Structure theorems and extremal problems in incidence geometry

Hiu Chung Aaron Lin

A thesis submitted for the degree of
Doctor of Philosophy

Department of Mathematics
The London School of Economics
and Political Science

November 2019

Declaration

I certify that the thesis I have presented for examination for the MPhil/PhD degree of the London School of Economics and Political Science is my own work, with the following exceptions.

Parts of Section 3.3, parts of Chapter 4, Section 5.3, and Section 6.3 are based on [40], which is published in Discrete & Computational Geometry, and is joint work with Mehdi Makhul, Hossein Nassajian Mojarrad, Josef Schicho, Konrad Swanepoel, and Frank de Zeeuw.

Lemma 3.16 of Section 3.2, Section 5.1, and Section 6.1 are based on [41], which is accepted to the Journal of the London Mathematical Society, and is joint work with Konrad Swanepoel.

Lemma 2.6 of Section 2.1, Section 2.2.2, Section 3.2, parts of Chapter 4, Section 5.2, and Section 6.2 are based on [42], which is joint work with Konrad Swanepoel.

Parts of Section 3.3, Section 5.4, and Section 6.4 are based on [43], which is joint work with Konrad Swanepoel.

The copyright of this thesis rests with the author. Quotation from it is permitted, provided that full acknowledgement is made. This thesis may not be reproduced without the prior written consent of the author.

I warrant that this authorisation does not, to the best of my belief, infringe the rights of any third party.

Abstract

In this thesis, we prove variants and generalisations of the Sylvester-Gallai theorem, which states that a finite non-collinear point set in the plane spans an ordinary line. Green and Tao proved a structure theorem for sufficiently large sets spanning few ordinary lines, and used it to find exact extremal numbers for ordinary and 3-rich lines, solving the Dirac-Motzkin conjecture and the classical orchard problem respectively.

We prove structure theorems for sufficiently large sets spanning few ordinary planes, hyperplanes, circles, and hyperspheres, showing that such sets lie mostly on algebraic curves (or on a hyperplane or hypersphere). We then use these structure theorems to solve the corresponding analogues of the Dirac-Motzkin conjecture and the orchard problem.

For planes in 3-space and circles in the plane, we are able to find exact extremal numbers for ordinary and 4-rich planes and circles. We also show that there are irreducible rational space quartics such that any n-point subset spans only $O(n^{8/3})$ coplanar quadruples, answering a question of Raz, Sharir, and De Zeeuw [51].

For hyperplanes in d-space, we are able to find tight asymptotic bounds on the extremal numbers for ordinary and $(d+1)$-rich hyperplanes. This also gives a recursive method to compute exact extremal numbers for a fixed dimension d.

For hyperspheres in d-space, we are able to find a tight asymptotic bound on the minimum number of ordinary hyperspheres, and an asymptotic bound on the maximum number of $(d+2)$-rich hyperspheres that is tight in even dimensions. The recursive method in the hyperplanes case also applies here.

Our methods rely on Green and Tao's results on ordinary lines, as well as results from classical algebraic geometry, in particular on projections, inversions, and algebraic curves.

Acknowledgements

I would first like to thank my supervisor Konrad, without whom this thesis would only be a dream. Thank you for your support, from even before I started my PhD, for your wisdom and passion, not only in mathematics but also in life, for putting up with my stubbornness, and most of all for embarking on this journey with me, even though you really did not have to.

I would also like to thank the Maths Department at the LSE. Thank you to Nóra, Jan, Keat, Attila, Edin, Stan for all the fun and games. Thank you to Becca, Kate, Enfale, Sarah, Ed for making my life as easy as possible. Thank you to Jozef, Jan, Peter, Julia for creating such a comfortable atmosphere, for making the department home.

You, and everyone along the way that lead me to this point, deserve much more thanks than I am ever capable of expressing. Teachers – Mrs. Teo, Mr. Sanders, Kerry – who inspired me down this path, lifelong friends who supported me through this journey, thank you.

Finally, I would like to thank my family – my parents and my brother – for their unwavering support, for being my eternal shelter, for just being there whenever things get rough. Thank you for always indulging me.

Contents

Chapter 1

Introduction

1.1 Background

It was known in the 18th and 19th centuries, by Maclaurin and Hesse among others [2], that an elliptic cubic curve in the complex plane has nine inflection points, and that the line through any two of them contains a third. Sylvester [61] asked in 1893 the natural question on whether this can happen in the real plane.

Definition 1.1. An *ordinary line* of a set in the real plane is a line that contains exactly two points of the set.

No correct proof was known until Erdős rediscovered the question on the existence of an ordinary line in the 1930s, after which it was solved by Gallai [14, p. 302], resulting in the following classical result in incidence geometry.

Theorem 1.2 (Sylvester–Gallai)**.** *Any finite non-collinear point set in the real plane spans at least one ordinary line.*

The earliest published proof however was due to Melchior [44], who proved the dual statement and showed that one can in fact always find at least three ordinary lines. The natural next step is then to find how many ordinary lines a non-collinear n-point set in the real plane spans. The so-called Dirac–Motzkin conjecture asserts that if $n > 13$, then this number should be

$n/2$. Starting from Melchior's proof, Green and Tao [25] characterised all extremal and near-extremal configurations by proving the following structure theorem, which roughly states that any point set spanning a linear number of ordinary lines must lie mostly on a cubic curve. (See [25, Section 2] for the group structure on elliptic and acnodal cubic curves.)

Theorem 1.3 (Green–Tao [25, Theorem 1.5])**.** *Let $K > 0$ and suppose n is sufficiently large depending on K. If a set P of n points in $\mathbb{RP}^2$ spans at most Kn ordinary lines, then up to a projective transformation, P differs in at most $O(K)$ points from a configuration of one of the following types:*

(*i*) *$n - O(K)$ points on a line;*

(*ii*) *the vertex set of a regular m-gon and the m points at infinity corresponding to the diagonals of the m-gon, for some $m = n/2 \pm O(K)$;*

(*iii*) *a coset $H \oplus x$ of a subgroup H of an elliptic or acnodal cubic curve, for some x such that $3x \in H$.*

They [25] used Theorem 1.3 to prove the Dirac–Motzkin conjecture for sufficiently large n, and went further to show the following theorem.

Theorem 1.4 (Dirac–Motzkin conjecture [25, Theorem 2.2])**.** *If n is sufficiently large, the minimum number of ordinary lines spanned by a non-collinear set of n points in $\mathbb{RP}^2$ is equal to*

$$\begin{cases} n/2 & \text{if } n \equiv 0, 2 \pmod 4, \\ \lfloor 3n/4 \rfloor & \text{if } n \equiv 1 \pmod 4, \\ \lfloor 3n/4 \rfloor - 2 & \text{if } n \equiv 3 \pmod 4. \end{cases}$$

For small n, the bound $6n/13$ due to Csima and Sawyer [17] is the best known lower bound on the number of ordinary lines.

Green and Tao [25] also solved the even older orchard problem (for sufficiently large n), which asks for the maximum number of lines that contain exactly three points of a given finite set in the plane. We first make the following definition.

Definition 1.5. A 3-*rich line* of a set in the real (projective) plane is a line that contains exactly three points of the set.

More generally, a $(d+1)$-*rich hyperplane* of a set in real projective d-space, where every d points span a hyperplane, is a hyperplane that contains exactly $d+1$ points of the set.

The upper bound $\frac{1}{3}\binom{n}{2}$ on the number of 3-rich lines is easily proved by double counting, but this is not the exact maximum. Using group laws on certain cubic curves, Green and Tao [25] proved the following theorem.

Theorem 1.6 (Orchard problem [25, Theorem 1.3])**.** *If n is sufficiently large, the maximum number of 3-rich lines spanned by a set of n points in $\mathbb{RP}^2$ is equal to $\left\lfloor \frac{1}{6}n(n-3)+1 \right\rfloor$.*

This does not follow directly from the Dirac–Motzkin conjecture, but it does follow from Theorem 1.3, Green and Tao's structure theorem for sets spanning few ordinary lines.

A natural generalisation is to consider higher dimensional analogues. However, Motzkin [46] noted that there are finite non-coplanar point sets in 3-space that span no plane containing exactly three points of the set. His one example consists of the ten intersection points of triples of five planes in general position, and another consists of points chosen from two skew lines. He proposed considering instead hyperplanes Π in d-space such that all but one point contained in Π is contained in a $(d-2)$-flat of Π. The existence of such a hyperplane was shown by Motzkin [46] in 3-space and by Hansen [27] in higher dimensions. Hansen [28] also improved Motzkin's lower bound in 3-space to $2n/5$, but no other improvements seem to have been made since.

Purdy and Smith [49] considered instead finite non-coplanar point sets in 3-space that are in general position in the sense that no three points are collinear, proving a quadratic lower bound of $\frac{4}{13}\binom{n}{2}$ on the number of planes containing exactly three points of the set. Ball [4] also considered this notion, and together with Monserrat [6] considered a higher dimensional generalisation. In particular, they made the following definition.

Definition 1.7. An *ordinary plane* of a set in real projective 3-space with no three collinear is a plane that contains exactly three points of the set.

More generally, an *ordinary hyperplane* of a set in real projective d-space, where every d points span a hyperplane, is a hyperplane that contains exactly d points of the set.

Thus, in this thesis, ordinary (planes and) hyperplanes are of sets in general position in the weak sense that any d points span a hyperplane. In 3-space, this means no three points are collinear; in 2-space, this means only that the points are distinct.

