=0}^{d+1} p_i P_i$, where

$$P_i(x_0,y_0,x_1,y_1,\ldots,x_d,y_d) := \sum_{I \in \binom{\{0,1,\ldots,d\}}{i}} \prod_{j\in \bar{I}} x_j \prod_{j\in I} y_j \tag{1}$$

for each $i = 0,\ldots,d+1$. Here the sum is taken over all subsets I of $\{0,1,\ldots,d\}$ of size i, and $\bar{I}$ denotes the complement of I in $\{0,1,\ldots,d\}$. It is easy to see that the binary form f_p is the *restitution* of G_p, namely [5, Section 1.2]

$$f_p(x,y) = G_p(x,y,x,y,\ldots,x,y).$$

Since the polarisation of the restitution of a multilinear form is itself [5, Section 1.2], we must thus have $F_p = G_p$. (This can also be checked directly.)

Lemma 3.4. *Let δ_p be an irreducible non-degenerate rational curve of degree $d+1$ in $\mathbb{CP}^d$, $d \geqslant 2$, where $p \in \mathbb{CP}^{d+1} \setminus \nu_{d+1}$. A hyperplane intersects δ_p in $d+1$ points $\delta_p[x_i,y_i]$, $i = 0,\ldots,d$, counting multiplicity, if and only if $F_p(x_0,y_0,x_1,y_1,\ldots,x_d,y_d) = 0$.*

Proof. We first prove the statement for distinct points $[x_i,y_i] \in \mathbb{CP}^1$. Then the points $\delta_p[x_i,y_i]$ are all on a hyperplane if and only if the hyperplane in $\mathbb{CP}^{d+1}$ through the points $\nu_{d+1}[x_i,y_i]$ passes through p. It will be sufficient to prove the identity

$$D := \det \begin{pmatrix} \nu_{d+1}[x_0,y_0] \\ \vdots \\ \nu_{d+1}[x_d,y_d] \\ p \end{pmatrix} = F_p(x_0,y_0,x_1,y_1,\ldots,x_d,y_d) \prod_{0\leqslant j<k\leqslant d} \begin{vmatrix} x_j & x_k \\ y_j & y_k \end{vmatrix}, \tag{2}$$

since the second factor on the right-hand side does not vanish because the points $[x_i,y_i]$ are distinct. We first note that

$$D = \begin{vmatrix} y_0^{d+1} & -x_0y_0^d & x_0^2y_0^{d-1} & \ldots & (-x_0)^d y_0 & (-x_0)^{d+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ y_d^{d+1} & -x_dy_d^d & x_d^2y_d^{d-1} & \ldots & (-x_d)^d y_d & (-x_d)^{d+1} \\ p_0 & p_1 & p_2 & \cdots & p_d & p_{d+1} \end{vmatrix}$$

$$= (-1)^{\lfloor \frac{d+2}{2} \rfloor} \begin{vmatrix} y_0^{d+1} & x_0 y_0^d & x_0^2 y_0^{d-1} & \dots & x_0^d y_0 & x_0^{d+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ y_d^{d+1} & x_d y_d^d & x_d^2 y_d^{d-1} & \dots & x_d^d y_d & x_d^{d+1} \\ p_0 & -p_1 & p_2 & \dots & (-1)^d p_d & (-1)^{d+1} p_{d+1} \end{vmatrix}. \tag{3}$$

We next replace $(-1)^i p_i$ by $x^i y^{d+1-i}$ for each $i = 0, \dots, d+1$ in the last row of the determinant in (3) and obtain the Vandermonde determinant

$$\begin{aligned} &(-1)^{\lfloor \frac{d+2}{2} \rfloor} \begin{vmatrix} y_0^{d+1} & x_0 y_0^d & x_0^2 y_0^{d-1} & \dots & x_0^d y_0 & x_0^{d+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ y_d^{d+1} & x_d y_d^d & x_d^2 y_d^{d-1} & \dots & x_d^d y_d & x_d^{d+1} \\ y^{d+1} & xy^d & x^2 y^{d-1} & \dots & x^d y & x^{d+1} \end{vmatrix} \\ &= (-1)^{\lfloor \frac{d+2}{2} \rfloor} \prod_{0 \leqslant j < k \leqslant d} \begin{vmatrix} y_j & y_k \\ x_j & x_k \end{vmatrix} \prod_{0 \leqslant j \leqslant d} \begin{vmatrix} y_j & y \\ x_j & x \end{vmatrix} \\ &= (-1)^{\lfloor \frac{d+2}{2} \rfloor} (-1)^{\binom{d+2}{2}} \prod_{0 \leqslant j < k \leqslant d} \begin{vmatrix} x_j & x_k \\ y_j & y_k \end{vmatrix} \prod_{0 \leqslant j \leqslant d} \begin{vmatrix} x_j & x \\ y_j & y \end{vmatrix}. \end{aligned}$$

Finally, note that $(-1)^{\lfloor (d+2)/2 \rfloor} (-1)^{\binom{d+2}{2}} = 1$ and that the coefficient of $x^i y^{d+1-i}$ in $\prod_{0 \leqslant j \leqslant d} \begin{vmatrix} x_j & x \\ y_j & y \end{vmatrix}$ is

$$\sum_{I \subseteq \binom{\{0,\dots,d\}}{i}} \prod_{j \in I} (-y_j) \prod_{j \in \overline{I}} x_j = (-1)^i P_i,$$

where P_i is as defined in (1). It follows that the coefficient of p_i in (3) is P_i, and (2) follows.

We next complete the argument for the case when the points $[x_i, y_i]$ are not all distinct. First suppose that a hyperplane Π intersects δ_p in $\delta_p[x_i, y_i]$, $i = 0, \dots, d$. By Bertini's theorem [12, Theorem II.8.18 and Remark II.8.18.1], there is an arbitrarily close perturbation Π' of Π that intersects δ_p in distinct points $\delta_p[x_i', y_i']$. By what has already been proved, $F_p(x_0', y_0', \dots, x_d', y_d') = 0$. Since Π' is arbitrarily close and F_p is continuous, $F_p[x_0, y_0, \dots, x_d, y_d] = 0$.

Conversely, suppose that $F_p(x_0, y_0, \dots, x_d, y_d) = 0$ where the $[x_i, y_i]$ are not all distinct. Perturb the points $[x_0, y_0], \dots, [x_{d-1}, y_{d-1}]$ by an arbitrarily small amount to $[x_0', y_0'], \dots, [x_{d-1}', y_{d-1}']$ respectively, so as to make $\delta_p[x_0', y_0'], \dots, \delta_p[x_{d-1}', y_{d-1}']$ span a hyperplane Π' that intersects δ_p again in $\delta_p[x_d', y_d']$, say, and so that $[x_0', y_0'], \dots, [x_d', y_d']$ are all distinct. If we take the limit as $[x_i', y_i'] \to [x_i, y_i]$ for each $i = 0, \dots, d-1$, we obtain a hyperplane Π intersecting δ_p in $\delta_p[x_0, y_0], \dots, \delta_p[x_{d-1}, y_{d-1}], \delta_p[x_d'', y_d'']$, say. Then $F_p(x_0, y_0, \dots, x_{d-1}, y_{d-1}, x_d'', y_d'') = 0$. Since the multilinear form F_p is non-trivial, it follows that $[x_d, y_d] = [x_d'', y_d'']$. Therefore, Π is a hyperplane that intersects δ_p in $\delta_p[x_i, y_i]$, $i = 0, \dots, d$. □

The secant variety $\mathrm{Sec}_{\mathbb{C}}(\nu_{d+1})$ of the rational normal curve ν_{d+1} in $\mathbb{CP}^{d+1}$ is equal to the set of points that lie on a proper secant or tangent line of ν_{d+1}, that is, on a line with intersection multiplicity at least 2 with ν_{d+1}. We also define the real secant variety of ν_{d+1} to be the set $\mathrm{Sec}_{\mathbb{R}}(\nu_{d+1})$ of points in $\mathbb{RP}^{d+1}$ that lie on a line that either intersects ν_{d+1} in two distinct real points or is a tangent line of ν_{d+1}. The *tangent variety* $\mathrm{Tan}_{\mathbb{F}}(\nu_{d+1})$ of ν_{d+1} is defined to be the set of points in $\mathbb{FP}^{d+1}$ that lie on a tangent line

of ν_{d+1}. We note that although $\mathrm{Tan}_{\mathbb{R}}(\nu_{d+1}) = \mathrm{Tan}_{\mathbb{C}}(\nu_{d+1}) \cap \mathbb{RP}^{d+1}$, we only have a proper inclusion $\mathrm{Sec}_{\mathbb{R}}(\nu_{d+1}) \subset \mathrm{Sec}_{\mathbb{C}}(\nu_{d+1}) \cap \mathbb{RP}^{d+1}$ for $d \geqslant 2$.

We will need a concrete description of $\mathrm{Sec}_{\mathbb{C}}(\nu_{d+1})$ and its relation to the smoothness of the curves δ_p. For any $p \in \mathbb{FP}^{d+1}$ and $k = 2, \ldots, d-1$, define the $(k+1) \times (d-k+2)$ matrix

$$M_k(p) := \begin{pmatrix} p_0 & p_1 & p_2 & \cdots & p_{d-k+1} \\ p_1 & p_2 & p_3 & \cdots & p_{d-k+2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p_k & p_{k+1} & p_{k+2} & \cdots & p_{d+1} \end{pmatrix}.$$

Suppose that δ_p has a double point, say $\delta_p[x_0, y_0] = \delta_p[x_1, y_1]$. This is equivalent to p, $\nu_{d+1}[x_0, y_0]$, and $\nu_{d+1}[x_1, y_1]$ being collinear, which is equivalent to p being on the secant variety of ν_{d+1}. (In the degenerate case where $[x_0, y_0] = [x_1, y_1]$, we have that $p \in \mathrm{Tan}_{\mathbb{F}}(\nu_{d+1})$.) Then $\delta_p[x_0, y_0]$, $\delta_p[x_1, y_1]$, $\delta_p[x_2, y_2]$,..., $\delta_p[x_d, y_d]$ are on a hyperplane in $\mathbb{FP}^d$ for all $[x_2, y_2], \ldots, [x_d, y_d] \in \mathbb{FP}^1$. It follows that the coefficients of $F_p(x_0, y_0, x_1, y_1, x_2, y_2, \ldots, x_d, y_d)$ as a polynomial in $x_2, y_2, \ldots, x_d, y_d$ all vanish, that is,

$$p_i x_0 x_1 + p_{i+1}(x_0 y_1 + y_0 x_1) + p_{i+2} y_0 y_1 = 0$$

for all $i = 0, \ldots, d-1$. This can be written as $[x_0 x_1, x_0 y_1 + y_0 x_1, y_0 y_1] M_2(p) = 0$. Conversely, if $M_2(p)$ has rank 2 with say $[c_0, 2c_1, c_2] M_2(p) = 0$, then there is a non-trivial solution to the linear system with $c_0 = x_0 x_1$, $c_1 = x_0 y_1 + y_0 x_1$, $c_2 = y_0 y_1$, and we have $c_0 x^2 + 2c_1 xy + c_2 y^2 = (x_0 x + y_0 y)(x_1 x + y_1 y)$. In the degenerate case where $[x_0, y_0] = [x_1, y_1]$, we have that the quadratic form has repeated roots.

It follows that $M_2(p)$ has rank at most 2 if and only if $p \in \mathrm{Sec}_{\mathbb{C}}(\nu_{d+1})$ (also note that $M_2(p)$ has rank 1 if and only if $p \in \nu_{d+1}$). We note for later use that since the null space of $M_2(p)$ is 1-dimensional if it has rank 2, it follows that each $p \in \mathrm{Sec}_{\mathbb{C}}(\nu_{d+1})$ lies on a unique secant (which might degenerate to a tangent). This implies that δ_p has a unique singularity when $p \in \mathrm{Sec}_{\mathbb{C}}(\nu_{d+1}) \setminus \nu_{d+1}$, which is a node if $p \in \mathrm{Sec}_{\mathbb{C}}(\nu_{d+1}) \setminus \mathrm{Tan}_{\mathbb{C}}(\nu_{d+1})$ and a cusp if $p \in \mathrm{Tan}_{\mathbb{C}}(\nu_{d+1}) \setminus \nu_{d+1}$. In the real case there are two types of nodes. If $p \in \mathrm{Sec}_{\mathbb{R}}(\nu_{d+1}) \setminus \nu_{d+1}$, then the roots $[x_0, y_0], [x_1, y_1]$ are real, and δ_p has either a cusp when $p \in \mathrm{Tan}_{\mathbb{R}}(\nu_{d+1}) \setminus \nu_{d+1}$ and $[x_0, y_0] = [x_1, y_1]$, or a crunode when $p \in \mathrm{Sec}_{\mathbb{R}}(\nu_{d+1}) \setminus \mathrm{Tan}_{\mathbb{R}}(\nu_{d+1})$ and $[x_0, y_0]$ and $[x_1, y_1]$ are distinct roots of the real binary quadratic form $c_0 x^2 + 2c_1 xy + c_2 y^2$. If $p \in \mathrm{Sec}_{\mathbb{C}}(\nu_{d+1}) \setminus \mathrm{Sec}_{\mathbb{R}}(\nu_{d+1}) \cap \mathbb{RP}^{d+1}$ then the quadratic form has conjugate roots $[x_0, y_0] = [\overline{x_1}, \overline{y_1}]$ and δ_p has an acnode.

If $p \notin \mathrm{Sec}(\nu_{d+1})$, then δ_p is a smooth curve of degree $d+1$. It follows that δ_p is singular if and only if $p \in \mathrm{Sec}(\nu_{d+1}) \setminus \nu_{d+1}$. For the purposes of this paper, we make the following definitions.

Definition. A *rational singular curve* is an irreducible non-degenerate singular rational curve of degree $d+1$ in $\mathbb{CP}^d$. In the real case, a *rational cuspidal curve*, *rational crunodal curve*, or *rational acnodal curve* is a rational singular curve isomorphic to a singular planar cubic with a cusp, crunode, or acnode respectively.

In particular, we have shown the case $k = 2$ of the following well-known result.

Proposition 3.5 ([11, Proposition 9.7])**.** *Let $d \geqslant 3$. For any $k = 2, \ldots, d-1$, the secant variety of ν_{d+1} is equal to the locus of all $[p_0, p_1, \ldots, p_{d+1}]$ such that $M_k(p)$ has rank at most 2.*

Corollary 3.6. *Let $d \geqslant 3$. For any $k = 2, \dots, d-1$ and $p \in \mathbb{CP}^{d+1} \setminus \nu_{d+1}$, the curve δ_p of degree $d+1$ in $\mathbb{CP}^d$ is singular if and only if* $\operatorname{rank} M_k(p) \leqslant 2$.

We next use Corollary 3.6 to show that the projection of a smooth rational curve of degree $d+1$ in $\mathbb{CP}^d$ from a generic point on the curve is again smooth when $d \geqslant 4$. This is not true for $d = 3$, as there is a trisecant through each point of a quartic curve of the second species in 3-space. (The union of the trisecants form the unique quadric on which the curve lies [11, Exercise 8.13].)

Lemma 3.7. *Let δ_p be a smooth rational curve of degree $d+1$ in $\mathbb{CP}^d$, $d \geqslant 4$. Then for all but at most three points $q \in \delta_p$, the projection $\overline{\pi_q(\delta_p \setminus \{q\})}$ is a smooth rational curve of degree d in $\mathbb{CP}^{d-1}$.*

Proof. Let $q = \delta_p[x_0, y_0]$. Suppose that $\overline{\pi_q(\delta_p \setminus \{q\})}$ is singular. Then there exist $[x_1, y_1]$ and $[x_2, y_2]$ such that $\pi_q(\delta_p[x_1, y_1]) = \pi_q(\delta_p[x_2, y_2])$ and the points $\delta_p[x_0, y_0]$, $\delta_p[x_1, y_1]$, and $\delta_p[x_2, y_2]$ are collinear. Then for arbitrary $[x_3, y_3], \dots, [x_d, y_d] \in \mathbb{CP}^1$, the points $\delta_p[x_i, y_i]$, $i = 0, \dots, d$ are on a hyperplane, so by Lemma 3.4, $F_p(x_0, y_0, \dots, x_d, y_d)$ is identically 0 as a polynomial in $x_3, y_3, \dots, x_d, y_d$. The coefficients of this polynomial are of the form

$$p_i x_0 x_1 x_2 + p_{i+1}(x_0 x_1 y_2 + x_0 y_1 x_2 + y_0 x_1 x_2) + p_{i+2}(x_0 y_1 y_2 + y_0 x_1 y_2 + y_0 y_1 x_2) + p_{i+3} y_0 y_1 y_2$$

for $i = 0, \dots, d-2$. This means that the linear system $[c_0, 3c_1, 3c_2, c_3] M_3(p) = 0$ has a non-trivial solution $c_0 = x_0 x_1 x_2$, $3c_1 = x_0 x_1 y_2 + x_0 y_1 x_2 + y_0 x_1 x_2$, $3c_2 = x_0 y_1 y_2 + y_0 x_1 y_2 + y_0 y_1 x_2$, $c_3 = y_0 y_1 y_2$. The binary cubic form $c_0 x^3 + 3c_1 x^2 y + c_2 x y^2 + c_3 y^3$ then has the factorisation $(x_0 x + y_0 y)(x_1 x + y_1 y)(x_2 x + y_2 y)$, hence its roots give the collinear points on δ_p. Since δ_p is smooth, $M_3(p)$ has rank at least 3 by Corollary 3.6, and so the cubic form is unique up to scalar multiples. It follows that there are at most three points q such that the projection $\overline{\pi_q(\delta_p \setminus \{q\})}$ is not smooth. □

We need the following theorem on the fundamental binary form f_p that is essentially due to Sylvester [30] to determine the natural group structure on rational singular curves. Reznick [26] gives an elementary proof of the generic case where p does not lie on the tangent variety. (See also Kanev [16, Lemma 3.1] and Iarrobino and Kanev [13, Section 1.3].) We provide a very elementary proof that includes the non-generic case.

Theorem 3.8 (Sylvester [30])**.** *Let $d \geqslant 2$.*

(*i*) *If $p \in \operatorname{Tan}_{\mathbb{C}}(\nu_{d+1})$, then there exist binary linear forms L_1, L_2 such that $f_p(x, y) = L_1(x, y)^d L_2(x, y)$. Moreover, if $p \notin \nu_{d+1}$ then L_1 and L_2 are linearly independent, and if $p \in \mathbb{RP}^{d+1}$ then L_1 and L_2 are both real.*

(*ii*) *If $p \in \operatorname{Sec}_{\mathbb{C}}(\nu_{d+1}) \setminus \operatorname{Tan}_{\mathbb{C}}(\nu_{d+1})$, then there exist linearly independent binary linear forms L_1, L_2 such that $f_p(x, y) = L_1(x, y)^{d+1} - L_2(x, y)^{d+1}$. Moreover, if $p \in \mathbb{RP}^{d+1} \setminus \operatorname{Sec}_{\mathbb{R}}(\nu_{d+1})$ then L_1 and L_2 are complex conjugates, while if $p \in \operatorname{Sec}_{\mathbb{R}}(\nu_{d+1})$ then there exist linearly independent real binary linear forms L_1, L_2 such that $f_p(x, y) = L_1(x, y)^{d+1} \pm L_2(x, y)^{d+1}$, where we can always choose the lower sign when d is even, and otherwise depends on p.*

Proof. (*i*): We work over $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$. Let $p = [p_0, p_1, \ldots, p_{d+1}] \in \mathrm{Tan}_{\mathbb{F}}(\nu_{d+1})$. Let $p_* = \nu_{d+1}[\alpha_1, \alpha_2]$ be the point on ν_{d+1} such that the line pp_* is tangent to ν_{d+1} (if $p \in \nu_{d+1}$, we let $p_* = p$). We will show that

$$f_p(x,y) = \sum_{i=0}^{d+1} p_i \binom{d+1}{i} x^{d+1-i} y^i = (\alpha_2 x - \alpha_1 y)^d (\beta_2 x - \beta_1 y) \tag{4}$$

for some $[\beta_1, \beta_2] \in \mathbb{FP}^1$.

First consider the special case $\alpha_1 = 0$. Then $p_* = [1, 0, \ldots, 0]$ and the tangent to ν_{d+1} at p_* is the line $x_2 = x_3 = \cdots = x_{d+1} = 0$. It follows that $f_p(x,y) = p_0 x^{d+1} + p_1(d+1)x^d y = (1x - 0y)^d (p_0 x + p_1(d+1)y)$. If $p_1 = 0$, then $p = p_* \in \nu_{d+1}$. Thus, if $p \notin \nu_{d+1}$, then $p_1 \neq 0$, and x and $p_0 x + p_1(d+1)y$ are linearly independent.

We next consider the general case $\alpha_1 \neq 0$. Equating coefficients in (4), we see that we need to find $[\beta_1, \beta_2]$ such that

$$p_i \binom{d+1}{i} = \binom{d}{i} \alpha_2^{d-i} (-\alpha_1)^i \beta_2 - \binom{d}{i-1} \alpha_2^{d-i+1} (-\alpha_1)^{i-1} \beta_1$$

for each $i = 0, \ldots, d+1$, where we use the convention $\binom{d}{-1} = \binom{d}{d+1} = 0$. This can be simplified to

$$p_i = \left(1 - \frac{i}{d+1}\right) \alpha_2^{d-i} (-\alpha_1)^i \beta_2 - \frac{i}{d+1} \alpha_2^{d-i+1} (-\alpha_1)^{i-1} \beta_1. \tag{5}$$

Since we are working projectively, we can fix the value of β_1 from the instance $i = d+1$ of (5) to get

$$p_{d+1} = -(-\alpha_1)^d \beta_1. \tag{6}$$

If $p_{d+1} \neq 0$, we can divide (5) by (6). After setting $\alpha = \alpha_2/\alpha_1$, $\beta = \beta_2/\beta_1$, and $a_i = p_i/p_{d+1}$, we then have to show that for some $\beta \in \mathbb{F}$,

$$a_i = -\left(1 - \frac{i}{d+1}\right) (-\alpha)^{d-i} \beta + \frac{i}{d+1} (-\alpha)^{d-i+1} \tag{7}$$

for each $i = 0, \ldots, d$. We next calculate in the affine chart $x_{d+1} = 1$ where the rational normal curve becomes $\nu_{d+1}(t) = ((-t)^{d+1}, (-t)^d, \ldots, -t)$, $p = (a_0, \ldots, a_d)$, and $p_* = \nu_{d+1}(\alpha)$. The tangency condition means that $p_* - p$ is a scalar multiple of

$$\nu'_{d+1}(\alpha) = ((d+1)(-\alpha)^d, d(-\alpha)^{d-1}, \ldots, 2\alpha, -1),$$

that is, we have for some $\lambda \in \mathbb{F}$ that $(-\alpha)^{d+1-i} - a_i = \lambda(d+1-i)(-\alpha)^{d-i}$ for all $i = 0, \ldots, d$. Set $\beta = \alpha + \lambda(d+1)$. Then $(-\alpha)^{d+1-i} - a_i = (\beta - \alpha)(1 - \frac{i}{d+1})(-\alpha)^{d-i}$, and we have

$$\begin{aligned} a_i &= (-\alpha)^{d+1-i} - (\beta - \alpha)\left(1 - \frac{i}{d+1}\right)(-\alpha)^{d-i} \\ &= -\left(1 - \frac{i}{d+1}\right)(-\alpha)^{d-i}\beta + \frac{i}{d+1}(-\alpha)^{d-i+1}, \end{aligned}$$

giving (7) as required. If $\alpha=\beta$, then $\lambda=0$ and $p=p_*\in\nu_{d+1}$. Thus, if $p\notin\nu_{d+1}$, then $\alpha\neq\beta$, and $\alpha_2x-\alpha_1y$ and $\beta_2x-\beta_1y$ are linearly independent.

We still have to consider the case $p_{d+1}=0$. Then $\beta_1=0$ and we need to find β_2 such that

$$p_i=\left(1-\frac{i}{d+1}\right)\alpha_2^{d-i}(-\alpha_1)^i\beta_2 \tag{8}$$

for all $i=0,\dots,d$. Since $p_{d+1}=0$, we have that $\nu'_{d+1}(\alpha)$ is parallel to $(p_0,\dots,p_d)$, that is,

$$p_i=\lambda(d+1-i)(-\alpha)^{d-i}$$

for some $\lambda\in\mathbb{F}^*$. Set $\beta_2=\lambda(d+1)/(-\alpha_1)^d$. Then

$$p_i=\frac{(-\alpha_1)^d\beta_2}{d+1}(d+1-i)\left(\frac{\alpha_2}{-\alpha_1}\right)^{d-i}=\left(1-\frac{i}{d+1}\right)\alpha_2^{d-i}(-\alpha_1)^i\beta_2,$$

again giving (8) as required. Note that since $\alpha_1\neq0$ but $\beta_1=0$, $\alpha_2x-\alpha_1y$ and $\beta_2x-\beta_1y$ are linearly independent. Note also that since $\lambda\neq0$, we have $\beta_2\neq0$ and $p\neq[1,0,\dots,0]$, hence $p\notin\nu_{d+1}$.

(ii): Let $p=[p_0,\dots,p_{d+1}]\in\mathrm{Sec}_{\mathbb{C}}(\nu_{d+1})\setminus\mathrm{Tan}_{\mathbb{C}}(\nu_{d+1})$, and suppose that p lies on the secant line through the distinct points $p_1:=\nu_{d+1}[\alpha_1,\alpha_2]$ and $p_2:=\nu_{d+1}[\beta_1,\beta_2]$. Since p,p_1,p_2 are distinct and collinear, there exist $\mu_1,\mu_2\in\mathbb{C}^*$ such that $p=\mu_1p_1+\mu_2p_2$. This means that for $i=0,\dots,d+1$, we have

$$p_i=\mu_1(-\alpha_1)^i\alpha_2^{d+1-i}+\mu_2(-\beta_1)^i\beta_2^{d+1-i}.$$

Then

$$\begin{aligned}
f_p(x,y)&=\sum_{i=0}^{d+1}p_i\binom{d+1}{i}x^{d+1-i}y^i\\
&=\mu_1\sum_{i=0}^{d+1}\binom{d+1}{i}(\alpha_2x)^{d+1-i}(-\alpha_1y)^i+\mu_2\sum_{i=0}^{d+1}\binom{d+1}{i}(\beta_2x)^{d+1-i}(-\beta_1y)^i\\
&=\mu_1(\alpha_2x-\alpha_1y)^{d+1}+\mu_2(\beta_2x-\beta_1y)^{d+1}\\
&=L_1(x,y)^{d+1}-L_2(x,y)^{d+1}
\end{aligned}$$

where the linear forms L_1,L_2 are linearly independent.