Following Green and Tao's approach, Ball [4] proved a structure theorem for sets spanning few ordinary planes, showing such sets lie mostly on the intersection curve of two linearly independent quadrics. Ball and Monserrat [6] used this to find the exact minimum number of ordinary planes spanned by sufficiently large finite non-coplanar point sets with no three points collinear, solving a 3-dimensional analogue of the Dirac–Motzkin conjecture. Using an alternative method, we will prove a more detailed structure theorem but with a stronger condition (on the size of the sets), and confirm their determination of the exact minimum. In contrast to Purdy and Smith's lower bound, the correct asymptotics are $\frac{1}{2}\binom{n}{2} - O(n)$ if n is even, and $\frac{3}{4}\binom{n}{2} - O(n)$ if n is odd.

In higher dimensions, building on Ball's ideas [4], Ball and Jimenez [5] proved a structure theorem for sets spanning few ordinary hyperplanes in 4-space, showing such sets lie mostly on the intersection curve of five linearly independent quadrics. On the other hand, Monserrat [45] proved a structure theorem stating that sets in general position (as in Definition 1.7) spanning few ordinary hyperplanes in d-space lie mostly on the intersection curve of $d-1$ hypersurfaces of degree at most 3. Ball and Monserrat [6] also proved bounds on the minimum number of ordinary hyperplanes spanned by sets not contained in a hyperplane (see also [45]). Using our methods, we will prove a more detailed structure theorem in d-space for all $d \geqslant 4$, and use it to find a tight bound on the minimum number of ordinary hyperplanes spanned by sufficiently large sets in general position (again as in Definition 1.7) that

are not contained in a hyperplane, solving a d-dimensional analogue of the Dirac–Motzkin conjecture. For the exact minimum numbers for some small n and d, see [6].

We will also solve a d-dimensional analogue of the orchard problem for all $d \geqslant 3$, finding the maximum number of $(d+1)$-rich hyperplanes spanned by sufficiently large sets in d-space, where every d points span a hyperplane. We will determine the exact maximum number in 3-space, and prove a tight bound in higher dimensions.

The main idea of our proofs is to leverage the structure theorem in one dimension lower via projection. Since our sets will lie mostly on algebraic curves, we also need a good understanding on how they behave under projection. Thus, we rely on Green and Tao's results on ordinary lines [25] as well as methods from classical algebraic geometry.

Another natural variant is to consider circles (see for instance [14, Section 7.2] or [37, Chapter 6]) and its higher dimensional analogues.

Definition 1.8. An *ordinary circle* of a set in the real plane is a circle (including the degenerate case of a line) that contains exactly three points of the set. A *strict ordinary circle* is an ordinary circle that is not a line.

More generally, an *ordinary hypersphere* of a set in real d-space, where no $d+1$ points are contained in a $(d-2)$-sphere or a $(d-2)$-flat, is a hypersphere (including the degenerate case of a hyperplane) that contains exactly $d+1$ points of the set.

Similarly, a *$(d+2)$-rich hypersphere* of such a set is one that contains exactly $d+2$ points of the set.

As with (planes and) hyperplanes, ordinary (and $(d+2)$-rich) hyperspheres are of sets in general position in the weak sense that no $d+1$ points are contained in a $(d-2)$-sphere or a $(d-2)$-flat. In 3-space, this means no four points are concyclic or collinear; in 2-space, this means only that the points are distinct.

Elliott [20] introduced the problem for circles in 1967, and proved that an n-point set in the plane, not all on a circle or a line, spans at least $\frac{2}{63}n^2 -$

$O(n)$ strict ordinary circles. He suggested, cautiously, that the optimal bound is $\frac{1}{6}n^2 - O(n)$. Elliott's result was improved by Bálintová and Bálint [3, Remark, p. 288] to $\frac{11}{247}n^2 - O(n)$, and Zhang [68] obtained $\frac{1}{18}n^2 - O(n)$. Zhang also gave constructions of point sets on two concentric circles with $\frac{1}{4}n^2 - O(n)$ strict ordinary circles.

It turns out that it is more natural to consider lines as degenerate circles, as inversion maps circles and lines to circles and lines, and more generally maps hyperspheres and hyperplanes to hyperspheres and hyperplanes. Just as the number of ordinary and $(d+1)$-rich hyperplanes spanned by a set in real projective d-space remain unchanged under a projective transformation, the number of ordinary and $(d+2)$-rich hyperspheres spanned by a set in affine d-space remain unchanged under an inversion.

We will prove a structure theorem for sets spanning few ordinary circles, and use it to show that $\frac{1}{4}n^2 - O(n)$ is asymptotically the right answer for strict ordinary circles, disproving the bound suggested by Elliott [20]. We note that Nassajian Mojarrad and De Zeeuw proved this bound in an earlier preprint [48], which is now subsumed by [40]. As is the case with ordinary planes, the correct asymptotics for ordinary circles are $\frac{1}{2}\binom{n}{2} - O(n)$ if n is even, and $\frac{3}{4}\binom{n}{2} - O(n)$ if n is odd. We will also find the exact minimum number of (strict) ordinary circles for sufficiently large n, solving a circular analogue of the Dirac–Motzkin conjecture. For small n, the bound $\frac{1}{9}\binom{n}{2}$ due to Zhang [68] remains the best known lower bound on the number of (strict) ordinary circles.

In higher dimensions, we will prove a structure theorem for sets spanning few ordinary hyperspheres in d-space for all $d \geqslant 3$, and use it to find a tight bound on the minimum number of ordinary hyperspheres spanned by sufficiently large sets in general position (as in Definition 1.8) not contained in a hypersphere or a hyperplane. This solves a d-dimensional circular analogue of the Dirac–Motzkin conjecture. On a related note, Purdy and Smith [49] considered ordinary spheres in 3-space in the slightly more restricted setting of a finite set of points with no four concyclic and no *three* collinear.

Finally, we will also consider a d-dimensional circular analogue of the orchard problem of finding the maximum number of $(d+2)$-rich hyperspheres

spanned by sufficiently large sets in general position (again as in Definition 1.8) in d-space. However, unlike the previous cases, we will only be able to prove a tight bound on the maximum number of $(d+2)$-rich hyperspheres if d is even; if d is odd, we only get an upper bound.

For the circular variants, the main idea is to leverage our structure theorems for sets spanning few ordinary (planes and) hyperplanes in one dimension higher via stereographic projection. As in the (planar and) hyperplanar cases, we rely on the behaviour of certain algebraic curves under stereographic projection (and thus inversion), which again require methods from classical algebraic geometry.

1.2 Results

The main results of this thesis are collected in this section. Prisms, antiprisms, and 'aligned' and 'offset' double polygons will be introduced in Section 4.2. Roughly speaking, prisms and antiprisms are the vertex sets of prisms and antiprisms over regular polygons in 3-space, while double polygons are the vertex sets of two concentric regular polygons in 2-space. Hence they are all contained in the union of two conics. All algebraic curves appearing in the statements below will be introduced in Chapter 3, where we will also define group laws on them. For now, it suffices to note their degrees and their irreducibility.

1.2.1 Structure theorems

We first state our structure theorems for sets P spanning few ordinary planes, hyperplanes, circles, and hyperspheres. They all state that P differs in at most a bounded number of points from a set S, which is either contained in a hyperplane (or a hypersphere in the circular variants) or an algebraic curve of low degree in some special configuration. In particular, P can be obtained from S by adding and/or removing a bounded number of points.

Our first main result is a structure theorem for sets spanning few ordinary

planes. Prisms and antiprisms will be introduced in Section 4.2 (see Definition 4.3). Elliptic and acnodal space quartics will be introduced in Chapter 3 (see Definitions 3.6 and 3.12), where we will also define group laws on them.

Theorem 1.9 (Ordinary planes)**.** *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 three collinear. If P spans at most Kn^2 ordinary planes, then up to a projective transformation, 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 prism or an antiprism;*

(*iii*) *a coset $H \oplus x$ of a subgroup H of an elliptic space quartic curve or the smooth points of an acnodal space quartic curve, for some x such that $4x \in H$.*

Conversely, every set of these types spans at most $C'Kn^2$ ordinary planes for some absolute constant $C' > 0$.

We will later show that prisms, antiprisms, elliptic space quartics, and acnodal space quartics all arise as intersections of two linearly independent quadrics, thus agreeing with Ball's structure theorem [4]. We also note that Ball's condition of $K = o(n^{1/7})$ is weaker than ours, but he does not specify the intersection curve nor its group structure.

Theorem 1.9 forms the basis for proving the following structure theorem for sets spanning few ordinary hyperplanes. Elliptic normal curves and rational acnodal curves will be introduced in Chapter 3 (see Definitions 3.6 and 3.12), where we will also define group laws on them.

Theorem 1.10 (Ordinary hyperplanes)**.** *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 $(d+1)x \in H$.*

Conversely, every set of these types spans at most $C'2^d K\binom{n-1}{d-1}$ ordinary hyperplanes for some absolute constant $C' > 0$.

Theorem 1.10 proves Ball and Jimenez's [5, Conjecture 12], noting that elliptic normal curves and rational acnodal curves lie on $\binom{d}{2} - 1$ linearly independent quadrics [21, Proposition 5.3; 38, p. 365]. As in the planes case, Ball and Jimenez's condition of $K = o(n^{1/7})$ is weaker than ours, but again they do not specify the intersection curve nor its group structure. In contrast to the planes case, we no longer have configurations lying mostly on non-irreducible curves.

By stereographic projection and Theorem 1.9, we obtain Theorem 1.11 below. This is a strict strengthening of Theorem 5.15, which we will prove in an alternative way that requires less algebraic geometry. In Theorem 5.15, we need $n \geqslant \exp\exp(CK^C)$; here we only assume $n \geqslant CK^8$. Circular curves will be introduced in Section 3.3 (see Definition 3.19), where we will define group laws on them (and on ellipses). Double polygons, both 'aligned' and 'offset', will be introduced in Section 4.2 (see Definition 4.4).