If $p\in\mathbb{RP}^{d+1}\setminus\mathrm{Sec}_{\mathbb{R}}(\nu_{d+1})$, then f_p is real and p_1 and p_2 are non-real points. Taking conjugates, we have

$$p=\overline{\mu_1}\nu_{d+1}[\overline{\alpha_1},\overline{\alpha_2}]+\overline{\mu_2}\nu_{d+1}[\overline{\beta_1},\overline{\beta_2}]$$

as vectors, and because of the uniqueness of secants of the rational normal curve through a given point, we obtain $\overline{\mu_1}=\mu_2$ and $\nu_{d+1}[\overline{\alpha_1},\overline{\alpha_2}]=\nu_{d+1}[\beta_1,\beta_2]$, hence $\overline{\alpha_1}=\beta_1$ and $\overline{\alpha_2}=\beta_2$. It follows that $\overline{L_1(x,y)}=L_2(\bar{x},\bar{y})$.

If $p\in\mathrm{Sec}_{\mathbb{R}}(\nu_{d+1})$, then p_1 and p_2 are real, so $[\mu_1,\mu_2],[\alpha_1,\alpha_2],[\beta_1,\beta_2]\in\mathbb{RP}^1$, and we obtain $f_p(x,y)=L_1^{d+1}\pm L_2^{d+1}$ for some linearly independent L_1,L_2 over $\mathbb{R}$, where the choice of sign depends on p. □

We are now in a position to describe the group laws on rational singular curves. We first note the effect of a change of coordinates on the parametrisation of δ_p. Let $\varphi\colon \mathbb{FP}^1 \to \mathbb{FP}^1$ be a projective transformation. Then $\nu_{d+1}\circ\varphi$ is a reparametrisation of the rational normal curve. It is not difficult to see that there exists a projective transformation $\psi\colon \mathbb{FP}^{d+1} \to \mathbb{FP}^{d+1}$ such that $\nu_{d+1}\circ\varphi = \psi\circ\nu_{d+1}$. It follows that if we reparametrise δ_p using φ, we obtain

$$\delta_p\circ\varphi = \pi_p\circ\nu_{d+1}\circ\varphi = \pi_p\circ\psi\circ\nu_{d+1} = \psi'\circ\pi_{\psi^{-1}(p)}\circ\nu_{d+1} \cong \delta_{\psi^{-1}(p)},$$

where $\psi'\colon \mathbb{FP}^d \to \mathbb{FP}^d$ is an appropriate projective transformation such that first transforming $\mathbb{FP}^{d+1}$ with ψ and then projecting from p is the same as projecting from $\psi^{-1}(p)$ and then transforming $\mathbb{FP}^d$ with ψ'. So by reparametrising δ_p, we obtain $\delta_{p'}$ for some other point p' that is in the orbit of p under the action of projective transformations that fix ν_{d+1}.

Since $\delta_p\circ\varphi[x_0,y_0],\dots,\delta_p\circ\varphi[x_d,y_d]$ lie on a hyperplane if and only if the $\delta_{\psi^{-1}(p)}[x_i,y_i]$'s are on a hyperplane, it follows from Lemma 3.4 that $F_p(\varphi(x_0,y_0),\dots,\varphi(x_d,y_d))$ is a scalar multiple of $F_{\psi^{-1}(p)}(x_0,y_0,\dots,x_d,y_d)$, in which case $f_p\circ\varphi = f_{\psi^{-1}(p)}$ up to a scalar multiple. Thus, we obtain the same reparametrisation of the fundamental binary form f_p.

Proposition 3.9. *A rational singular curve δ_p in $\mathbb{CP}^d$ has a natural group structure on its subset of smooth points δ_p^* such that $d+1$ points in δ_p^* lie on a hyperplane if and only if they sum to the identity. This group is isomorphic to $(\mathbb{C},+)$ if the singularity of δ_p is a cusp and isomorphic to $(\mathbb{C}^*,\cdot)$ if the singularity is a node.*

If the curve is real and cuspidal or acnodal, then it has a group isomorphic to $(\mathbb{R},+)$ or $\mathbb{R}/\mathbb{Z}$ depending on whether the singularity is a cusp or an acnode, such that $d+1$ points in δ_p^* lie on a hyperplane if and only if they sum to the identity. If the curve is real and the singularity is a crunode, then the group is isomorphic to $(\mathbb{R},+)\times\mathbb{Z}_2$, but $d+1$ points in δ_p^* lie on a hyperplane if and only if they sum to $(0,0)$ or $(0,1)$, depending on p.

Proof. First suppose δ_p is cuspidal and $\mathbb{F}\in\{\mathbb{R},\mathbb{C}\}$, so that $p\in \mathrm{Tan}_{\mathbb{F}}(\nu_{d+1})\setminus\nu_{d+1}$. By Theorem 3.8, $f_p = L_1^d L_2$ for some linearly independent linear forms L_1 and L_2. By choosing φ appropriately, we may assume without loss of generality that $L_1(x,y)=x$ and $L_2(x,y)=(d+1)y$, so that $f_p(x,y) = (d+1)x^d y$ and $p=[0,1,0,\dots,0]$, with the cusp of δ_p at $\delta_p[0,1]$. It follows that the polarisation of f_p is $F_p(x_0,y_0,\dots,x_d,y_d) = P_1 = x_0x_1\cdots x_d\sum_{i=0}^d y_i/x_i$. For $[x_i,y_i]\neq[0,1]$, $i=0,\dots,d$, the points $\delta_p[x_i,y_i]$ are on a hyperplane if and only if $\sum_{i=0}^d y_i/x_i = 0$. Thus we identify $\delta_p[x,y]\in\delta_p^*$ with $y/x\in\mathbb{F}$, and the group is $(\mathbb{F},+)$.

Next suppose δ_p is nodal, so that $p\in \mathrm{Sec}_{\mathbb{C}}(\nu_{d+1})\setminus\mathrm{Tan}_{\mathbb{C}}(\nu_{d+1})$. By Theorem 3.8, $f_p = L_1^{d+1} - L_2^{d+1}$ for some linearly independent linear forms L_1 and L_2. Again by choosing φ appropriately, we may assume without loss of generality that $L_1(x,y)=x$ and $L_2(x,y)=y$, so that $f_p(x,y)=x^{d+1}-y^{d+1}$ and $p=[1,0,\dots,0,-1]$, with the node of δ_p at $\delta_p[0,1]=\delta_p[1,0]$. The polarisation of f_p is $F_p(x_0,y_0,\dots,x_d,y_d) = P_0 - P_{d+1} = x_0x_1\cdots x_d - y_0y_1\cdots y_d$. Therefore, $\delta_p[x_i,y_i]$, $i=0,\dots,d$, are on a hyperplane if and only if $\prod_{i=0}^d y_i/x_i = 1$. Thus we identify $\delta_p[x,y]\in\delta_p^*$ with $y/x\in\mathbb{C}^*$, and the group is $(\mathbb{C}^*,\cdot)$.

Now suppose δ_p is real and the node is an acnode. Then the linearly independent linear forms L_1 and L_2 given by Theorem 3.8 are $L_1(x,y)=\alpha x+\beta y$ and $L_2(x,y)=\overline{\alpha}x+\overline{\beta}y$ for some $\alpha,\beta\in\mathbb{C}\setminus\mathbb{R}$. There exists $\varphi\colon\mathbb{RP}^1\to\mathbb{RP}^1$ such that $L_1\circ\varphi = x+iy$ and $L_2\circ\varphi = x-iy$, hence we may assume after such a reparametrisation that $f_p(x,y) = (x+iy)^{d+1} - (x-iy)^{d+1}$ and that the node is at $\delta_p[i,1]=\delta_p[-i,1]$.

The polarisation of f_p is $F_p(x_0,y_0,\dots,x_d,y_d) = \prod_{j=0}^d (x_j+iy_j) - \prod_{j=0}^d (x_j-iy_j)$, and it follows that $\delta_p[x_0,y_0],\dots,\delta_p[x_d,y_d]$ are collinear if and only if $\prod_{j=0}^d \frac{x_j+iy_j}{x_j-iy_j} = 1$. We now identify $\mathbb{RP}^1$ with the circle $\mathbb{R}/\mathbb{Z} \cong \{z \in \mathbb{C} : |z| = 1\}$ using the Möbius transformation $[x,y] \to \frac{x+iy}{x-iy}$.

It remains to consider the crunodal case. Then, similar to the complex nodal case, we obtain after a reparametrisation that $\delta_p[x_i,y_i]$, $i = 0,\dots,d$, are on a hyperplane if and only if $\prod_{i=0}^d y_i/x_i = \pm 1$, where the sign depends on p. Thus we identify $\delta_p[x,y] \in \delta_p^*$ with $y/x \in \mathbb{R}^*$, and the group is $(\mathbb{R}^*,\cdot) \cong \mathbb{R} \times \mathbb{Z}_2$, where $\pm 1 \in \mathbb{R}^*$ corresponds to $(0,0),(0,1) \in \mathbb{R} \times \mathbb{Z}_2$ respectively. □

The group on an elliptic normal curve or a rational singular curve of degree $d+1$ as described in Propositions 3.1 and 3.9 is not uniquely determined by the property that $d+1$ points lie on a hyperplane if and only if they sum to some fixed element c. Indeed, for any $t \in (\delta^*,\oplus)$, $x \boxplus y := x \oplus y \oplus t$ defines another abelian group on δ^* with the property that $d+1$ points lie on a hyperplane if and only if they sum to $c \oplus dt$. However, these two groups are isomorphic in a natural way with an isomorphism given by the translation map $x \mapsto x \ominus t$. The next proposition show that we always get uniqueness up to some translation. It will be used in Section 5.

Proposition 3.10. *Let $(G,\oplus,0)$ and $(G,\boxplus,0')$ be abelian groups on the same ground set, such that for some $d \geqslant 2$ and some $c,c' \in G$,*

$$x_1 \oplus \dots \oplus x_{d+1} = c \iff x_1 \boxplus \dots \boxplus x_{d+1} = c' \quad \text{for all } x_1,\dots,x_{d+1} \in G.$$

Then $(G,\oplus,0) \to (G,\boxplus,0'), x \mapsto x \boxminus 0 = x \oplus 0'$ is an isomorphism, and

$$c' = c \boxplus \underbrace{0 \boxplus \dots \boxplus 0}_{d \text{ times}} = c \ominus (\underbrace{0' \oplus \dots \oplus 0'}_{d \text{ times}}).$$

Proof. It is clear that the cases $d \geqslant 3$ follow from the case $d = 2$, which we now show. First note that for any $x,y \in G$, $x \boxplus y \boxplus (c \ominus x \ominus y) = c'$ and $(x \oplus y) \boxplus 0 \boxplus (c \ominus x \ominus y) = c'$, since $x \oplus y \oplus (c \ominus x \ominus y) = (x \oplus y) \oplus 0 \oplus (c \ominus x \ominus y) = c$. Thus we have $x \boxplus y = (x \oplus y) \boxplus 0$, hence $(x \oplus y) \boxminus 0 = x \boxplus y \boxminus 0 \boxminus 0 = (x \boxminus 0) \boxplus (y \boxminus 0)$. Similarly we have $x \oplus y = (x \boxplus y) \oplus 0'$, hence $x \boxplus y = x \oplus y \ominus 0'$, so in particular $0' = 0 \boxminus 0 = 0 \oplus (\boxminus 0) \ominus 0'$, and $\boxminus 0 = 0' \oplus 0'$. So we also have $x \boxminus 0 = x \oplus (\boxminus 0) \ominus 0' = x \oplus 0'$, and $(G,\oplus,0) \to (G,\boxplus,0'), x \mapsto x \boxminus 0 = x \oplus 0'$ is an isomorphism. □

4 Structure theorem

We prove Theorem 1.1 in this section. The main idea is to induct on the dimension d via projection. We start with the following statement of the slightly different case $d = 3$, which is [20, Theorem 1.1]. Note that it contains one more type that does not occur when $d \geqslant 4$.

Theorem 4.1. *Let $K > 0$ and suppose $n \geqslant C\max\{K^8,1\}$ for some sufficiently large absolute constant $C > 0$. Let P be a set of n points in $\mathbb{RP}^3$ with no 3 points collinear. If P spans at most Kn^2 ordinary planes, then up to projective transformations, P differs in at most $O(K)$ points from a configuration of one of the following types:*

(*i*) *A subset of a plane;*

(*ii*) *A subset of two disjoint conics lying on the same quadric with* $\frac{n}{2} \pm O(K)$ *points of* P *on each of the two conics;*

(*iii*) *A coset of a subgroup of the smooth points of an elliptic or acnodal space quartic curve.*

We first prove the following weaker lemma using results from Section 2.

Lemma 4.2. *Let* $d \geqslant 4$, $K > 0$, *and suppose* $n \geqslant C\max\{d^3 2^d K, (dK)^8\}$ *for some sufficiently large absolute constant* $C > 0$. *Let* P *be a set of* n *points in* $\mathbb{RP}^d$ *where every* d *points span a hyperplane. If* P *spans at most* $K\binom{n-1}{d-1}$ *ordinary hyperplanes, then all but at most* $O(d2^d K)$ *points of* P *are contained in a hyperplane or an irreducible non-degenerate curve of degree* $d+1$ *that is either elliptic or rational and singular.*

Proof. We use induction on $d \geqslant 4$ to show that for all $K > 0$ and all $n \geqslant f(d,K)$, for all sets P of n points in $\mathbb{RP}^d$ with any d points spanning a hyperplane, if P has at most $K\binom{n-1}{d-1}$ ordinary hyperplanes, then all but at most $g(d,K)$ points of P are contained in a hyperplane or an irreducible non-degenerate curve of degree $d+1$, and that if the curve is rational then it has to be singular, where

$$g(d,K) := \sum_{k=0}^{d} k^3 2^{d-k} + C_1 2^d (d-1)K$$

and

$$f(d,K) := d^2(g(d,K) + C_2 d^{10}) + C(d-1)^8 K^8$$

for appropriate $C_1, C_2 > 0$ to be determined later and C from Theorem 4.1. We assume that this holds in $\mathbb{RP}^{d-1}$ if $d \geqslant 5$, while Theorem 4.1 takes the place of the induction hypothesis when $d = 4$.

Let P' denote the set of points $p \in P$ such that there are at most $\frac{d-1}{d-2}K\binom{n-2}{d-2}$ ordinary hyperplanes through p. By counting incident point-ordinary-hyperplane pairs, we obtain

$$dK\binom{n-1}{d-1} > (n - |P'|)\frac{d-1}{d-2}K\binom{n-2}{d-2},$$

which gives $|P'| > n/(d-1)^2$. For any $p \in P'$, the projected set $\pi_p(P \setminus \{p\})$ has $n-1$ points and spans at most $\frac{d-1}{d-2}K\binom{n-2}{d-2}$ ordinary $(d-2)$-flats in $\mathbb{RP}^{d-1}$, and any $d-1$ points of $\pi_p(P \setminus \{p\})$ span a $(d-2)$-flat. To apply the induction hypothesis, we need

$$f(d,K) \geqslant 1 + f(d-1, \tfrac{d-1}{d-2}K),$$

as well as $f(3,K) \geqslant C\max\{K^8, 1\}$, both of which easily follow from the definition of $f(d,K)$. Then all except $g(d-1, \frac{d-1}{d-2}K)$ points of $\pi_p(P \setminus \{p\})$ are contained in a $(d-2)$-flat or a non-degenerate curve γ_p of degree d in $\mathbb{RP}^{d-1}$, which is either irreducible or possibly two conics with $\frac{n}{2} \pm O(K)$ points on each when $d = 4$.

If there exists a $p \in P'$ such that all but at most $g(d-1, \frac{d-1}{d-2}K)$ points of $\pi_p(P \setminus \{p\})$ are contained in a $(d-2)$-flat, then we are done, since $g(d,K) > g(d-1, \frac{d-1}{d-2}K)$. Thus we may assume without loss of generality that for all $p \in P'$ we obtain a curve γ_p.

Let p and p' be two distinct points of P'. Then all but at most $2g(d-1,\frac{d-1}{d-2}K)$ points of P lie on the intersection δ of the two cones $\overline{\pi_p^{-1}(\gamma_p)}$ and $\overline{\pi_{p'}^{-1}(\gamma_{p'})}$. Since the curves γ_p and $\gamma_{p'}$ are 1-dimensional, the two cones are 2-dimensional. Since their vertices p and p' are distinct, the cones do not have a common irreducible component, so their intersection is a variety of dimension at most 1. By Bézout's theorem (Theorem 2.1), δ has total degree at most d^2, so has to have at least one 1-dimensional irreducible component. Let $\delta_1,\dots,\delta_k$ be the 1-dimensional components of δ, where $1\leqslant k\leqslant d^2$. Let δ_1 be the component with the most points of P' amongst all the δ_i, so that

$$|P'\cap\delta_1|\geqslant\frac{|P'|-2g(d-1,\frac{d-1}{d-2}K)}{d^2}.$$

Choose a $q\in P'\cap\delta_1$ such that π_q is generically one-to-one on δ_1. By Lemma 2.2 there are at most $O(\deg(\delta_1)^4)=O(d^8)$ exceptional points, so we need

$$|P'\cap\delta_1|>C_2d^8. \tag{9}$$

Since $|P'|>n/(d-1)^2$, we need

$$\frac{\frac{n}{(d-1)^2}-2g(d-1,\frac{d-1}{d-2}K)}{d^2}>C_2d^8,$$

or equivalently, $n>(d-1)^2(2g(d-1,\frac{d-1}{d-2}K)+C_2d^{10})$. However, this follows from the definition of $f(d,K)$. If π_q does not map $\delta_1\setminus\{q\}$ into γ_q, then by Bézout's theorem (Theorem 2.1), $n-1-g(d-1,\binom{d-1}{d-2}K)\leqslant d^3$. However, this does not occur since $f(d,K)>g(d-1,\binom{d-1}{d-2}K)+d^3+1$. Thus, π_q maps $\delta_1\setminus\{q\}$ into γ_q, hence δ_1 is an irreducible curve of degree $d+1$ (or, when $d=4$, possibly a twisted cubic containing at most $n/2+O(K)$ points of P).

We first consider the case where δ_1 has degree $d+1$. We apply Lemma 2.4 to δ_1 and each δ_i, $i=2,\dots,k$, and for this we need $|P'\cap\delta_1|>C''d^4$, since $\deg(\delta_1)\leqslant d^2$ and $\sum_{i=2}^d\deg(\delta_i)\leqslant d^2$. However, this condition is implied by (9). Thus we find a $q'\in P'\cap\delta_1$ such that $\overline{\pi_{q'}(\delta_1\setminus\{q'\})}=\gamma_{q'}$ as before, and in addition, the cone $\overline{\pi_{q'}^{-1}(\gamma_{q'})}$ does not contain any other δ_i, $i=2,\dots,k$. Since all points of P except $2g(d-1,\frac{d-1}{d-2}K)+d^2$ lie on $\delta_1\cup\dots\cup\delta_k$, we obtain by Bézout's theorem (Theorem 2.1) that

$$|P\setminus\delta_1|\leqslant d(d^2-d-1)+d^2+2g(d-1,\tfrac{d-1}{d-2}K)<g(d,K).$$

We next dismiss the case where $d=4$ and δ_1 is a twisted cubic. We redefine P' to be the set of points $p\in P$ such that there are at most $12Kn^2$ ordinary hyperplanes through p. Then $|P'|\geqslant 2n/3$. Since we have $|P\cap\delta_1|\leqslant n/2+O(K)$, by Lemma 2.3 there exists $q'\in P'\setminus\delta_1$ such that the projection from q' will map δ_1 onto a twisted cubic in $\mathbb{RP}^3$. However, by Bézout's theorem (Theorem 2.1) and Theorem 4.1, $\pi_{q'}(\delta_1\setminus\{q'\})$ has to be mapped onto a conic, which gives a contradiction.

Note that $g(d,K)=O(d2^dK)$ since $K=\Omega(1/d)$ by [3, Theorem 2.4]. We have shown that all but $O(d2^dK)$ points of P are contained in a hyperplane or an irreducible non-degenerate curve δ of degree $d+1$. By Proposition 3.2, this curve is either elliptic or rational. It remains to show that if δ is rational, then it has to be singular. Similar to what was shown above, we can find more than 3 points $p\in\delta$ for which the projection $\overline{\pi_p(\delta\setminus\{p\})}$ is a rational curve of degree d that is singular by the induction hypothesis. Lemma 3.7 now implies that δ is singular. □

To get the coset structure on the curves as stated in Theorem 1.1, we use a simple generalisation of an additive combinatorial result used by Green and Tao [9, Proposition A.5]. This captures the principle that if a finite subset of a group is almost closed, then it is close to a subgroup. The case $d = 3$ was shown in [19].

Lemma 4.3. *Let $d \geqslant 2$. Let $A_1, A_2, \dots, A_{d+1}$ be $d+1$ subsets of some abelian group $(G, \oplus)$, all of size within K of n, where $K \leqslant cn/d^2$ for some sufficiently small absolute constant $c > 0$. Suppose there are at most Kn^{d-1} d-tuples $(a_1, a_2, \dots, a_d) \in A_1 \times A_2 \times \cdots \times A_d$ for which $a_1 \oplus a_2 \oplus \cdots \oplus a_d \notin A_{d+1}$. Then there is a subgroup H of G and cosets $H \oplus x_i$ for $i = 1, \dots, d$ such that*

$$|A_i \triangle (H \oplus x_i)|, \left| A_{d+1} \triangle \left(H \oplus \bigoplus_{i=1}^{d} x_i \right) \right| = O(K).$$

Proof. We use induction on $d \geqslant 2$ to show that the symmetric differences in the conclusion of the lemma have size at most $C \prod_{i=1}^{d} (1 + \frac{1}{i^2}) K$ for some sufficiently large absolute constant $C > 0$. The base case $d = 2$ is [9, Proposition A.5].

Fix a $d \geqslant 3$. By the pigeonhole principle, there exists $b_1 \in A_1$ such that there are at most

$$\frac{1}{n-K} K n^{d-1} \leqslant \frac{1}{1 - \frac{c}{d^2}} K n^{d-2}$$

$(d-1)$-tuples $(a_2, \dots, a_d) \in A_2 \times \cdots \times A_d$ for which $b_1 \oplus a_2 \oplus \cdots \oplus a_d \notin A_{d+1}$, or equivalently $a_2 \oplus \cdots \oplus a_d \notin A_{d+1} \ominus b_1$. Since

$$\frac{1}{1 - \frac{c}{d^2}} K \leqslant \frac{c}{d^2 - c} n \leqslant \frac{c}{(d-1)^2} n,$$

we can use induction to get a subgroup H of G and $x_2, \dots, x_d \in G$ such that for $j = 2, \dots, d$ we have

$$|A_j \triangle (H \oplus x_j)|, \left| (A_{d+1} \ominus b_1) \triangle \left(H \oplus \bigoplus_{j=2}^{d} x_j \right) \right| \leqslant C \prod_{i=1}^{d-1} \left(1 + \frac{1}{i^2} \right) \frac{1}{1 - \frac{c}{d^2}} K.$$

Since $|A_d \cap (H \oplus x_d)| \geqslant n - K - C \prod_{i=1}^{d-1} (1 + \frac{1}{i^2}) \frac{1}{1 - \frac{c}{d^2}} K$, we repeat the same pigeonhole argument on $A_d \cap (H \oplus x_d)$ to find a $b_d \in A_d \cap (H \oplus x_d)$ such that there are at most

$$\begin{aligned}
\frac{1}{n - K - C \prod_{i=1}^{d-1} \left(1 + \frac{1}{i^2}\right) \frac{1}{1 - \frac{c}{d^2}} K} K n^{d-1} &\leqslant \frac{1}{1 - \frac{c}{d^2} - C \prod_{i=1}^{d-1} \left(1 + \frac{1}{i^2}\right) \frac{c}{d^2 - c}} K n^{d-2} \\
&\leqslant \frac{1}{1 - C_1 \frac{c}{d^2 - c}} K n^{d-2} \\
&\leqslant \left(1 + \frac{C_2 c}{d^2 - c} \right) K n^{d-2} \\
&\leqslant \left(1 + \frac{1}{d^2} \right) K n^{d-2}
\end{aligned}$$

$(d-1)$-tuples $(a_1,\dots,a_{d-1}) \in A_1 \times \cdots A_{d-1}$ with $a_1 \oplus \cdots \oplus a_{d-1} \oplus b_d \notin A_{d+1}$, for some absolute constants $C_1, C_2 > 0$ depending on C, by making c sufficiently small. Now $(1+\frac{1}{d^2})K \leqslant cn/(d-1)^2$, so by induction again, there exist a subgroup H' of G and elements $x_1, x_2', \dots, x_{d-1}' \in G$ such that for $k = 2, \dots, d-1$ we have

$$|A_1 \triangle (H' \oplus x_1)|, |A_k \triangle (H' \oplus x_k')|, \left| (A_{d+1} \ominus b_d) \triangle \left(H' \oplus x_1 \oplus \bigoplus_{k=2}^{d-1} x_k' \right) \right| \leqslant C \prod_{i=1}^{d-1} \left(1 + \frac{1}{i^2}\right) \left(1 + \frac{1}{d^2}\right) K.$$

From this, it follows that $|(H \oplus x_k) \cap (H' \oplus x_k')| \geqslant n - K - 2C\prod_{i=1}^{d}(1+\frac{1}{i^2})K = n - O(K)$. Since $(H \oplus x_k) \cap (H' \oplus x_k')$ is non-empty, it has to be a coset of $H' \cap H$. If $H' \neq H$, then $|H' \cap H| \leqslant n/2 + O(K)$, a contradiction since c is sufficiently small. Therefore, $H = H'$, and $H \oplus x_k = H' \oplus x_k'$. So we have

$$|A_i \triangle (H \oplus x_i)|, \left| A_{d+1} \triangle \left(H \oplus \bigoplus_{\ell=1}^{d-1} x_\ell \oplus b_d \right) \right| \leqslant C \prod_{i=1}^{d} \left(1 + \frac{1}{i^2}\right) K.$$

Since $b_d \in H \oplus x_d$, we also obtain

$$\left| A_{d+1} \triangle \left(H \oplus \bigoplus_{i=1}^{d} x_i \right) \right| \leqslant C \prod_{i=1}^{d} \left(1 + \frac{1}{i^2}\right) K. \qquad \square$$

To apply Lemma 4.3, we first need to know that removing K points from a set does not change the number of ordinary hyperplanes it spans by too much.