Theorem 1.11 (Ordinary circles)**.** *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 $\mathbb{R}^2$. If P spans at most Kn^2 ordinary circles, then up to inversions and similarities of the plane, P differs in at most $O(K)$ points from a configuration of one of the following types:*

(*i*) *a subset of a line;*

(*ii*) *a coset $H \oplus x$ of a subgroup H of an ellipse, for some x such that $4x \in H$;*

(*iii*) *a coset $H \oplus x$ of a subgroup H of a circular elliptic cubic curve, for some x such that $4x \in H$;*

(*iv*) *a double polygon that is 'aligned' or 'offset'.*

Conversely, every set of these types spans at most $C'Kn^2$ *ordinary circles for some absolute constant* $C' > 0$.

Similarly, by stereographic projection and Theorem 1.10, we get the following structure theorem for sets spanning few ordinary hyperspheres. Spherical curves will be introduced in Section 3.3 (see Definition 3.19), where we will also define group laws on them.

Theorem 1.12 (Ordinary hyperspheres)**.** *Let* $d \geqslant 3$, $K > 0$, *and suppose* $n > C\max\{(dK)^8, d^3 2^d K\}$ *for some sufficiently large absolute constant* $C > 0$. *Let* P *be a set of* n *points in* $\mathbb{R}^d$ *where no* $d+1$ *points lie on a* $(d-2)$*-sphere or a* $(d-2)$*-flat. Suppose* P *spans at most* $K\binom{n}{d}$ *ordinary hyperspheres.*

If d *is odd, then all but at most* $O(d2^d K)$ *points of* P *lie on a hypersphere or a hyperplane.*

If $d = 2k$ *is even, then up to an inversion,* 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 a bounded* $(k-1)$*-spherical rational normal curve of degree* d, *for some* x *such that* $(d+2)x \in H$;

(*iii*) *a coset* $H \oplus x$ *of a subgroup* H *of a* k*-spherical elliptic normal curve of degree* $d+1$, *for some* x *such that* $(d+2)x \in H$.

Conversely, every set of these types spans at most $C'2^d K\binom{n}{d}$ *ordinary hyperspheres for some absolute constant* $C' > 0$.

1.2.2 Extremal theorems

We now state our extremal theorems, which solve the corresponding analogues of the Dirac–Motzkin conjecture and the orchard problem. We also describe constructions that attain these extrema. The exact extremal values turn out to be quasipolynomials in n with a period of $2(d+1)$, where n is

the size of the set and d is the dimension, that is, there exist polynomials $q_0, \ldots, q_{2d+1} \in \mathbb{Q}[n]$ such that the extremal value is equal to $q_i(n)$ where $n \equiv i \pmod{2(d+1)}$.

The following is a restatement of Ball and Monserrat's result on the minimum number of ordinary planes [6], but we will give an alternative proof based on our Theorem 1.9.

Theorem 1.13 (Ordinary planes)**.**

(*i*) *If n is sufficiently large, the minimum number of ordinary planes spanned by a non-coplanar set of n points in $\mathbb{RP}^3$ with no three collinear is equal to*

$$\begin{cases} \frac{1}{4}n^2 - n & \text{if } n \equiv 0 \pmod 4, \\ \frac{3}{8}n^2 - n + \frac{5}{8} & \text{if } n \equiv 1 \pmod 4, \\ \frac{1}{4}n^2 - \frac{1}{2}n & \text{if } n \equiv 2 \pmod 4, \\ \frac{3}{8}n^2 - \frac{3}{2}n + \frac{17}{8} & \text{if } n \equiv 3 \pmod 4. \end{cases}$$

(*ii*) *Let $C > 0$ be a sufficiently large absolute constant. If a non-coplanar set P of n points in $\mathbb{RP}^3$ with no three collinear spans fewer than $\frac{1}{2}n^2 - Cn$ ordinary planes, then P is contained in a prism or an antiprism.*

In Chapter 4, we will describe constructions that meet the lower bound in part (*i*) of Theorem 1.13. If n is even, the bound is attained by prisms or antiprisms, while if n is odd, the bound is attained by prisms or antiprisms with a point removed.

Theorem 1.14 (4-rich planes)**.**

(*i*) *If n is sufficiently large, the maximum number of 4-rich planes spanned by a set of n points in $\mathbb{RP}^3$ with no three collinear is equal to*

$$\begin{cases} \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{5}{6}n & \text{if } n \equiv 0 \pmod 8, \\ \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{11}{24}n - \frac{1}{4} & \text{if } n \equiv 1, 3, 5, 7 \pmod 8, \\ \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{7}{12}n - \frac{1}{2} & \text{if } n \equiv 2, 6 \pmod 8, \\ \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{5}{6}n - 1 & \text{if } n \equiv 4 \pmod 8. \end{cases}$$

(*ii*) *Let $C > 0$ be a sufficiently large absolute constant. If a set P of n points in $\mathbb{RP}^3$ with no three collinear spans more than $\frac{1}{24}n^3 - \frac{7}{24}n^2 + Cn$ 4-rich planes, then P lies on an elliptic or acnodal space quartic curve.*

We will again describe constructions meeting the upper bound in part (*i*) of Theorem 1.14 in Chapter 4. In this case, they are all attained by cosets of elliptic or acnodal space quartics.

We also consider the number of *coplanar quadruples* (four distinct coplanar points) spanned by an n-point set on quartic curves in complex 3-space. Raz, Sharir, and De Zeeuw [50] showed that such a set spans $O(n^{8/3})$ coplanar quadruples unless the curve contains a planar or a quartic component (see Theorem 2.27). They left it as an open problem whether there always exist configurations on rational space quartic curves (that are not contained in a plane) spanning $\Theta(n^3)$ coplanar quadruples. The properties of space quartic curves that we need to prove Theorem 1.9 also enable us prove the following theorem.

Theorem 1.15 (Coplanar quadruples)**.** *Let δ be a rational space quartic curve in $\mathbb{CP}^3$. If δ is singular, then there exist n points on δ that span $\Theta(n^3)$ coplanar quadruples. If δ is smooth, then any n points on δ span $O(n^{8/3})$ coplanar quadruples.*

We will also prove in Section 3.2 that a rational space quartic is always contained in a quadric, and is contained in at least two linearly independent quadrics if and only if it is singular.

Moving on to hyperplanes, Theorem 1.16 below proves [6, Conjecture 3], which asserts the existence of a constant c_d such that the minimum number of ordinary hyperplanes spanned by a sufficiently large n-point set is at least $\frac{1}{(d-1)!}n^{d-1} - c_d n^{d-2}$. Ball and Monserrat [6] also remarked that it might be possible the minimum is exactly $\binom{n-1}{d-1}$. Note that as a consequence of Theorem 1.10, we do not have extremal constructions lying on non-irreducible curves in both Theorems 1.16 and 1.17 below. Hence the same constructions are extremal for both ordinary and $(d+1)$-rich hyperplanes. The only difference is that the trivial example, where all but one point is contained in a hyperplane, is sometimes extremal for ordinary hyperplanes.

Theorem 1.16 (Ordinary hyperplanes)**.** *Let $d \geqslant 4$ and let $n \geqslant Cd^3 2^d d!$ 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*

$$\binom{n-1}{d-1} - O\left(d^2 2^{-d/2}\binom{n}{\lfloor (d-1)/2 \rfloor} + \binom{n}{\lfloor (d-3)/2 \rfloor}\right).$$

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.

Theorem 1.17 ($(d+1)$-rich hyperplanes)**.** *Let $d \geqslant 4$ and let $n \geqslant Cd^3 2^d d!$ for some sufficiently large absolute constant $C > 0$. The maximum number of $(d+1)$-rich hyperplanes spanned by a set of n points in $\mathbb{RP}^d$ where every d points span a hyperplane is*

$$\frac{1}{d+1}\left[\binom{n-1}{d} + O\left(d^2 2^{-d/2}\binom{n}{\lfloor (d-1)/2 \rfloor} + \binom{n}{\lfloor (d-3)/2 \rfloor}\right)\right].$$

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 $d+1$.

The rest of our extremal theorems now concern our circular variants. The following theorem is both more natural and easier to obtain than Theorem 1.19 below. Recall from Definition 1.8 that a line containing exactly three points of the set is also an ordinary circle.

Theorem 1.18 (Ordinary circles)**.**

(*i*) *If n is sufficiently large, the minimum number of ordinary circles spanned by a non-concyclic and non-collinear set of n points in $\mathbb{R}^2$ is equal to*

$$\begin{cases} \frac{1}{4}n^2 - n & \text{if } n \equiv 0 \pmod 4, \\ \frac{3}{8}n^2 - n + \frac{5}{8} & \text{if } n \equiv 1 \pmod 4, \\ \frac{1}{4}n^2 - \frac{1}{2}n & \text{if } n \equiv 2 \pmod 4, \\ \frac{3}{8}n^2 - \frac{3}{2}n + \frac{17}{8} & \text{if } n \equiv 3 \pmod 4. \end{cases}$$

(*ii*) *Let $C > 0$ be a sufficiently large absolute constant. If a set P of n points in $\mathbb{R}^2$ spans fewer than $\frac{1}{2}n^2 - Cn$ ordinary circles, then P lies on the union of two disjoint circles, or the union of a circle and a disjoint line.*

Note that the lower bound in part (*i*) of Theorem 1.18 is exactly the same as in Theorem 1.13, and in fact the constructions that meet this lower bound in both cases are related by stereographic projection. We will discuss this in Chapter 4, where we describe these constructions.

Part (*i*) of the following theorem solves Problem 6 in [14, Section 7.2], which asks to determine the supremum of all values c such that any n points in the plane, not all concyclic, spans at least $(c + o(1))n^2$ strict ordinary circles.

Theorem 1.19 (Strict ordinary circles)**.**

(*i*) *If n is sufficiently large, the minimum number of strict ordinary circles spanned by a non-concyclic and non-collinear set of n points in $\mathbb{R}^2$ is equal to*

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

(*ii*) *Let $C > 0$ be a sufficiently large absolute constant. If a set P of n points in $\mathbb{R}^2$ spans fewer than $\frac{1}{2}n^2 - Cn$ strict ordinary circles, then P lies on the union of two disjoint circles, or the union of a circle and a disjoint line.*

For even n, the bound in part (*i*) is attained by certain constructions on the union of two disjoint circles, while for odd n, the bound is attained by constructions on the union of a circle and a disjoint line. This is in contrast to Theorem 1.18, where constructions that are extremal can be contained in either the union of two circles or the union of a circle and a line regardless of the parity of n. We will describe all of these constructions in more detail in Chapter 4.

Theorem 1.20 (4-rich circles)**.**

(*i*) *If n is sufficiently large, the maximum number of 4-rich circles spanned by a set of n points in $\mathbb{R}^2$ is equal to*

$$\begin{cases} \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{5}{6}n & \text{if } n \equiv 0 \pmod 8, \\ \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{11}{24}n - \frac{1}{4} & \text{if } n \equiv 1,3,5,7 \pmod 8, \\ \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{7}{12}n - \frac{1}{2} & \text{if } n \equiv 2,6 \pmod 8, \\ \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{5}{6}n - 1 & \text{if } n \equiv 4 \pmod 8. \end{cases}$$

(*ii*) *Let $C > 0$ be a sufficiently large absolute constant. If a set P of n points in $\mathbb{R}^2$ spans more than $\frac{1}{24}n^3 - \frac{7}{24}n^2 + Cn$ 4-rich circles, then up to an inversion, P lies on a ellipse or a circular elliptic cubic curve.*

As with Theorem 1.18, the upper bound in part (*i*) of Theorem 1.20 is exactly the same as in Theorem 1.14, and the constructions that meet this upper bound in both cases are related by stereographic projection. We will again discuss this in Chapter 4, where we describe these constructions. Note that Theorem 1.20 remains true even if we do not count lines as degenerate circles. This is because we can apply an inversion to any set of n points spanning the maximum number of 4-rich circles in such a way that all 4-rich lines become circles.

Theorems 1.21 and 1.22 below are the circular analogues of Theorems 1.16 and 1.17 respectively, and we get them by stereographic projection. However, the situation is very different in odd dimensions, where the only construction meeting the lower bound for ordinary hyperspheres is the trivial example with all but one point contained in a hypersphere or a hyperplane, and we do not have a tight upper bound for $(d+2)$-rich hyperspheres.

Theorem 1.21 (Ordinary hyperspheres)**.** *Let $d \geqslant 3$ and let $n \geqslant Cd^4 2^d d!$ for some sufficiently large absolute constant $C > 0$. Let P be a set of n points in $\mathbb{R}^d$ where no $d+1$ points lie on a $(d-2)$-sphere or a $(d-2)$-flat. If P is not contained in a hypersphere or a hyperplane, then the minimum number of ordinary hyperspheres spanned by P is exactly $\binom{n-1}{d}$ if d is odd*

and is

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

if d is even.

If d is odd, this minimum is attained by $n-1$ points in a hypersphere or a hyperplane together with a point not in the hypersphere or hyperplane.

If $d = 2k$ is even, this minimum is attained by a coset of a subgroup of a bounded $(k-1)$-spherical rational normal curve of degree d or a k-spherical elliptic normal curve of degree $d+1$, and when $d+1$ and n are coprime, by $n-1$ points in a hypersphere or a hyperplane together with a point not in the hypersphere or hyperplane.

Theorem 1.22 ($(d+2)$-rich hyperspheres)**.** *Let $d \geqslant 3$ and let $n \geqslant Cd^4 2^d d!$ for some sufficiently large absolute constant $C > 0$. Let P be a set of n points in $\mathbb{R}^d$ where no $d+1$ points lie on a $(d-2)$-sphere or a $(d-2)$-flat. Then the maximum number of $(d+2)$-rich hyperspheres spanned by P is bounded above by*

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

and this bound is tight when d is even.

If $d = 2k$ is even, this maximum is attained by a coset of a subgroup of a bounded $(k-1)$-spherical rational normal curve of degree d or a k-spherical elliptic normal curve of degree $d+1$.

1.3 Outline

In Chapter 2, we describe the main tools needed to prove our theorems above. We first state some of Green and Tao's results on ordinary lines [25], and prove an extension of one of their additive combinatorial results so that it applies to our higher dimensional analogues. To leverage their results, we then introduce the necessary classical algebraic geometry. As mentioned in Section 1.1, this includes studying projections and inversions. In particular, we need to understand non-generic projections of algebraic curves and the relationship between inversion and stereographic projection. We end with

the statements of the 3- and 4-dimensional Elekes–Szabó theorems and a couple of their applications by Raz, Sharir, and De Zeeuw [50, 51], which we need to prove some of our extremal theorems.

In Chapter 3, we introduce the curves that are central to our results. As seen in the statement of our theorems in Section 1.2, we are particularly interested in algebraic curves of degree $d+1$ in d-space. These turn out to be either elliptic or rational, and we examine each type in turn. The main goal of the chapter is to define group laws on these curves that encode when points are contained in a hyperplane (or a hypersphere). While the elliptic case is well-studied, we could not find references for the rational case and thus consider this in detail. We also introduce special classes of curves in d-space that are invariant under inversion, which we call *spherical curves*. This is a higher dimensional analogue of the classical circular curves in the plane (see for instance [34]).

In Chapter 4, we describe constructions that are (near-)extremal, and count the number of ordinary hyperplanes and hyperspheres (as well as $(d+1)$-rich hyperplanes and $(d+2)$-rich hyperspheres) they span. These include prisms, antiprisms, 'aligned' and 'offset' double polygons, and cosets of the curves introduced in Chapter 3. We find exact values for the number of ordinary and 4-rich planes and circles spanned, and asymptotic values for hyperplanes and hyperspheres. In the latter case, we provide a recursive method to calculate the exact values for a given d, and present these values for $d = 4, 5, 6$.

In Chapter 5, we prove the structure theorems stated in Section 1.2.1. We first prove the structure theorem for sets spanning few ordinary planes, which plays the role of the base case of the inductive proof of the structure theorem for sets spanning few ordinary hyperplanes. The 3-dimensional case turns out to be trickier than the higher dimensional cases. The circular variants are proved by stereographic projection from the (plane and) hyperplane versions. We also give an alternative proof of a (slightly weaker) structure theorem for sets spanning few ordinary circles based only on inversion and Green and Tao's structure theorem for sets spanning few ordinary lines (Theorem 2.1, which is a weaker restatement of Theorem 1.3).

In Chapter 6, we prove the extremal theorems stated in Section 1.2.2. It turns out that sets spanning many 4-rich planes span few ordinary planes, and the same goes for hyperplanes, circles, and hyperspheres. Thus by our structure theorems, extremal constructions differ in at most a bounded number of points from one of a few configurations, and we look at each case in turn. Combining this with our analysis of the constructions described in Chapter 4 then establishes our precise statements.

1.4 Notation

Asymptotics

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 $-CB \leqslant A \leqslant 0$. By $A = \Omega(B)$, we mean $B = O(A)$. None of the $O(\cdot)$ or $\Omega(\cdot)$ statements in this thesis have implicit dependence on the dimension d.

Projective space

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 $\mathbb{FP}^d$ by a $(d+1)$-dimensional vector $[x_0, x_1, \ldots, x_d]$, and identify the affine part where $x_0 \neq 0$ with $\mathbb{F}^d$. We call the hyperplane defined by $x_0 = 0$ the *hyperplane at infinity*, and denote it by Π_∞. Similarly, points on Π_∞ are referred to as *points at infinity*. 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.

Algebraic geometry

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 denote the Zariski closure of a set $S \subseteq \mathbb{CP}^d$ by $\overline{S}$. 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. In particular, we consider a *space curve* to be a non-degenerate curve in $\mathbb{FP}^3$. We say that a curve is *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.

Hyperspheres

By a hypersphere in $\mathbb{R}^d$, we mean a $(d-1)$-dimensional variety defined by the equation $(x_1 - a_1)^2 + \cdots + (x_d - a_d)^2 = r^2$ for some $a_1, \ldots, a_d \in \mathbb{R}$ and $r > 0$. Let $\mathbb{S}^{d-1}$ denote the hypersphere in $\mathbb{C}^d$ with equation $x_1^2 + \cdots + x_d^2 = 1$, so that its Zariski closure is the projective variety $\overline{\mathbb{S}^{d-1}} \subset \mathbb{CP}^d$ defined by the homogeneous equation $x_0^2 = x_1^2 + \cdots + x_d^2$. The *north pole* of $\overline{\mathbb{S}^{d-1}}$ is the point $N := [1, 0, \ldots, 0, 1]$. We call the intersection $\overline{\mathbb{S}^{d-1}} \cap \Pi_\infty$ the *imaginary sphere at infinity* and denote it by Σ_∞. This is a $(d-2)$-sphere on Π_∞ and is the intersection of Π_∞ with the Zariski closure of any hypersphere in $\mathbb{C}^d$. As with k-flats, we call the k-dimensional generalisation of a sphere in $\mathbb{FP}^d$ a *k-sphere*; thus a 0-sphere consists of two points, a 1-sphere is a circle, a 2-sphere is a sphere, and a $(d-1)$-sphere is a hypersphere.

Chapter 2

Tools

In this chapter, we detail the tools needed to help prove our results. This includes Green and Tao's work on ordinary lines, some classical algebraic geometry, and the Elekes–Szabó theorem.