Lemma 4.4. *Let P be a set of n points in $\mathbb{RP}^d$, $d \geqslant 2$, where every d points span a hyperplane. Let P' be a subset that is obtained from P by removing at most K points. If P spans m ordinary hyperplanes, then P' spans at most $m + \frac{1}{d}K\binom{n-1}{d-1}$ ordinary hyperplanes.*

Proof. Fix a point $p \in P$. Since every d points span a hyperplane, there are at most $\binom{n-1}{d-1}$ sets of d points from P containing p that span a hyperplane through p. Thus, the number of $(d+1)$-point hyperplanes through p is at most $\frac{1}{d}\binom{n-1}{d-1}$, since a set of $d+1$ points that contains p has d subsets of size d that contain p. If we remove points of P one-by-one to obtain P', we thus create at most $\frac{1}{d}K\binom{n-1}{d-1}$ ordinary hyperplanes. $\square$

The following lemma then translates the additive combinatorial Lemma 4.3 to our geometric setting.

Lemma 4.5. *Let $d \geqslant 4$, $K > 0$, and suppose $n \geqslant C(d^3K + d^4)$ for some sufficiently large absolute constant $C > 0$. Let P be a set of n points in $\mathbb{RP}^d$ where every d points span a hyperplane. Suppose P spans at most $K\binom{n-1}{d-1}$ ordinary hyperplanes, and all but at most dK points of P lie on an elliptic normal curve or a rational singular curve δ. Then P differs in at most $O(dK + d^2)$ points from a coset $H \oplus x$ of a subgroup H of δ^*, the smooth points of δ, for some x such that $(d+1)x \in H$. In particular, δ is either an elliptic normal curve or a rational acnodal curve.*

Proof. Let $P' = P \cap \delta^*$. Then by Lemma 4.4, P' spans at most $K\binom{n-1}{d-1} + d\frac{1}{d}K\binom{n-1}{d-1} = 2K\binom{n-1}{d-1}$ ordinary hyperplanes.

First suppose δ is an elliptic normal curve or a rational cuspidal or acnodal curve. If $a_1,\dots,a_d \in \delta^*$ are distinct, then by Propositions 3.1 and 3.9, the hyperplane through $a_1,\dots,a_d$ meets δ again in the unique point $a_{d+1} = \ominus(a_1 \oplus \cdots \oplus a_d)$. This implies that $a_{d+1} \in P'$ for all but at most $d!O(K\binom{n-1}{d-1})$ d-tuples $(a_1,\dots,a_d) \in (P')^d$ with all a_i distinct. There are also at most $\binom{d}{2}n^{d-1}$ d-tuples $(a_1,\dots,a_d) \in (P')^d$ for which the a_i are not all distinct. Thus, $a_1 \oplus \cdots \oplus a_d \in \ominus P'$ for all but at most $O((dK+d^2)n^{d-1})$ d-tuples $(a_1,\dots,a_d) \in (P')^d$. Applying Lemma 4.3 with $A_1 = \cdots = A_d = P'$ and $A_{d+1} = \ominus P'$, we obtain a finite subgroup H of δ^* and a coset $H \oplus x$ such that $|P' \triangle (H \oplus x)| = O(dK+d^2)$ and $|\ominus P' \triangle (H \oplus dx)| = O(dK+d^2)$, the latter being equivalent to $|P' \triangle (H \ominus dx)| = O(dK+d^2)$. Thus we have $|(H \oplus x) \triangle (H \ominus dx)| = O(dK+d^2)$, which implies $(d+1)x \in H$. Also, δ cannot be cuspidal, otherwise by Proposition 3.9 we have $\delta^* \cong (\mathbb{R},+)$, which has no finite subgroup of order greater than 1.

Now suppose δ is a rational crunodal curve. By Proposition 3.9, there is a bijective map $\varphi : (\mathbb{R},+) \times \mathbb{Z}_2 \to \delta^*$ such that $d+1$ points in δ^* lie in a hyperplane if and only if they sum to h, where $h = \varphi(0,0)$ or $\varphi(0,1)$ depending on the curve δ. If $h = \varphi(0,0)$ then the above argument follows through, and we obtain a contradiction as we have by Proposition 3.9 that $\delta^* \cong (\mathbb{R},+) \times \mathbb{Z}_2$, which has no finite subgroup of order greater than 2. Otherwise, the hyperplane through distinct $a_1,\dots,a_d \in \delta^*$ meets δ again in the unique point $a_{d+1} = \varphi(0,1) \ominus (a_1 \oplus \cdots \oplus a_d)$. As before, this implies that $a_{d+1} \in P'$ for all but at most $O((dK+d^2)n^{d-1})$ d-tuples $(a_1,\dots,a_d) \in (P')^d$, or equivalently $a_1 \oplus \cdots \oplus a_d \in \varphi(0,1) \ominus P'$. Applying Lemma 4.3 with $A_1 = \cdots = A_d = P'$ and $A_{d+1} = \varphi(0,1) \ominus P'$, we obtain a finite subgroup H of δ^*, giving a contradiction as before. □

We can now prove Theorem 1.1.

Proof of Theorem 1.1. By Lemma 4.2, all but at most $O(d2^dK)$ points of P are contained in a hyperplane or an irreducible curve δ of degree $d+1$ that is either elliptic or rational and singular. In the prior case, we get Case (*i*) of the theorem, so suppose we are in the latter case. We then apply Lemma 4.5 to obtain Case (*ii*) of the theorem, completing the proof. □

5 Extremal configurations

We prove Theorems 1.2 and 1.3 in this section. It will turn out that minimising the number of ordinary hyperplanes spanned by a set is equivalent to maximising the number of $(d+1)$-point planes, thus we can apply Theorem 1.1 in both theorems. Then we only have two cases to consider, where most of our point set is contained either in a hyperplane or a coset of a subgroup of an elliptic normal curve or the smooth points of a rational acnodal curve.

The first case is easy, and we get the following lower bound.

Lemma 5.1. *Let $d \geqslant 4$, $K \geqslant 1$, and let $n \geqslant 2dK$. Let P be a set of n points in $\mathbb{RP}^d$ where every d points span a hyperplane. If all but K points of P lie on a hyperplane, then P spans at least $\binom{n-1}{d-1}$ ordinary hyperplanes, with equality if and only if $K = 1$.*

Proof. Let Π be a hyperplane with $|P \cap \Pi| = n-K$. Since $n-K > d$, any ordinary hyperplane spanned by P must contain at least one point not in Π. Let m_i be the number of hyperplanes containing exactly

$d-1$ points of $P\cap\Pi$ and exactly i points of $P\setminus\Pi$, $i=1,\dots,K$. Then the number of unordered d-tuples of elements from P with exactly $d-1$ elements in Π is

$$K\binom{n-K}{d-1}=m_1+2m_2+3m_3+\cdots+Km_K.$$

Now consider the number of unordered d-tuples of elements from P with exactly $d-2$ elements in Π, which equals $\binom{K}{2}\binom{n-K}{d-2}$. One way to generate such a d-tuple is to take one of the m_i hyperplanes containing i points of $P\setminus\Pi$ and $d-1$ points of $P\cap\Pi$, choose two of the i points, and remove one of the $d-1$ points. Since any d points span a hyperplane, there is no overcounting. This gives

$$\begin{aligned}\binom{K}{2}\binom{n-K}{d-2}&\geqslant(d-1)\left(\binom{2}{2}m_2+\binom{3}{2}m_3+\binom{4}{2}m_4+\cdots\right)\\&\geqslant\frac{d-1}{2}(2m_2+3m_3+4m_4+\cdots).\end{aligned}$$

Hence the number of ordinary hyperplanes is at least

$$m_1\geqslant K\binom{n-K}{d-1}-\frac{K(K-1)}{d-1}\binom{n-K}{d-2}=K\binom{n-K}{d-1}\frac{n-2K-d+3}{n-K-d+2}.$$

We next show that for all $K\geqslant 2$, if $n\geqslant 2dK$ then

$$K\binom{n-K}{d-1}\frac{n-2K-d+3}{n-K-d+2}>\binom{n-1}{d-1}.$$

This is equivalent to

$$K>\frac{n-K+1}{n-2K-d+3}\prod_{i=1}^{K-2}\frac{n-i}{n-d-i+1}. \tag{10}$$

Note that

$$\frac{n-K+1}{n-2K-d+3}<2 \tag{11}$$

if $n>3K+2d-5$ and

$$\frac{n-i}{n-d-i+1}<\frac{i+2}{i+1} \tag{12}$$

if $n\geqslant(i+2)d$ for each $i=1,\dots,K-2$. However, since $2dK>(i+2)d$ and also $2dK>4K+2d-5$, the inequality (10) now follows from (11) and (12). □

The second case needs more work. We first consider the number of ordinary hyperplanes spanned by a coset of a subgroup of the smooth points δ^* of an elliptic normal curve or a rational acnodal curve. By Propositions 3.1 and 3.9, we can consider δ^* as a group isomorphic to either $\mathbb{R}/\mathbb{Z}$ or $\mathbb{R}/\mathbb{Z}\times\mathbb{Z}_2$. Let $H\oplus x$ be a coset of a subgroup H of δ^* of order n where $(d+1)x=\ominus c\in H$. Since H is a subgroup of order n of $\mathbb{R}/\mathbb{Z}$ or $\mathbb{R}/\mathbb{Z}\times\mathbb{Z}_2$, we have that either H is cyclic, or $\mathbb{Z}_{n/2}\times\mathbb{Z}_2$ when n is divisible by 4. The exact group will matter only when we make exact calculations.

Note that it follows from the group property that any d points on δ^* span a hyperplane. Also, since any hyperplane intersects δ^* in $d+1$ points, counting multiplicity, it follows that an ordinary

hyperplane of $H \oplus x$ intersects δ^* in d points, of which exactly one of them has multiplicity 2, and the others multiplicity 1. Denote the number of ordered k-tuples $(a_1, \dots, a_k)$ with distinct $a_i \in H$ that satisfy $m_1 a_1 \oplus \cdots \oplus m_k a_k = c$ by $[m_1, \dots, m_k; c]$. Then the number of ordinary hyperplanes spanned by $H \oplus x$ is

$$\frac{1}{(d-1)!}[2, \underbrace{1, \dots, 1}_{d-1 \text{ times}}; c]. \tag{13}$$

We show that we can always find a value of c for which (13) is at most $\binom{n-1}{d-1}$.

Lemma 5.2. *Let δ^* be an elliptic normal curve or the smooth points of a rational acnodal curve in $\mathbb{RP}^d$, $d \geqslant 2$. Then any finite subgroup H of δ^* of order n has a coset $H \oplus x$ with $(d+1)x \in H$, that spans at most $\binom{n-1}{d-1}$ ordinary hyperplanes. Furthermore, if $d+1$ and n are coprime, then any such coset spans exactly $\binom{n-1}{d-1}$ ordinary hyperplanes.*

Proof. It suffices to show that there exists $c \in H$ such that the number of solutions $(a_1, \dots, a_d) \in H^d$ of the equation $2a_1 \oplus a_2 \oplus \cdots \oplus a_d = c$, where $c = \ominus(d+1)x$, is at most $(d-1)!\binom{n-1}{d-1}$.

Fix a_1 and consider the substitution $b_i = a_i - a_1$ for $i = 2, \dots, d$. Note that $2a_1 \oplus \cdots \oplus a_d = c$ and $a_1, \dots, a_d$ are distinct if and only if $b_2 \oplus \cdots \oplus b_d = c \ominus (d+1)a_1$ and $b_2, \dots, b_d$ are distinct and non-zero. Let

$$A_{c,j} = \{(j, a_2, \dots, a_d) : 2j \oplus a_2 \oplus \cdots \oplus a_d = c, a_2, \dots, a_d \in H \setminus \{j\} \text{ distinct}\},$$

and let

$$B_k = \{(b_2, \dots, b_d) : b_2 \oplus \cdots \oplus b_d = k, b_2, \dots, b_d \in H \setminus \{0\} \text{ distinct}\}.$$

Then $|A_{c,j}| = |B_{c \ominus (d+1)j}|$, and the number of ordinary hyperplanes spanned by $H \oplus x$ is

$$\frac{1}{(d-1)!} \sum_{j \in H} |A_{c,j}|.$$

If $d+1$ is coprime to n, then $c \ominus (d+1)j$ runs through all elements of H as j varies. So we have $\sum_j |B_{c \ominus (d+1)j}| = (n-1) \cdots (n-d+1)$, hence for all c,

$$\frac{1}{(d-1)!} \sum_{j \in H} |A_{c,j}| = \binom{n-1}{d-1}.$$

If $d+1$ is not coprime to n, then $c \ominus (d+1)j$ runs through a coset of a subgroup of H of size $n/\gcd(d+1, n)$ as j varies. We now have

$$\sum_{j \in H} |B_{c \ominus (d+1)j}| = \gcd(d+1, n) \sum_{k \in c \ominus (d+1)H} |B_k|.$$

Summing over c gives

$$\sum_{c \in H} \sum_{j \in H} |A_{c,j}| = \gcd(d+1, n) \sum_{c \in H} \sum_{k \in c \ominus (d+1)H} |B_k|$$

$$= \gcd(d+1,n)\frac{n}{\gcd(d+1,n)}(n-1)\cdots(n-d+1)$$
$$= n(n-1)\cdots(n-d+1).$$

By the pigeonhole principle, there must then exist a c such that

$$\frac{1}{(d-1)!}\sum_{j\in H}|A_{c,j}| \leqslant \binom{n-1}{d-1}. \qquad \square$$

We next want to show that $[2,\overbrace{1,\dots,1}^{d-1 \text{ times}};c]$ is always very close to $(d-1)!\binom{n-1}{d-1}$, independent of c or the group H. Before that, we prove two simple properties of $[m_1,\dots,m_k;c]$.