The main strategy in proving our structure theorems stated in Section 1.2.1 is to leverage other structure theorems, starting with the structure theorem for sets spanning few ordinary lines. Since these structure theorems all state that certain sets lie mostly on algebraic curves, algebraic geometry, especially classical algebraic geometry of curves, is the main tool we need. The 3- and 4-dimensional Elekes–Szabó theorems and their applications then help us with some of the counting we do to prove our extremal theorems concerning planes and circles.

2.1 Ordinary lines

We first restate Theorem 1.3, Green and Tao's structure theorem for sets spanning few ordinary lines [25], in a weaker form that is sufficient for our purposes. We use this in Section 5.3 to prove Theorem 5.15, which is a weaker Theorem 1.11, our structure theorem for sets spanning few ordinary circles, but with a more elementary proof. Note that we can take $n \geqslant \exp\exp(CK^C)$ in the following theorem for some sufficiently large absolute constant $C > 0$, but we make no use of this explicit bound.

Theorem 2.1 (Green–Tao [25, Theorem 1.5])**.** *Let $K > 0$ and suppose n is sufficiently large depending on K. If a set P of n points in $\mathbb{RP}^2$ spans at most Kn ordinary lines, then P differs in at most $O(K)$ points from a configuration of one of the following types:*

(*i*) *$n - O(K)$ points on a line;*

(*ii*) *m points each on a conic and a disjoint line, for some $m = n/2 \pm O(K)$;*

(*iii*) *$n \pm O(K)$ points on an elliptic or acnodal cubic curve.*

As mentioned in Section 1.1, sets spanning few ordinary lines thus are contained in a cubic curve, which is possibly non-irreducible.

To prove Theorem 1.9, our structure theorem for sets spanning few ordinary planes, and thus the rest of our structure theorems, we use instead Green and Tao's intermediate structure theorem for sets spanning few ordinary lines, stated below. While the conclusions might be weaker than in Theorems 1.3 or 2.1, there is no bound on n.

Theorem 2.2 (Green–Tao [25, Proposition 5.3])**.** *Let P be a set of n points in $\mathbb{RP}^2$, spanning at most Kn ordinary lines, for some $K \geqslant 1$. Then we have one of the following:*

(*i*) *P is contained in the union of $O(K)$ lines and an additional $O(K^6)$ points;*

(*ii*) *P lies on the union of an irreducible conic σ and an additional $O(K^4)$ lines, with $|P \cap \sigma| = n/2 \pm O(K^5)$;*

(*iii*) *P is contained in the union of an irreducible cubic curve and an additional $O(K^5)$ points.*

The following two lemmas help us get more precise descriptions of sets that lie on certain cubic curves and span few ordinary lines. Green and Tao used them to bridge the gap from from Theorem 2.2 to Theorem 1.3, but the bound on n is still modest.

Lemma 2.3 (Green–Tao [25, Lemma 7.4])**.** *Let P be a set of n points in $\mathbb{RP}^2$ spanning at most Kn ordinary lines, and suppose $n \geqslant CK$ for some sufficiently large absolute constant $C > 0$. Suppose all but K points of P lie on the union of an irreducible conic σ and a line ℓ, with $n/2 \pm O(K)$ points of P on each of σ and ℓ. Then up to a projective transformation, P differs in at most $O(K)$ points from the vertices of a regular m-gon and the m points at infinity corresponding to the diagonals of the m-gon, for some $m = n/2 \pm O(K)$.*

For the group structure on cubic curves mentioned in the following lemma, see [25, Section 2] or Chapter 3.

Lemma 2.4 (Green–Tao [25, Lemma 7.2])**.** *Let P be a set of n points in $\mathbb{RP}^2$ spanning at most Kn ordinary lines, and suppose $n \geqslant CK$ for some sufficiently large absolute constant $C > 0$. Suppose all but K points of P lie on an irreducible cubic γ. Then P differs in at most $O(K)$ points from a coset of a subgroup of γ^*, the smooth points of γ. In particular, γ is either an elliptic or acnodal cubic curve.*

To get the cosets on the curves in the lemmas above (there is also an underlying group structure in Lemma 2.3), Green and Tao used the following additive combinatorial result. It captures the principle that if a finite subset of a group is almost closed, then it is close to a subgroup.

Proposition 2.5 (Green–Tao [25, Proposition A.5])**.** *Let A, B, C be three subsets of some abelian group $(G, \oplus)$, all of size within K of n, where $K \leqslant cn$ for some sufficiently small absolute constant $c > 0$ independent of G. Suppose there are at most Kn pairs $(a, b) \in A \times B$ for which $a \oplus b \notin C$. Then there is a finite subgroup H of G and cosets $H \oplus x$, $H \oplus y$ such that*

$$|A \triangle (H \oplus x)|, |B \triangle (H \oplus y)|, |C \triangle (H \oplus x \oplus y)| = O(K).$$

We extend the above proposition from three sets to $d + 1$ sets, which helps to get cosets on curves in d dimensions.

Lemma 2.6. *Let $d \geqslant 2$. Let $A_1, A_2, \ldots, A_{d+1}$ 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 $c > 0$ independent of G. Suppose there are at most Kn^{d-1} d-tuples $(a_1, a_2, \ldots, a_d) \in A_1 \times A_2 \times \cdots \times A_d$ for which $a_1 \oplus a_2 \oplus \cdots \oplus a_d \notin A_{d+1}$. Then there is a finite subgroup H of G and cosets $H \oplus x_i$ for $i = 1, \ldots, d$ 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 Proposition 2.5.

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 $(a_2, \ldots, a_d) \in A_2 \times \cdots \times A_d$ 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 $x_2, \ldots, x_d \in G$ such that for $j = 2, \ldots, d$ 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

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

$$\leqslant \left(1 + \frac{C_2 c}{d^2 - c}\right) K n^{d-2}$$
$$\leqslant \left(1 + \frac{1}{d^2}\right) K n^{d-2}$$

$(d-1)$-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 exists a subgroup H' of G and $x_1, x'_2, \dots, x'_{d-1} \in G$ 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

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

Finally, we need the following two technical lemmas. These help reduce the polynomial errors in Theorem 2.2 to linear errors as in Theorem 1.3, Theorem 2.1, and our structure theorems.

Lemma 2.7 (Green–Tao [25, Corollary 7.6])**.** *Let $X_{2m} \subset \mathbb{RP}^2$ be the vertex set of a regular m-gon centred at the origin $[1, 0, 0]$ together with the m points at infinity corresponding to the diagonals of the m-gon. Let p be a point not on the line at infinity, not the origin, and not a vertex of the m-gon. Then at least $2m - O(1)$ of the $2m$ lines joining p to a point of X_{2m} do not pass through any further point of X_{2m}.*

Lemma 2.8 (Green–Tao [25, Lemma 7.7]). *Let γ^* be an elliptic cubic curve or the smooth points of an acnodal cubic curve. Let X be a coset of a finite subgroup of γ^* of order n, where n is greater than a sufficiently large absolute constant. If $p \in \mathbb{RP}^2 \setminus \gamma^*$, then there are at least $n/1000$ lines through p that pass through exactly one point in X.*

2.2 Classical algebraic geometry

We now look at the algebraic geometry needed to leverage the results on ordinary lines in the previous section. We focus on planes and hyperplanes in Section 2.2.2, since projection maps flats to flats, and focus on circles and hyperspheres in Section 2.2.3, since inversion maps spheres (and flats) to spheres (and flats).

2.2.1 Bézout's theorem

Bézout's theorem gives the degree of an intersection of varieties. While it is often formulated as an equality, we mostly 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 2.9 (Bézout [23, Section 2.3]). *Let X and Y be varieties in $\mathbb{CP}^d$ with no common irreducible component. Then $\deg(X \cap Y) \leqslant \deg(X) \deg(Y)$.*

When we deal with ordinary hyperspheres, we need the following formulation of Bézout's theorem instead. Two pure-dimensional varieties X and Y in $\mathbb{CP}^d$ intersect *properly* if $\dim(X \cap Y) = \dim(X) + \dim(Y) - d$.

Theorem 2.10 (Bézout [29, Theorem 18.4]). *Let X and Y be varieties of pure dimension in $\mathbb{CP}^d$ that intersect properly. Then the total degree of $X \cap Y$ is equal to $\deg(X) \deg(Y)$, counting multiplicity.*

2.2.2 Projection

We focus on planes and hyperplanes in this section.

Definition 2.11. 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.

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.

The main reason why projections are important for us is the following. Let P be a finite set in $\mathbb{RP}^d$ where every d points span a hyperplane. If we project $P \setminus \{p\}$ from a point $p \in P$, all ordinary hyperplanes spanned by P that contain p map to ordinary hyperplanes spanned by $\pi_p(P \setminus \{p\})$ in $\mathbb{RP}^{d-1}$. Also, since every d points in P span a hyperplane in $\mathbb{RP}^d$, every $d-1$ points in $\pi_p(P \setminus \{p\})$ span a hyperplane in $\mathbb{RP}^{d-1}$. Thus we can use structure theorems in $\mathbb{RP}^{d-1}$, starting with Green and Tao's structure theorems for sets spanning few ordinary lines. But to successfully do so requires a thorough understanding of projections of curves, since the structure theorems tell us up to a bounded number of points, our point set is contained in (a coset of) a curve (or a hyperplane, which is easy to deal with).

However, results in classical algebraic geometry are usually formulated only for smooth varieties and for generic points. Since we are working with extremal problems, there is no guarantee that the curves on which the points lie are smooth; on the contrary, it should not be surprising that singularities occur in extremal objects. Although it turns out that the curves that we consider are smooth in the generic case, curves with singularities also appear. Thus our tools have to deal with singular curves as well. Consider also the following definition and proposition, which we use over and over implicitly.

Definition 2.12. Let $\delta \subset \mathbb{CP}^d$ be an irreducible non-degenerate 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 $\delta \setminus \{p\}$ [29, p. 77].)

Proposition 2.13 ([29, Example 18.16; 39, Section 1.15]). *Let $\delta \subset \mathbb{CP}^d$ be an irreducible non-degenerate curve of degree e. 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 .*

In the projections that we will make, we will not have complete freedom in choosing a projection point, and therefore we cannot guarantee that π_p is generically one-to-one on δ. For this reason, we will need more sophisticated results on the projection of curves from a point. We start with the following more elementary proposition, which is a restatement of [4, Lemma 6.6].

Proposition 2.14. *Let σ_1 and σ_2 be two irreducible conics given by the intersection of two distinct planes and a quadric surface in $\mathbb{CP}^3$. Then there are at most two quadric cones containing both σ_1 and σ_2.*

We define a *trisecant* of an irreducible non-degenerate curve δ in $\mathbb{CP}^d$ to be a line that intersects δ in at least three distinct points, or that can be approximated in the Zariski topology by such lines. The classical trisecant lemma states that the number of points on an irreducible non-degenerate curve in $\mathbb{CP}^d$ that lie on infinitely many trisecants is finite [1, pp. 109–111; 56, p. 85, footnote]. The following generalisation of the trisecant lemma applies to curves that are not necessarily irreducible.

Lemma 2.15 (Trisecant lemma [35, Theorem 2]). *Let δ be a curve in $\mathbb{CP}^d$, $d \geqslant 3$, such that no union of irreducible components contained in a plane has total degree at least 3. Then the number of points on δ that lie on infinitely many trisecants of δ is finite.*

Note that a point p on a non-degenerate curve δ lies on infinitely many trisecants of δ if and only if the projection π_p is not generically one-to-one on δ. Thus, according to the trisecant lemma there are finitely many such projection points on δ. The following special case of a theorem of Segre [54] shows that there are also finitely many such projection points not on δ.

Proposition 2.16 (Segre [54])**.** *Let δ be an irreducible non-degenerate curve in $\mathbb{CP}^d$, $d \geqslant 3$. Then the set of points*

$$X = \left\{ x \in \mathbb{CP}^d \setminus \delta : \pi_x \text{ is not generically one-to-one on } \delta \right\}$$

is finite.

We now prove three quantitative versions of the trisecant lemma, which all state that most projections are well-behaved. For a curve δ and a point p in $\mathbb{CP}^d$, denote the cone over δ with vertex p by $C_p(\delta)$, that is,

$$C_p(\delta) := \overline{\pi_p^{-1}(\pi_p(\delta \setminus \{p\}))}.$$

The following result is the 1-dimensional case of a result of Ballico [7]; see also [8, Remark 1]. We provide the proof of this special case for convenience.

Lemma 2.17. *Let δ be an irreducible non-degenerate 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.*

Proof. By Proposition 2.16, the set

$$X = \left\{ x \in \mathbb{CP}^d \setminus \delta : \pi_x \text{ is not generically one-to-one on } \delta \right\}$$

is finite, and we want to show that $|X| = O(e^3)$.

We first characterise X as an intersection of cones $C_p(\delta)$ for some $p \in \delta$. Let $x \in X$. Since δ has finitely many singularities and there are only finitely many lines through x that are tangent to δ, we have that for all but finitely many points $p \in \delta$, the line px intersects δ in a third point, that is, $x \in C_p(\delta)$ for all $p \in \delta \setminus E_x$, for some finite subset E_x of δ. Let $\delta' = \delta \setminus \bigcup_{x \in X} E_x$ and $S = \bigcap_{p \in \delta'} C_p(\delta)$. Then clearly $X \subseteq S \setminus \delta$. Conversely, if $x \in S \setminus \delta$, then for any $p \in \delta'$, the line px intersects δ with multiplicity at least 2. Since only finitely many lines through x can be tangent to δ, it follows that for all but finitely many points $p \in \delta$, the line px intersects δ in a third point, hence $x \in X$. This shows that $X = S \setminus \delta$.

We next show that X is essentially contained in the intersection of three cones and use Bézouts theorem (Theorem 2.9) to bound the number of

points in this intersection. Fix distinct $p, p' \in \delta'$. Then $X \subseteq C_p(\delta) \cap C_{p'}(\delta)$. This intersection consists of δ, the line pp', and some further irreducible curves $\delta_1, \ldots, \delta_k$ of total degree at most $e^2 - e - 1$, by Bézout's theorem (Theorem 2.9).

If some $\delta_i \subset C_p(\delta)$ for all $p \in \delta'$, then $\delta_i \subseteq S$, and since $\delta_i \cap \delta$ is finite by Bézout's theorem (Theorem 2.9), we obtain that X is infinite, a contradiction. Therefore, for each δ_i there is a point $p_i \in \delta'$ such that $\delta_i \not\subset C_{p_i}(\delta)$. By Bézout's theorem (Theorem 2.9), $|X \cap \delta_i| \leqslant |C_{p_i}(\delta) \cap \delta_i| \leqslant e \deg(\delta_i)$. It follows that $|X \setminus pp'| \leqslant \sum_{i=1}^{k} |X \cap \delta_i| \leqslant \sum_{i=1}^{k} e \deg(\delta_i) = O(e^3)$.

Now find a third point $p'' \in \delta'$ such that p, p', p'' are not collinear. As before, $|X \setminus pp''| = O(e^3)$. Since $pp' \cap pp''$ is a singleton, it follows that $|X| = O(e^3)$. □

If an irreducible non-planar curve δ of degree e in $\mathbb{RP}^3$ is smooth, then by a well-known result going back to Cayley (see [9, 12, 26]), the trisecant variety of δ (the Zariski closure in $\mathbb{CP}^3$ of the union of all trisecants of δ) has degree $O(e^3)$. For $p \in \delta$, if π_p restricted to $\delta \setminus \{p\}$ is not generically one-to-one, then $C_p(\delta)$ is a component of the trisecant variety and has degree at least 2. It follows that there can be at most $O(e^3)$ points $p \in \delta$ such that π_p is not generically one-to-one on δ.

However, if δ is not smooth, we are not aware of any estimates of the degree of the trisecant variety, and we thus include the proof of the weaker bound $O(e^4)$ below in Lemma 2.19, based on an argument of Furukawa [24]. This lemma answers the 1-dimensional case of a question of Ballico [8, Question 1].

We say that a point $z \in Z$ is a *vertex* of a surface Z in $\mathbb{CP}^3$ if the projection $\overline{\pi_z(Z \setminus \{z\})}$ is a planar curve with Z equal to the cone $C_z(\overline{\pi_z(Z \setminus \{z\})})$. Furukawa [24] characterised vertices of a surface in terms of partial derivatives, which we state below as Lemma 2.18, and include his proof for completeness. For any 4-tuple of non-negative integers $\boldsymbol{i} = (i_0, i_1, i_2, i_3)$, we define $|\boldsymbol{i}| = i_0 + i_1 + i_2 + i_3$. For any homogeneous polynomial $f \in \mathbb{C}[x_0, x_1, x_2, x_3]$

of degree e', we define

$$D_{\boldsymbol{i}} f = \frac{1}{i_0! i_1! i_2! i_3!} \frac{\partial^{i_0}}{\partial x_0^{i_0}} \frac{\partial^{i_1}}{\partial x_1^{i_1}} \frac{\partial^{i_2}}{\partial x_2^{i_2}} \frac{\partial^{i_3}}{\partial x_3^{i_3}} f.$$

Let Df be the column vector $[D_{\boldsymbol{i}} f]_{\boldsymbol{i}}$, where $\boldsymbol{i}$ varies over all 4-tuples such that $|\boldsymbol{i}| = e' - 1$. Then Df is an $\binom{e'+2}{3}$-dimensional vector of linear forms in x_0, x_1, x_2, x_3.

Lemma 2.18 ([24, Lemma 2.3])**.** *Let $Z = Z_{\mathbb{C}}(f)$ be the surface in $\mathbb{CP}^3$ defined by a homogeneous polynomial $f \in \mathbb{C}[x_0, x_1, x_2, x_3]$ of degree e'. Then $z \in Z$ is a vertex of Z if and only if $(Df)(z)$ is the zero vector.*

Proof. Let $z \in Z$. Note that if $Z' = Z_{\mathbb{C}}(f')$ is obtained from Z by a projective transformation φ, then by the chain rule, we have $(Df')(\varphi(z)) = 0$ if and only if $(Df)(z) = 0$. We may thus assume without loss of generality that $z = [0, 0, 0, 1]$. Let $\boldsymbol{I}$ be the set of 4-tuples $\boldsymbol{i} = (i_0, i_1, i_2, i_3)$ of non-negative integers such that $|\boldsymbol{i}| = i_0 + i_1 + i_2 + i_3 = e' - 1$, and let $\boldsymbol{J}$ be the set of 4-tuples $\boldsymbol{j} = (j_0, j_1, j_2, j_3)$ of non-negative integers such that $|\boldsymbol{j}| = j_0 + j_1 + j_2 + j_3 = e'$.

If z is a vertex of Z, then f is independent of x_3, hence $(D_{\boldsymbol{i}} f)(z) = 0$ for each $\boldsymbol{i} \in \boldsymbol{I}$, and so $(Df)(z) = 0$.