Lemma 5.3. $[m_1,\dots,m_k;c] \leqslant 2m_k(k-1)!\binom{n}{k-1}$.

Proof. Consider a solution $(a_1,\dots,a_k)$ of $m_1a_1 \oplus \cdots \oplus m_ka_k = c$ where all the a_i are distinct. We can choose $a_1,\dots,a_{k-1}$ arbitrarily in $(k-1)!\binom{n}{k-1}$ ways, and a_k satisfies the equation $m_ka_k = c \ominus m_1a_1 \ominus \cdots \ominus m_{k-1}a_{k-1}$, which has at most m_k solutions if $H = \mathbb{Z}_n$ and at most $2m_k$ solutions if $H = \mathbb{Z}_2 \times \mathbb{Z}_{n/2}$. $\square$

Lemma 5.4. *We have the recurrence relation*

$$\begin{aligned}[m_1,\dots,m_{k-1},1;c] = (k-1)!\binom{n}{k-1} &- [m_1+1,m_2,\dots,m_{k-1};c]\\ &- [m_1,m_2+1,m_3,\dots,m_{k-1};c]\\ &- \cdots\\ &- [m_1,\dots,m_{k-2},m_{k-1}+1;c].\end{aligned}$$

Proof. We can arbitrarily choose distinct values from H for $a_1,\dots,a_{k-1}$, which determines a_k, and then we have to subtract the number of k-tuples where a_k is equal to one of the other a_i, $i = 1,\dots,k-1$. $\square$

Lemma 5.5.

$$[2,\underbrace{1,\dots,1}_{d-1 \text{ times}};c] = (d-1)!\left(\binom{n-1}{d-1} + \varepsilon(d,n)\right),$$

where

$$|\varepsilon(d,n)| = \begin{cases} O\left(2^{-d/2}\binom{n}{(d-1)/2} + \binom{n}{(d-3)/2}\right) & \text{if } d \text{ is odd,}\\ O\left(d2^{-d/2}\binom{n}{d/2-1} + \binom{n}{d/2-2}\right) & \text{if } d \text{ is even.}\end{cases}$$

Proof. Applying Lemma 5.4 once, we obtain

$$[2,\underbrace{1,\dots,1}_{d-1 \text{ times}};c] = (d-1)!\binom{n}{d-1} - [3,\underbrace{1,\dots,1}_{d-2 \text{ times}};c] - (d-2)[2,2,\underbrace{1,\dots,1}_{d-3 \text{ times}};c].$$

Note that at each stage of the recurrence in Lemma 5.4 (as long as it applies), there are $(d-1)(d-2)\cdots(d-k)$ terms of length $d-k$, where we define the *length* of $[m_1,\dots,m_k;c]$ to be k.

If d is odd, we can continue this recurrence until we reach

$$[2,\underbrace{1,\dots,1}_{d-1 \text{ times}};c] = (d-1)!\left(\binom{n}{d-1} - \binom{n}{d-2} + \cdots + (-1)^{(d+1)/2}\binom{n}{(d+1)/2}\right) + (-1)^{(d-1)/2}R,$$

where R is the sum of $(d-1)(d-2)\cdots(d-(d-1)/2)$ terms of length $(d+1)/2$. Among these there are

$$\frac{\binom{d-1}{2}\binom{d-3}{2}\cdots\binom{2}{2}}{(\frac{d-1}{2})!} = (d-2)(d-4)\cdots 3\cdot 1$$

terms of the form $[2,\dots,2;c]$. We now write $R = A+B$, where A is the same sum as R, except that we replace each occurrence of $[2,\dots,2;c]$ by $[1,\dots,1;c]$, and

$$B := (d-2)(d-4)\cdots 3\cdot 1([\underbrace{2,\dots,2}_{\frac{d+1}{2} \text{ times}};c] - [\underbrace{1,\dots,1}_{\frac{d+1}{2} \text{ times}};c]).$$

We next bound A and B. We apply Lemma 5.4 to each term in A, after which we obtain $(d-1)(d-2)\cdots(d-(d+1)/2)$ terms of length $(d-1)/2$. Then using the bound in Lemma 5.3, we obtain

$$\begin{aligned} A &= (d-1)!\binom{n}{(d-1)/2} - O\left((d-1)(d-2)\cdots(d-(d+1)/2)\,(\tfrac{d-3}{2})!\binom{n}{(d-3)/2}\right) \\ &= (d-1)!\left(\binom{n}{(d-1)/2} - O\left(\binom{n}{(d-3)/2}\right)\right). \end{aligned}$$

For B, we again use Lemma 5.3 to get

$$\begin{aligned} |B| &= O\left((d-2)(d-4)\cdots 3\cdot 1\left(\frac{d-1}{2}\right)!\binom{n}{(d-1)/2}\right) \\ &= O\left((d-2)(d-4)\cdots 3\cdot 1\cdot 2^{-\frac{d-1}{2}}(d-1)(d-3)\cdots 4\cdot 2\binom{n}{(d-1)/2}\right) \\ &= O\left((d-1)!2^{-\frac{d-1}{2}}\binom{n}{(d-1)/2}\right). \end{aligned}$$

Thus we obtain

$$\begin{aligned} [2,\underbrace{1,\dots,1}_{d-1 \text{ times}};c] &= (d-1)!\left(\binom{n}{d-1} - \binom{n}{d-2} + \cdots + (-1)^{\frac{d+1}{2}}\binom{n}{(d+1)/2}\right) \\ &\quad + (-1)^{\frac{d-1}{2}}(d-1)!\left(\binom{n}{(d-1)/2} - O\left(\binom{n}{(d-3)/2}\right)\right) + (-1)^{\frac{d-1}{2}}B \\ &= (d-1)!\left(\binom{n-1}{d-1} + (-1)^{\frac{d+1}{2}}O\left(\binom{n}{(d-3)/2}\right) \pm O\left(2^{-\frac{d-1}{2}}\binom{n}{(d-1)/2}\right)\right), \end{aligned}$$

which finishes the proof for odd d.

If d is even, we obtain

$$[2,\underbrace{1,\dots,1}_{d-1 \text{ times}};c] = (d-1)!\left(\binom{n}{d-1} - \binom{n}{d-2} + \dots + (-1)^{\frac{d}{2}+1}\binom{n}{d/2}\right) + (-1)^{d/2}R,$$

where R now is the sum of $(d-1)(d-2)\cdots(d-d/2)$ terms of length $d/2$. Among these there are

$$\frac{(d-1)\binom{d-2}{2}\binom{d-4}{2}\cdots\binom{2}{2}}{(\frac{d-2}{2})!} + \frac{2\binom{d-1}{3}\binom{d-4}{2}\cdots\binom{2}{2}}{(\frac{d-4}{2})!} = (d+1)(d-1)\cdots 7\cdot 5$$

terms of the form $[3,2,\dots,2;c]$. Again we write $R = A+B$, where A is the same sum as R, except that each occurrence of $[3,2,\dots,2;c]$ is replaced by $[1,\dots,1;c]$, and

$$B := (d+1)(d-1)\cdots 7\cdot 5([3,\underbrace{2,\dots,2}_{\frac{d}{2}-1 \text{ times}};c] - [\underbrace{1,\dots,1}_{\frac{d}{2} \text{ times}};c]).$$

Similar to the previous case, we obtain

$$A = (d-1)!\left(\binom{n}{d/2-1} - O\left(\binom{n}{d/2-2}\right)\right)$$

and

$$|B| = O\left((d+1)(d-1)\cdots 7\cdot 5(\tfrac{d}{2}-1)!\binom{n}{d/2-1}\right) = O\left(2^{-d/2}d!\binom{n}{d/2-1}\right),$$

which finishes the proof for even d. □

Computing $[2,\dots,2;c]$ and $[3,2,\dots,2;c]$ exactly is more subtle and depends on c and the group H. We do not need this for the asymptotic Theorems 1.2 and 1.3, and will only need to do so when computing exact extremal values.

To show that a coset is indeed extremal, we first consider the effect of adding a single point. The case where the point is on the curve is done in Lemma 5.6, while Lemma 5.7 covers the case where the point is off the curve. We then obtain a more general lower bound in Lemma 5.8.

Lemma 5.6. *Let δ^* be an elliptic normal curve or the smooth points of a rational acnodal curve in $\mathbb{RP}^d$, $d \geqslant 2$. Suppose $H \oplus x$ is a coset of a finite subgroup H of δ^* of order n, with $(d+1)x \in H$. Let $p \in \delta^* \setminus (H \oplus x)$. Then there are at least $\binom{n}{d-1}$ hyperplanes through p that meet $H \oplus x$ in exactly $d-1$ points.*

Proof. Take any $d-1$ points $p_1,\dots,p_{d-1} \in H \oplus x$. Suppose that the (unique) hyperplane through $p, p_1,\dots,p_{d-1}$ contains another point $p' \in H \oplus x$. Since $p \oplus p_1 \oplus \dots \oplus p_{d-1} \oplus p' = 0$ by Propositions 3.1 and 3.9, we obtain that $p \in H \ominus dx$. Since $(d+1)x \in H$, we obtain $p \in H \oplus x$, a contradiction. Therefore, the hyperplane through $p, p_1,\dots,p_{d-1}$ does not contain any other point of $H \oplus x$.

It remains to show that if $\{p_1,\dots,p_{d-1}\} \neq \{p'_1,\dots,p'_{d-1}\}$ where also $p'_1,\dots,p'_{d-1} \in H \oplus x$, then the two sets span different hyperplanes with p. Suppose they span the same hyperplane. Then $\ominus(p \oplus p_1 \oplus$

$\cdots \oplus p_{d-1})$ also lies on this hyperplane, but not in $H \oplus x$, as shown above. Also, $p_i' \notin \{p_1, \ldots, p_{d-1}\}$ for some i, and then $p_1, \ldots, p_{d-1}, p_i'$, and $\ominus(p \oplus p_1 \oplus \cdots \oplus p_{d-1})$ are $d+1$ distinct points on a hyperplane, so their sum is 0, which implies $p = p_i'$, a contradiction.

So there are $\binom{n}{d-1}$ hyperplanes through p meeting $H \oplus x$ in exactly $d-1$ points. □

The following Lemma generalises [9, Lemma 7.7], which states that if δ^* is an elliptic curve or the smooth points of an acnodal cubic curve in the plane, $H \oplus x$ is a coset of a finite subgroup of order $n > 10^4$, and if $p \notin \delta^*$, then there are at least $n/1000$ lines through p that pass through exactly one element of $H \oplus x$. A naive generalisation to dimension 3 would state that if δ^* is an elliptic or acnodal space quartic curve with a finite subgroup H of sufficiently large order n, and $x \in \delta^*$ and $p \notin \delta^*$, then there are $\Omega(n^2)$ planes through p and exactly two elements of $H \oplus x$. This statement is false, even if we assume that $4x \in H$ (the analogous assumption $3x \in H$ is not made in [9]), as can be seen from the following example.

Let δ be an elliptic quartic curve obtained from the intersection of a circular cylinder in $\mathbb{R}^3$ with a sphere which has centre c on the axis ℓ of the cylinder. Then δ is symmetric in the plane through c perpendicular to ℓ, and we can find a finite subgroup H of any even order n such that the line through any element of H parallel to ℓ intersects H in two points. If we now choose p to be the point at infinity on ℓ, then we obtain that any plane spanned by p and two points of H not collinear with p, intersects H in two more points. Note that the projection π_p maps δ to a conic, so is not generically one-to-one. The number of such p is bounded by the trisecant lemma (Lemma 2.3). However, as the next lemma shows, a generalisation of [9, Lemma 7.7] holds except that in dimension 3 we have to exclude such points p.

Lemma 5.7. *Let δ be an elliptic normal curve or a rational acnodal curve in $\mathbb{RP}^d$, $d \geqslant 2$, and let δ^* be its set of smooth points. Let H be a finite subgroup of δ^* of order n, where $n \geqslant Cd^4$ for some sufficiently large absolute constant $C > 0$. Let $x \in \delta^*$ satisfy $(d+1)x \in H$. Let $p \in \mathbb{RP}^d \setminus \delta^*$. If $d = 3$, assume furthermore that δ is not contained in a quadric cone with vertex p. Then there are at least $c\binom{n}{d-1}$ hyperplanes through p that meet the coset $H \oplus x$ in exactly $d-1$ points, for some sufficiently small absolute constant $c > 0$.*

Proof. We prove by induction on d that under the given hypotheses there are at least $c' \prod_{i=2}^{d} (1 - \frac{1}{i^2}) \binom{n}{d-1}$ such hyperplanes for some sufficiently small absolute constant $c' > 0$. The base case $d = 2$ is given by [9, Lemma 7.7].

Next assume that $d \geqslant 3$, and that the statement holds for $d-1$. Fix a $q \in H \oplus x$, and consider the projection π_q. Since q is a smooth point of δ, $\overline{\pi_q(\delta \setminus \{q\})}$ is a non-degenerate curve of degree d in $\mathbb{RP}^{d-1}$ (otherwise its degree would be at most $d/2$, but a non-degenerate curve has degree at least $d-1$). The projection π_q can be naturally extended to have a value at q, by setting $\pi_q(q)$ to be the point where the tangent line of δ at q intersects the hyperplane onto which δ is projected. (This point is the single point in $\overline{\pi_q(\delta \setminus \{q\})} \setminus \pi_q(\delta \setminus \{q\})$.) The curve $\pi_q(\delta)$ has degree d and is either elliptic or rational and acnodal, hence it has a group operation $\boxplus$ such that d points are on a hyperplane in $\mathbb{RP}^{d-1}$ if and only if they sum to the identity.

Observe that any d points $\pi_q(p_1), \ldots, \pi_q(p_d) \in \pi_q(\delta^*)$ lie on a hyperplane in $\mathbb{RP}^{d-1}$ if and only if $p_1 \oplus \cdots \oplus p_d \oplus q = 0$. By Proposition 3.10 it follows that the group on $\pi_q(\delta^*)$ obtained by transferring the group $(\delta^*, \oplus)$ by π_q is a translation of $(\pi_q(\delta^*), \boxplus)$. In particular, $\pi_q(H \oplus x) = H' \boxplus x'$ for some subgroup H' of $(\pi_q(\delta^*), \boxplus)$ of order n, and $(d+1)x' \in H'$.

We would like to apply the induction hypothesis, but we can only do that if $\pi_q(p) \notin \pi_q(\delta^*)$, and when $d = 4$, if $\pi_q(p)$ is not the vertex of a quadric cone containing $\pi_q(\delta)$. We next show that there are only $O(d^2)$ exceptional points q to which we cannot apply induction.

Note that $\pi_q(p) \in \pi_q(\delta^*)$ if and only if the line pq intersects δ with multiplicity 2, which means we have to bound the number of these lines through p. To this end, we consider the projection of δ from the point p. Suppose that π_p does not project δ generically one-to-one to a degree $d+1$ curve in $\mathbb{RP}^{d-1}$. Then $\pi_p(\delta)$ has degree at most $(d+1)/2$. However, its degree is at least $d-1$ because it is non-degenerate. It follows that $d = 3$, and that $\pi_p(\delta)$ has degree 2 and is irreducible, so δ is contained in a quadric cone with vertex p, which we ruled out by assumption.

Therefore, π_p projects δ generically one-to-one onto the curve $\pi_p(\delta)$, which has degree $d+1$ and has at most $\binom{d}{2}$ double points (this follows from the Plücker formulas after projecting to the plane [31, Chapter III, Theorem 4.4]). We thus have that an arbitrary point $p \in \mathbb{RP}^d \setminus \delta$ lies on at most $O(d^2)$ secants or tangents of δ (or lines through two points of δ^* if p is the acnode of δ).

If $d = 4$, we also have to avoid q such that $\pi_q(p)$ is the vertex of a cone on which $\pi_q(\delta)$ lies. Such q have the property that if we first project δ from q and then $\pi_q(\delta)$ from $\pi_q(p)$, then the composition of these two projections is not generically one-to-one. Another way to do these to successive projections is to first project δ from p and then $\pi_p(\delta)$ from $\pi_p(q)$. Thus, we have that $\pi_p(q)$ is a point on the quintic $\pi_p(\delta)$ in $\mathbb{RP}^3$ such that the projection of $\pi_p(\delta)$ from $\pi_p(q)$ onto $\mathbb{RP}^2$ is not generically one-to-one. However, there are only $O(1)$ such points by Lemma 2.3. Thus there are at most Cd^2 points $q \in H \oplus x$ to which we cannot apply the induction hypothesis.

For all remaining $q \in H \oplus x$, we obtain by the induction hypothesis that there are at least $c' \prod_{i=2}^{d-1}(1 - \frac{1}{i^2})\binom{n}{d-2}$ hyperplanes Π in $\mathbb{RP}^{d-1}$ through $\pi_q(p)$ and exactly $d-2$ points of $H' \boxplus x'$. If none of these $d-2$ points equal $\pi_q(q)$, then $\pi_q^{-1}(\Pi)$ is a hyperplane in $\mathbb{RP}^d$ through p and $d-1$ points of $H \oplus x$, one of which is q. There are at most $\binom{n-1}{d-3}$ such hyperplanes in $\mathbb{RP}^{d-1}$ through $\pi_q(q)$. Therefore, there are at least $c' \prod_{i=2}^{d-1}(1 - \frac{1}{i^2})\binom{n}{d-2} - \binom{n-1}{d-3}$ hyperplanes in $\mathbb{RP}^d$ that pass through p and exactly $d-1$ points of $H \oplus x$, one of them being q. If we sum over all $n - Cd^2$ points q, we count each hyperplane $d-1$ times, and we obtain that the total number of such hyperplanes is at least

$$\frac{n - Cd^2}{d-1}\left(c' \prod_{i=2}^{d-1}\left(1 - \frac{1}{i^2}\right)\binom{n}{d-2} - \binom{n-1}{d-3}\right). \tag{14}$$

It can easily be checked that

$$\frac{n - Cd^2}{d-1}\binom{n}{d-2} \geqslant \left(1 - \frac{1}{2d^2}\right)\binom{n}{d-1} \tag{15}$$

if $n > 2Cd^4$, and that

$$c' \prod_{i=2}^{d-1}\left(1 - \frac{1}{i^2}\right)\frac{1}{2d^2}\binom{n}{d-1} \geqslant \frac{n - Cd^2}{d-1}\binom{n-1}{d-3} \tag{16}$$

if $n > 4d^3/c'$. It now follows from (15) and (16) that the expression (14) is at least

$$c' \prod_{i=2}^{d}\left(1 - \frac{1}{i^2}\right)\binom{n}{d-1},$$

which finishes the induction. □

Lemma 5.8. *Let δ^* be an elliptic normal curve or the smooth points of a rational acnodal curve in $\mathbb{RP}^d$, $d \geqslant 4$, and let $H \oplus x$ be a coset of a finite subgroup H of δ^*, with $(d+1)x \in H$. Let $A \subseteq H \oplus x$ and $B \subset \mathbb{RP}^d \setminus (H \oplus x)$ with $|A| = a$ and $|B| = b$. Let $P = (H \oplus x \setminus A) \cup B$ with $|P| = n$ be such that every d points of P span a hyperplane. If A and B are not both empty and $n \geqslant C(a+b+d^2)d$ for some sufficiently large absolute constant $C > 0$, then P spans at least $(1+c)\binom{n-1}{d-1}$ ordinary hyperplanes for some sufficiently small absolute constant $c > 0$.*

Proof. We first bound from below the number of ordinary hyperplanes of $(H \oplus x) \setminus A$ that do not pass through a point of B.

The number of ordinary hyperplanes of $(H \oplus x) \setminus A$ that are disjoint from A is

$$\frac{1}{(d-1)!}\left|\left\{(a_1,\dots,a_d) \in (H \setminus (A \ominus x))^d : \begin{array}{c} 2a_1 \oplus a_2 \oplus \cdots \oplus a_d = \ominus(d+1)x, \\ a_1,\dots,a_d \text{ are distinct} \end{array}\right\}\right|.$$

If we denote by by $[m_1,\dots,m_k]'$ the number of ordered k-tuples $(a_1,\dots,a_k)$ with distinct $a_i \in H \setminus (A \ominus x)$ that satisfy $m_1a_1 \oplus \cdots \oplus m_ka_k = \ominus(d+1)x$, then we obtain, similar to the proofs of Lemmas 5.3 and 5.4, that

$$\begin{aligned}
[2,\underbrace{1,\dots,1}_{d-1 \text{ times}}]' &= (d-1)!\binom{n-b}{d-1} - [3,\underbrace{1,\dots,1}_{d-2 \text{ times}}]' - (d-2)[2,2,\underbrace{1,\dots,1}_{d-3 \text{ times}}]' \\
&\geqslant (d-1)!\binom{n-b}{d-1} - 2(d-2)!\binom{n-b}{d-2} - 2(d-2)(d-2)!\binom{n-b}{d-2} \\
&= (d-1)!\binom{n-b}{d-1} - 2(d-1)!\binom{n-b}{d-2},
\end{aligned}$$

and it follows that the number of ordinary hyperplanes of $(H \oplus x) \setminus A$ disjoint from A is at least $\binom{n-b}{d-1} - 2\binom{n-b}{2}$.

Next, we obtain an upper bound on the number of these hyperplanes that pass through a point $q \in B$. Let the ordinary hyperplane Π pass through $p_1, p_2, \dots, p_d \in (H \oplus x) \setminus A$, with p_1 being the double point. Since $q \in \Pi$ and any d points determine a hyperplane, Π is still spanned by $q, p_1, \dots, p_{d-1}$, after a relabelling of $p_2,\dots,p_d$. Let S be a minimal subset of $\{p_2,\dots,p_{d-1}\}$ such that the tangent line ℓ of δ at p_1 lies in the flat spanned by $S \cup \{q, p_1\}$.

If S is empty, then ℓ is a tangent from q to δ, of which there are at most $d(d+1)$ (this follows again from projection and the Plücker formulas [24, Corollary 2.5; 31, Chapter IV, p. 117]). Therefore, the number of ordinary hyperplanes through $p_1, p_2, \dots, p_d \in (H \oplus x) \setminus A$ with the tangent of δ at p_1 passing through q is at most $d(d+1)\binom{n-b}{d-2}$.

If on the other hand S is non-empty, then there is some p_i, say p_{d-1}, such that $q, p_1, \dots, p_{d-2}$ together with ℓ generate Π. Therefore, Π is determined by p_1, the tangent through p_1, and some $d-3$ more points p_i. There are at most $(n-b)\binom{n-b-1}{d-3} = (d-2)\binom{n-b}{d-2}$ ordinary hyperplanes through q in this case.

The number of ordinary hyperplanes of $(H \oplus x) \setminus A$ that contain a point from A is at least

$$a\left(\binom{n-b}{d-1} - a\binom{n-b}{d-2} - (n-b)\binom{n-b-1}{d-3}\right) = a\binom{n-b}{d-1} - (a^2 + a(d-2))\binom{n-b}{d-2},$$

since we can find such a hyperplane by choosing a point $p \in A$ and $d-1$ points $p_1, \dots, p_{d-1} \in (H \oplus x) \setminus A$, and then the remaining point $\ominus(p \oplus p_1 \oplus \cdots \oplus p_{d-1})$ might not be a new point in $(H \oplus x) \setminus A$ by either being in A (possibly equal to p) or being equal to one of the p_i. The number of these hyperplanes that also pass through some point of B is at most $ab\binom{n-b}{d-2}$.

Therefore, the number of ordinary hyperplanes of $(H \oplus x) \setminus A$ that miss B is at least

$$(1+a)\binom{n-b}{d-1} - \left(2+b(d(d+1)+d-2)+a^2+a(d-2)+ab\right)\binom{n-b}{d-2}. \tag{17}$$

Next, assuming that $B \neq \emptyset$, we find a lower bound to the number of ordinary hyperplanes through exactly one point of B and exactly $d-1$ points of $(H \oplus x) \setminus A$. The number of hyperplanes through at least one point of B and exactly $d-1$ points of $(H \oplus x) \setminus A$ is at least $bc'\binom{n-b}{d-1} - ab\binom{n-b}{d-2}$ by Lemmas 5.6 and 5.7 for some sufficiently small absolute constant $c' > 0$. The number of hyperplanes through at least two points of B and exactly $d-1$ points of $(H \oplus x) \setminus A$ is at most $\binom{b}{2}\binom{n-b}{d-2}$. It follows that there are at least $bc'\binom{n-b}{d-1} - \left(ab + \binom{b}{2}\right)\binom{n-b}{d-2}$ ordinary hyperplanes passing though a point of B.

Combining this with (17), P spans at least

$$(1+a+bc')\binom{n-b}{d-1} - \left(2+b(d(d+1)+d-2)+a^2+a(d-2)+2ab+\binom{b}{2}\right)\binom{n-b}{d-2} =: f(a,b)$$

ordinary hyperplanes. Since

$$f(a+1,b) - f(a,b) = \binom{n-b}{d-1} - (2a+2b+d-1)\binom{n-b}{d-2}$$

is easily seen to be positive for all $a \geqslant 0$ as long as $n > (2a+2b+d-1)(d-1)+b+d-2$, we have without loss of generality that $a = 0$ in the case that $b \geqslant 1$. Then $f(0,b+1) - f(0,b)$ is easily seen to be at least

$$c'\binom{n-b-1}{d-1} - (d^2+d-2+b)\binom{n-b-1}{d-2},$$

which is positive for all $b \geqslant 1$ if $n \geqslant C(b+d^2)d$ for C sufficiently large. Also, $f(0,1) = (1+c')\binom{n-1}{d-1} - (d^2+2d)\binom{n-1}{d-2}) \geqslant (1+c)\binom{n-1}{d-1}$ if $n \geqslant Cd^3$. This completes the proof in the case where B is non-empty.

If B is empty, then we can bound the number of ordinary hyperplanes from below by setting $b = 0$ in (17), and checking that the resulting expression

$$(1+a)\binom{n}{d-1} - \left(d+a^2+a(d-2)\right)\binom{n}{d-2}$$

is increasing in a if $n > (2a+d-1)(d-1)+d-2$, and larger than $\frac{3}{2}\binom{n-1}{d-1}$ if $n > Cd^3$. □

We are now ready to prove Theorems 1.2 and 1.3.

Proof of Theorem 1.2. Let P be the set of n points. By Lemma 5.2, we may assume that P has at most $\binom{n-1}{d-1}$ ordinary hyperplanes. Since $n \geqslant Cd^3 2^d$, we may apply Theorem 1.1 to obtain that up to $O(d2^d)$

points, P lies in a hyperplane or is a coset of a subgroup of an elliptic normal curve or the smooth points of a rational acnodal curve.

In the first case, by Lemma 5.1, since $n \geqslant Cd^3 2^d$, the minimum number of ordinary hyperplanes is attained when all but one point is contained in a hyperplane and we get exactly $\binom{n-1}{d-1}$ ordinary hyperplanes.