Conversely, let $f = \sum_{\boldsymbol{j} \in \boldsymbol{J}} f_{\boldsymbol{j}} x_0^{j_0} x_1^{j_1} x_2^{j_2} x_3^{j_3}$ where $f_{\boldsymbol{j}} \in \mathbb{C}$, and suppose $(Df)(z)$ is the zero vector. For $\boldsymbol{i} \in \boldsymbol{I}$, let $\boldsymbol{i} + \boldsymbol{\omega}$ denote the 4-tuple $(i_0, i_1, i_2, i_3 + 1) \in \boldsymbol{J}$. Then $(D_{\boldsymbol{i}} f)(z) = (i_3 + 1) f_{\boldsymbol{i} + \boldsymbol{\omega}} = 0$ for each $\boldsymbol{i} \in \boldsymbol{I}$, and so we must have $f_{\boldsymbol{j}} = 0$ for all $\boldsymbol{j} \in \boldsymbol{J}$ with $j_3 \neq 0$. This implies f is independent of x_3, and thus z is a vertex of Z. □

Lemma 2.19. *Let δ be an irreducible non-degenerate curve of degree e in $\mathbb{CP}^d$, $d \geqslant 3$. Then there are at most $O(e^4)$ points x on δ such that π_x restricted to $\delta \setminus \{x\}$ is not generically one-to-one.*

Proof. We first prove the $d = 3$ case. Let X be the set of points x on δ such that π_x restricted to $\delta \setminus \{x\}$ is not generically one-to-one. Let $V \subseteq \mathbb{C}[x_0, x_1, x_2, x_3]$ be the vector space of homogeneous polynomials of degree $e - 2$ that vanish on δ, and let $h_1, \ldots, h_r$ be a basis of V. Consider the matrix $A = [Dh_1, \ldots, Dh_r]$.

Suppose first that $x \in X$. Then $\deg(\overline{\pi_x(\delta \setminus \{x\})}) \leqslant e-2$, and there exists a cone of degree at most $e-2$ with vertex x containing δ. It follows that there is a polynomial $f \in V$ such that $Z_{\mathbb{C}}(f)$ contains δ. By Lemma 2.18, the rank of $A(x) = [Dh_1(x), \ldots, Dh_r(x)]$ is less than r, so each $r \times r$ minor of A vanishes at x. Note that each such minor defines a surface of degree at most r. Conversely, if x lies on all of the surfaces defined by the $r \times r$ minors of A, then $A(x)$ has rank less than r. There then exists $f \in V$ such that $(Df)(x)$ is the zero vector. By Lemma 2.18, x is a vertex of $Z_{\mathbb{C}}(f)$, which is a surface of degree at most $e-2$ and contains $\pi_x(\delta \setminus \{x\})$, so either x is a singular point of δ or $x \in X$.

Since δ has at most $O(e^2)$ singular points, it will follow that X has at most $O(e^4)$ points if we can show that there are at most $O(e^4)$ points in

$$\delta \cap \left\{x \in \mathbb{CP}^3 : \operatorname{rank}(A(x)) < r\right\}.$$

Now X is finite by the trisecant lemma (Lemma 2.15), so δ is not a subset of all of the surfaces defined by the $r \times r$ minors of $A(x)$. Fix one such surface Z not containing δ. It has degree at most r, so by Bézout's theorem (Theorem 2.9), $\delta \cap Z$ has at most er points. Since $r = O(e^3)$, the $d = 3$ case follows.

We now proceed by induction on d. Assume $d \geqslant 4$ and that the lemma holds in dimension $d-1$. Since $d > 3$ and the dimension of secant variety of δ (the Zariski closure of the set of points in $\mathbb{CP}^d$ that lie on a line through some two points of δ) is at most 3 [29, 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 an algebraic 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. □

We remark that we have no reason to believe that the estimate $O(e^4)$ in the above lemma is best possible.

Lemma 2.20. *Let δ_1 and δ_2 be two irreducible non-planar curves in $\mathbb{CP}^d$, $d \geqslant 3$, of degrees e_1 and e_2 respectively. Then there are at most $O(e_1e_2)$ points x on δ_1 such that $\overline{\pi_x(\delta_1 \setminus \{x\})}$ and $\overline{\pi_x(\delta_2 \setminus \{x\})}$ coincide.*

Proof. Let $X = \left\{x \in \delta_1 : \overline{\pi_x(\delta_1 \setminus \{x\})} = \overline{\pi_x(\delta_2 \setminus \{x\})}\right\}$, and let

$$S = \delta_1 \cap \bigcap_{p \in \delta_1 \setminus \delta_2} C_p(\delta_2).$$

We claim that $X \setminus \delta_2 = S \setminus \delta_2$.

First, let $x \in X \setminus \delta_2$ and $p \in \delta_1 \setminus \delta_2$. If $x = p$, then clearly $x \in C_p(\delta_2)$. Otherwise, $\pi_x(p) \in \pi_x(\delta_1 \setminus \{x\})$. Since $x \in X$, $\overline{\pi_x(\delta_1 \setminus \{x\})} = \overline{\pi_x(\delta_2 \setminus \{x\})}$, and since $x \notin \delta_2$, $\overline{\pi_x(\delta_2 \setminus \{x\})} = \pi_x(\delta_2 \setminus \{x\})$. Therefore, $\pi_x(p) \in \pi_x(\delta_2 \setminus \{x\})$, and it follows that the line px intersects δ_2, hence $x \in C_p(\delta_2)$. Since $X \subseteq \delta_1$, we conclude that $x \in S \setminus \delta_2$.

Conversely, let $x \in S \setminus \delta_2$. Then $x \in \delta_1$, and for all $p \in \delta_1 \setminus \delta_2$, we have $x \in C_p(\delta_2)$. Thus, if $x \neq p$, then the line px intersects δ_2. Therefore, $\pi_x(\delta_1 \setminus \{x\}) \subseteq \pi_x(\delta_2 \setminus \{x\})$. Since δ_2 is irreducible, the curve $\overline{\pi_x(\delta_2 \setminus \{x\})}$ is irreducible. Since δ_1 is not a line, $\overline{\pi_x(\delta_1 \setminus \{x\})}$ does not degenerate to a point. Therefore, $\overline{\pi_x(\delta_1 \setminus \{x\})} = \overline{\pi_x(\delta_2 \setminus \{x\})}$, and $x \in X$.

Next, note that each $x \in S$ lies on infinitely many trisecants of the curve $\delta_1 \cup \delta_2$. Since both δ_1 and δ_2 are non-planar, S is finite by the trisecant lemma (Lemma 2.15). Therefore, $\delta_1 \not\subset C_p(\delta_2)$ for some $p \in \delta_1 \setminus \delta_2$. By Bézout's theorem (Theorem 2.9), $|S| \leqslant |\delta_1 \cap C_p(\delta_2)| \leqslant e_1 \deg(C_p(\delta_2)) \leqslant e_1e_2$. Again by Bézout's theorem (Theorem 2.9), $|\delta_1 \cap \delta_2| \leqslant e_1e_2$. It then follows that $|X| \leqslant |X \setminus \delta_2| + |\delta_1 \cap \delta_2| = |S \setminus \delta_2| + |\delta_1 \cap \delta_2| \leqslant 2e_1e_2$. □

2.2.3 Inversion

We focus on circles and hyperspheres in this section.

A key tool in the earlier papers [3, 20, 68] on the (strict) ordinary circles problem is inversion; the first to use inversion in Sylvester–Gallai type problems was Motzkin [46]. The simple reason for the relevance of inversion is that if we invert in a point of the given set, an ordinary circle through that point is mapped to an ordinary line. Thus we can use results on ordinary lines, like those of Green and Tao [25] in Section 2.1, to deduce results about ordinary circles.

Inversion is also a main tool in our proof of Theorem 5.15. However, the main tool in our proofs of Theorems 1.11 and 1.12, our structure theorems for sets defining few circles and hyperspheres, is stereographic projection. In fact, inversion can be defined in terms of stereographic projection, and we do so in Definition 2.22 below.

Definition 2.21. *Stereographic projection* is defined to be the map

$$\pi : \mathbb{CP}^{d+1} \supset \overline{\mathbb{S}^d} \setminus \{N\} \to \{x_{d+1} = 0\} = \mathbb{CP}^d,$$

where N is the north pole of $\overline{\mathbb{S}^d}$, and $q \in \overline{\mathbb{S}^d} \setminus \{N\}$ is mapped to the intersection point of the line Nq and the hyperplane $\{x_{d+1} = 0\}$, which we identify with $\mathbb{CP}^d$.

Recall from Section 1.4 that the imaginary sphere at infinity Σ_∞ in $\mathbb{CP}^d$ is defined as the intersection of the unit hypersphere $\overline{\mathbb{S}^{d-1}}$ and the hyperplane at infinity Π_∞. It is not difficult to see that $\pi(\Pi_N \cap \overline{\mathbb{S}^d} \setminus \{N\}) = \Sigma_\infty$, where Π_N is the tangent hyperplane to $\overline{\mathbb{S}^d}$ at N. The image of π is thus $\{x_0 \neq 0\} \cup \Sigma_\infty = \mathbb{C}^d \cup \Sigma_\infty$. Also, π is injective on $\overline{\mathbb{S}^d} \setminus \Pi_N$, and for each $y \in \Sigma_\infty$, $\pi^{-1}(y) = \ell \setminus \{N\}$, where ℓ is the tangent line to $\overline{\mathbb{S}^d}$ at N through y.

To see why stereographic projection is relevant, consider the following. Let P be a finite set in $\mathbb{R}^d$ where no $d+1$ points lie on a $(d-2)$-sphere or a $(d-2)$-flat. If we project P onto $\overline{\mathbb{S}^d}$ stereographically, all ordinary hyperspheres spanned by P map to ordinary hyperplanes spanned by $\pi^{-1}(P) \subset \mathbb{R}^{d+1}$, and they are in one-to-one correspondence. Since we have in $\pi^{-1}(P)$ that every $d+1$ points span a hyperplane, we can use our structure theorem for sets spanning few ordinary hyperplanes. As with projection in the previous section, to do so successfully requires a thorough understanding of

how curves behave under stereographic projection, and we consider this in Section 3.3.