In the second case, by Lemma 5.8, again since $n \geqslant Cd^3 2^d$, the minimum number of ordinary hyperplanes is attained by a coset of an elliptic normal curve or the smooth points of a rational acnodal curve. Lemmas 5.2 and 5.5 then complete the proof. Note that the second term in the error term of Lemma 5.5 is dominated by the first term because of the lower bound on n, and that the error term here is negative by Lemma 5.2. □

Note that if we want to find the exact minimum number of ordinary hyperplanes spanned by a set of n points in $\mathbb{RP}^d$, $d \geqslant 4$, not contained in a hyperplane and where every d points span a hyperplane, we can continue with the calculation of $[2,1,\dots,1;c]$ in the proof of Lemma 5.5. As seen in the proof of Lemma 5.2, this depends on $\gcd(d+1,n)$. We also have to minimise over different values of $c \in H$, and if $n \equiv 0 \pmod 4$, consider both cases $H \cong \mathbb{Z}_n$ and $H \cong \mathbb{Z}_{n/2} \times \mathbb{Z}_2$.

For example, it can be shown that if $d = 4$, the minimum number is

$$\begin{cases} \binom{n-1}{3} - 4 & \text{if } n \equiv 0 \pmod 5, \\ \binom{n-1}{3} & \text{otherwise,} \end{cases}$$

if $d = 5$, the minimum number is

$$\begin{cases} \binom{n-1}{4} - \frac{1}{8}n^2 + \frac{1}{12}n - 1 & \text{if } n \equiv 0 \pmod 6, \\ \binom{n-1}{4} & \text{if } n \equiv 1,5 \pmod 6, \\ \binom{n-1}{4} - \frac{1}{8}n^2 + \frac{3}{4}n - 1 & \text{if } n \equiv 2,4 \pmod 6, \\ \binom{n-1}{4} - \frac{2}{3}n + 2 & \text{if } n \equiv 3 \pmod 6, \end{cases}$$

and if $d = 6$, the minimum number is

$$\begin{cases} \binom{n-1}{5} - 6 & \text{if } n \equiv 0 \pmod 7, \\ \binom{n-1}{5} & \text{otherwise.} \end{cases}$$

Proof of Theorem 1.3. We first show that there exist sets of n points, with every d points spanning a hyperplane, spanning at least $\frac{1}{d+1}\binom{n-1}{d} + O\left(2^{-d/2}\binom{n}{\lfloor \frac{d-1}{2} \rfloor}\right)$ $(d+1)$-point hyperplanes. Let δ^* be an elliptic normal curve or the smooth points of a rational acnodal curve. By Propositions 3.1 and 3.9, the number of $(d+1)$-point hyperplanes spanned by a coset $H \oplus x$ of δ^* is

$$\frac{1}{(d+1)!}[\underbrace{1,\dots,1}_{d+1 \text{ times}};c]$$

for some $c \in \delta^*$. Note that

$$[\underbrace{1,\dots,1}_{d+1 \text{ times}};c] = d!\binom{n}{d} - d[2,\underbrace{1,\dots,1}_{d-1 \text{ times}};c],$$

so if we take $H \oplus x$ to be a coset minimising the number of ordinary hyperplanes, then by Theorem 1.2, there are

$$\begin{aligned}&\frac{1}{d+1}\left(\binom{n}{d}-\binom{n-1}{d-1}\right)+O\left(2^{-\frac{d}{2}}\binom{n}{\lfloor\frac{d-1}{2}\rfloor}\right)\\&=\frac{1}{d+1}\binom{n-1}{d}+O\left(2^{-\frac{d}{2}}\binom{n}{\lfloor\frac{d-1}{2}\rfloor}\right)\end{aligned}\tag{18}$$

$(d+1)$-point hyperplanes.

Next let P be an arbitrary set of n points in $\mathbb{RP}^d$, $d \geqslant 4$, where every d points span a hyperplane. Suppose P spans the maximum number of $(d+1)$-point hyperplanes. Without loss of generality, we can thus assume P spans at least $\frac{1}{d+1}\binom{n-1}{d}+O\left(2^{-d/2}\binom{n}{\lfloor\frac{d-1}{2}\rfloor}\right)$ $(d+1)$-point hyperplanes.

Let m_i denote the number of i-point hyperplanes spanned by P. Counting the number of unordered d-tuples, we get

$$\binom{n}{d}=\sum_{i\geqslant d}\binom{i}{d}m_i \geqslant m_d+(d+1)m_{d+1},$$

hence we have

$$m_d \leqslant \binom{n}{d}-\binom{n-1}{d}-O\left(d2^{-\frac{d}{2}}\binom{n}{\lfloor\frac{d-1}{2}\rfloor}\right)=O\left(\binom{n-1}{d-1}\right),$$

and we can apply Theorem 1.1.

In the case where all but $O(d2^d)$ points of P are contained in a hyperplane, it is easy to see that P spans $O(d2^d\binom{n}{d-1})$ $(d+1)$-point planes, contradicting the assumption.

So all but $O(d2^d)$ points of P are contained in a coset $H \oplus x$ of a subgroup H of δ^*. Consider the identity

$$(d+1)m_{d+1}=\binom{n}{d}-m_d-\sum_{i\geqslant d+2}\binom{i}{d}m_i.$$

By Theorem 1.2 and Lemma 5.8, we know that $m_d \geqslant \binom{n-1}{d-1}-O\left(d2^{-d/2}\binom{n}{\lfloor\frac{d-1}{2}\rfloor}\right)$ and any deviation of P from the coset $H \oplus x$ adds at least $c\binom{n-1}{d-1}$ ordinary hyperplanes for some sufficiently small absolute constant $c>0$. Since we also have

$$\begin{aligned}\sum_{i\geqslant d+2}\binom{i}{d}m_i&=\binom{n}{d}-m_d-(d+1)m_{d+1}\\&=\binom{n}{d}-\binom{n-1}{d-1}-\binom{n-1}{d}+O\left(d2^{-\frac{d}{2}}\binom{n}{\lfloor\frac{d-1}{2}\rfloor}\right)\\&=O\left(d2^{-\frac{d}{2}}\binom{n}{\lfloor\frac{d-1}{2}\rfloor}\right),\end{aligned}$$

we can conclude that m_{d+1} is maximised when P is exactly a coset of a subgroup of δ^*, in which case (18) completes the proof. □

Knowing the exact minimum number of ordinary hyperplanes spanned by a set of n points in $\mathbb{RP}^d$, $d \geqslant 4$, not contained in a hyperplane and where every d points span a hyperplane then also gives the exact maximum number of $(d+1)$-point hyperplanes.

Continuing the above examples, for $d = 4$, the maximum number is

$$\begin{cases} \frac{1}{5}\binom{n-1}{4} + \frac{4}{5} & \text{if } n \equiv 0 \pmod 5, \\ \frac{1}{5}\binom{n-1}{4} & \text{otherwise,} \end{cases}$$

for $d = 5$, the maximum number is

$$\begin{cases} \frac{1}{6}\binom{n-1}{5} + \frac{1}{48}n^2 - \frac{1}{72}n + \frac{1}{6} & \text{if } n \equiv 0 \pmod 6, \\ \frac{1}{6}\binom{n-1}{5} & \text{if } n \equiv 1,5 \pmod 6, \\ \frac{1}{6}\binom{n-1}{5} + \frac{1}{48}n^2 - \frac{1}{8}n + \frac{1}{6} & \text{if } n \equiv 2,4 \pmod 6, \\ \frac{1}{6}\binom{n-1}{5} + \frac{1}{9}n - \frac{1}{3} & \text{if } n \equiv 3 \pmod 6, \end{cases}$$

and for $d = 6$, the maximum number is

$$\begin{cases} \frac{1}{7}\binom{n-1}{6} + \frac{6}{7} & \text{if } n \equiv 0 \pmod 7, \\ \frac{1}{7}\binom{n-1}{6} & \text{otherwise.} \end{cases}$$

Acknowledgments

We thank Peter Allen, Alex Fink, Misha Rudnev, and an anonymous referee for helpful remarks and for pointing out errors in a previous version.

References

[1] S. Ball, *On sets defining few ordinary planes*, Discrete Comput. Geom. **60** (2018), no. 1, 220–253. ↑2, 3

[2] S. Ball and E. Jimenez, *On sets defining few ordinary solids*. arXiv:1808.06388. ↑2

[3] S. Ball and J. Monserrat, *A generalisation of Sylvester's problem to higher dimensions*, J. Geom. **108** (2017), no. 2, 529–543. ↑2, 4, 17

[4] W. K. Clifford, *On the classification of loci*, Philosophical Transactions of the Royal Society of London **169** (1878), 663–681. ↑7

[5] I. Dolgachev, *Lectures on Invariant Theory*, Cambridge University Press, 2003. ↑8

[6] T. Fisher, *The invariants of a genus one curve*, Proc. Lond. Math. Soc. **97** (2008), no. 3, 753–782. ↑2

[7] W. Fulton, *Introduction to intersection theory in algebraic geometry*, CBMS Regional Conference Series in Mathematics, vol. 54, American Mathematical Society, 1984. ↑5

[8] K. Furukawa, *Defining ideal of the Segre locus in arbitrary characteristic*, J. Algebra **336** (2011), no. 1, 84–98. ↑6

[9] B. Green and T. Tao, *On sets defining few ordinary lines*, Discrete Comput. Geom. **50** (2013), no. 2, 409–468. ↑1, 2, 3, 4, 6, 18, 26

[10] S. Hansen, *A generalization of a theorem of Sylvester on the lines determined by a finite point set*, Math. Scand. **16** (1965), 175–180. ↑1

[11] J. Harris, *Algebraic Geometry: A First Course*, Springer, 1992. ↑5, 6, 7, 10, 11

[12] R. Hartshorne, *Algebraic Geometry*, Springer, 1977. ↑9

[13] A. Iarrobino and V. Kanev, *Power Sums, Gorenstein Algebras, and Determinantal Loci*, Lecture Notes in Mathematics, vol. 1721, Springer, 1999. ↑11

[14] E. Jimenez Izquierdo, *On sets of points with few ordinary hyperplanes*, Master's Thesis, Universitat Politècnica de Catalunya, 2018. ↑2

[15] J. Y. Kaminski, A. Kanel-Belov, and M. Teicher, *Trisecant lemma for nonequidimensional varieties*, J. Math. Sci. **149** (2008), no. 2, 1087–1097. ↑5

[16] V. Kanev, *Chordal varieties of Veronese varieties and catalecticant matrices*, J. Math. Sci. **94** (1999), no. 1, 1114–1125. ↑11

[17] F. Klein, *Über die elliptischen Normalcurven der Nten Ordnung und zugehörige Modulfunctionen der Nten Stufe*, Abhandlungen der mathematisch-physischen Classe der Königlich Sächsischen Gesellschaft der Wissenschaften **13** (1885), no. 4, 337–399. ↑2, 7

[18] J. Kollár, *Lectures on Resolution of Singularities*, Annals of Mathematics Studies, vol. 166, Princeton University Press, 2007. ↑5

[19] A. Lin, M. Makhul, H. Nassajian Mojarrad, J. Schicho, K. Swanepoel, and F. de Zeeuw, *On sets defining few ordinary circles*, Discrete Comput. Geom. **59** (2018), no. 1, 59–87. ↑18

[20] A. Lin and K. Swanepoel, *Ordinary planes, coplanar quadruples, and space quartics*, J. Lond. Math. Soc. (2) **100** (2019), 937–956. ↑2, 3, 4, 5, 6, 7, 15

[21] J. Monserrat, *Generalisation of Sylvester's problem*, Bachelor's Degree Thesis, Universitat Politècnica de Catalunya, 2015. ↑2

[22] T. Motzkin, *The lines and planes connecting the points of a finite set*, Trans. Amer. Math. Soc. **70** (1951), no. 3, 451–464. ↑1

[23] G. Muntingh, *Topics in polynomial interpolation theory*, Ph.D. Dissertation, University of Oslo, 2010. ↑4

[24] H. Nassajian Mojarrad and F. de Zeeuw, *On the number of ordinary circles*. arXiv:1412.8314. ↑28

[25] G. B. Purdy and J. W. Smith, *Lines, circles, planes and spheres*, Discrete Comput. Geom. **44** (2010), no. 4, 860–882. ↑2

[26] B. Reznick, *On the length of binary forms*, Quadratic and higher degree forms, Dev. Math., vol. 31, Springer, 2013, pp. 207–232. ↑11

[27] J. G. Semple and L. Roth, *Introduction to Algebraic Geometry*, The Clarendon Press, 1985. Reprint of the 1949 original. ↑7

[28] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Second Edition, Springer, 2009. ↑7

[29] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer, 1994. ↑7

[30] J. J. Sylvester, *On a remarkable discovery in the theory of canonical forms and of hyperdeterminants*, Philosophical Magazine **2** (1851), 391–410. Paper 41 in The Collected Mathematical Papers of James Joseph Sylvester, Cambridge University Press, 1904. ↑11

[31] R. J. Walker, *Algebraic Curves*, Springer, 1978. ↑27, 28

AUTHORS

Aaron Lin
Department of Mathematics
London School of Economics and Political Science
United Kingdom
aaronlinhk@gmail.com

Konrad Swanepoel
Department of Mathematics
London School of Economics and Political Science
United Kingdom
k.swanepoel@lse.ac.uk
http://personal.lse.ac.uk/swanepoe/