We now define inversion in terms of stereographic projection.

Definition 2.22. *Inversion in the origin* $o \in \mathbb{C}^d$ is defined to be the bijective map

$$\iota_o = \pi \circ \rho \circ \pi^{-1} : \mathbb{C}^d \setminus \{o\} \to \mathbb{C}^d \setminus \{o\},$$

where ρ is the orthogonal reflection map in the hyperplane $\{x_{d+1} = 0\}$.

Inversion in an arbitrary point $r \in \mathbb{C}^d$ is then defined to be the bijective map

$$\iota_r = \tau_r \circ \iota_o \circ \tau_{-r} : \mathbb{C}^d \setminus \{r\} \to \mathbb{C}^d \setminus \{r\},$$

where $\tau_r(x) = x + r$ is the translation map taking the origin to r.

Note that this agrees with the more standard definition of inversion in the real plane, where $\iota_r : \mathbb{R}^2 \setminus \{r\} \to \mathbb{R}^2 \setminus \{r\}$ defined be

$$\iota_r(x, y) = \left(\frac{x - x_r}{(x - x_r)^2 + (y - y_r)^2} + x_r, \frac{y - y_r}{(x - x_r)^2 + (y - y_r)^2} + y_r \right)$$

for $(x, y) \neq r = (x_r, y_r)$.

As is well-known in real space, if V is a hypersphere or a hyperplane, then the inverse $\overline{\iota_r(V \setminus \{r\})}$ is again a hypersphere or a hyperplane, depending on whether $r \notin V$ or $r \in V$ respectively. It is also easily seen that the inverse of a circle or a line is again a circle or a line. We note that the image of an algebraic curve under stereographic projection or inversion is again an algebraic curve in the following sense.

Definition 2.23. For any curve δ in $\mathbb{CP}^d$ there is a curve δ' in $\mathbb{CP}^d$ such that $\overline{\iota_r(\delta \setminus \{r\})} = \delta'$. We refer to δ' as the *inverse of* δ *in the point* r.

In Section 3.3, we introduce spherical curves, a special class of curves that are closed under inversion, and explore their interaction with stereographic projection.

2.3 The Elekes–Szabó theorem

Theorems 2.24 and 2.26 below are the 3- and 4-dimensional Elekes–Szabó theorems by Raz, Sharir, and De Zeeuw [50,51] respectively. Their relevance to our results are evident in their applications to counting collinear triples in the plane and coplanar quadruples in 3-space [50, 51], which are Theorems 2.25 and 2.27 below. We use Theorem 2.25 to help us count ordinary planes and circles, and Theorem 2.26 to prove Theorem 1.15, our result on coplanar quadruples, complementing Theorem 2.27. We state Theorem 2.24 for completeness.

Theorem 2.24 (Raz–Sharir–De Zeeuw [50, Theorem 1.1])**.** *Let F be an irreducible polynomial of degree d in $\mathbb{C}[t_1, t_2, t_3]$, with no $\partial F/\partial t_i$ identically zero. Then either for all $A \subset \mathbb{C}$ with $|A| = n$, we have $|Z_{\mathbb{C}}(F) \cap A^3| = O(d^{13/2}n^{11/6})$, or there exists a 1-dimensional subvariety $Z_0 \subset Z_{\mathbb{C}}(F)$ such that for any $(s_1, s_2, s_3) \in Z_{\mathbb{C}}(F) \setminus Z_0$, there exist open neighbourhoods U_i of s_i and injective analytic functions $\varphi_i : U_i \to \mathbb{C}$ such that*

$$F(t_1, t_2, t_3) = 0 \iff \varphi_1(t_1) + \varphi_2(t_2) + \varphi_3(t_3) = 0,$$

for all $(t_1, t_2, t_3) \in U_1 \times U_2 \times U_3$.

Theorem 2.25 (Raz–Sharir–De Zeeuw [50, Theorem 6.1])**.** *Let γ_1, γ_2, γ_3, be three (not necessarily distinct) irreducible algebraic curves of constant degree in $\mathbb{C}^2$, and let $S_1 \in \gamma_1$, $S_2 \in \gamma_2$, $S_3 \in \gamma_3$ be finite subsets. Then the number of collinear triples in $S_1 \times S_2 \times S_3$ is*

$$O\left(|S_1|^{\frac{1}{2}}|S_2|^{\frac{2}{3}}|S_3|^{\frac{2}{3}} + |S_1|^{\frac{1}{2}}\left(|S_1|^{\frac{1}{2}} + |S_2| + |S_3|\right)\right),$$

unless $\gamma_1 \cup \gamma_2 \cup \gamma_3$ is a line or a cubic curve.

Theorem 2.26 (Raz–Sharir–De Zeeuw [51, Theorem 1.1])**.** *Let F be an irreducible polynomial of constant degree in $\mathbb{C}[t_1, t_2, t_3, t_4]$, with no $\partial F/\partial t_i$ identically zero. Then either for all $A \subset \mathbb{C}$ with $|A| = n$, we have $|Z_{\mathbb{C}}(F) \cap A^4| = O(n^{8/3})$, or there exists a 2-dimensional subvariety $Z_0 \subset Z_{\mathbb{C}}(F)$ such that for any $(s_1, s_2, s_3, s_4) \in Z_{\mathbb{C}}(F) \setminus Z_0$, there exist open neighbourhoods U_i of s_i and injective analytic functions $\varphi_i : U_i \to \mathbb{C}$ such that*

$$F(t_1, t_2, t_3, t_4) = 0 \iff \varphi_1(t_1) + \varphi_2(t_2) + \varphi_3(t_3) + \varphi_4(t_4) = 0,$$

for all $(t_1, t_2, t_3, t_4) \in U_1 \times U_2 \times U_3 \times U_4$.

Theorem 2.27 (Raz–Sharir–De Zeeuw [51, Theorem 1.3])**.** *Let* δ *be an algebraic curve of constant degree in* $\mathbb{C}^3$*, and let* $S \subset \delta$ *be a finite set of size* n*. The the number of coplanar quadruples spanned by* S *is* $O(n^{8/3})$*, unless* δ *contains either a planar curve or a quartic curve.*

Chapter 3

Curves

In this chapter, we introduce the curves that appear in our theorems and describe their group structure, which encodes when points on the curve are contained in a hyperplane or a hypersphere. The main object of study here is an irreducible non-degenerate curve of degree $d+1$ in d-space, which appears in all of our structure theorems and gives rise to extremal constructions for all of our extremal theorems except for ordinary planes and circles. We first start with the following well-known classification (see for example [55, p. 38, Theorem VIII]), providing more detailed definitions later.

Proposition 3.1. *An irreducible non-degenerate curve of degree $d+1$ in $\mathbb{CP}^d$, $d \geqslant 2$, is either elliptic or rational.*

Proof. We proceed by induction on the dimension d. It is well-known that any irreducible cubic in $\mathbb{CP}^2$ is either elliptic or rational. Fix a $d \geqslant 3$ and suppose the result is true for dimension $d-1$. Let δ be an irreducible non-degenerate curve of degree $d+1$ in $\mathbb{CP}^d$. Choose a smooth projection point $p \in \delta$ such that π_p is generically one-to-one on δ, which is possible by the trisecant lemma (Lemma 2.15). Then $\delta' := \overline{\pi_p(\delta \setminus \{p\})}$ is an irreducible non-degenerate curve of degree d in $\mathbb{CP}^{d-1}$, which is elliptic or rational by the induction hypothesis. If δ' is elliptic, then δ is smooth and thus also elliptic, since the genus of a smooth curve is a birational invariant [30, Chapter III, Exercise 5.3]. If δ' is rational, then δ must also be rational since π_p is birational on δ. □

In 3-space, there is another classical classification of space quartics (see for example [60]). Since the dimension of the vector space of degree 2 homogeneous polynomials in four variables is 10, there exists a quadric surface Q containing any nine points of a space quartic δ. It then follows from Bézout's theorem (Theorem 2.9) that δ is contained in Q.

Definition 3.2. A space quartic in 3-space is of the *first species* if it is contained in at least two linearly independent quadrics. It is of the *second species* if it is contained in a unique quadric.

Since prisms and antiprisms (see Definition 4.3) are contained in two planar sections of a sphere, every curve that appears in Theorem 1.9, our structure theorem for sets spanning few ordinary planes, can be thought of as quartics (possibly non-irreducible) of the first species. We mention this classification mainly so that our structure theorem matches Ball's [4]. Elliptic quartics are always of the first species, and we will later show in Section 3.2 that rational quartics are of the first species if and only if they are singular.

It is well-known in the plane that we can define a group law on any elliptic cubic curve or the set of smooth points of a rational and 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 an elliptic 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 respectively. Over the real numbers, the group on an elliptic 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 [25] for a more detailed description.

In higher dimensions, it turns out that an irreducible non-degenerate curve of degree $d+1$ in d-space does not necessarily have a natural group structure, but if it does, the behaviour is similar to the planar case. In particular, elliptic curves and rational curves that are singular have a natural group

structure like their analogues in the plane, where $d+1$ points on the curve are contained in a hyperplane if and only if they sum to the identity. This also induces a group law on a special subset of these curves where $d+2$ points on the curve are contained in a hypersphere if and only if they sum to the identity. However, there exist rational curves that are smooth if $d \geqslant 3$, and these do not seem to have such a natural group structure.

The group laws, when they exist, are 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 shows that we always get uniqueness up to some translation.

Proposition 3.3. *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 $c, c' \in G$,*

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

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

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

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. □

We also note the following simple result for later use. Recall that a curve is real if each of its irreducible components contains infinitely many real points.

Lemma 3.4. *The homogeneous ideal of a real curve is generated by real polynomials.*

Proof. Without loss of generality, the real curve $\delta \subset \mathbb{CP}^d$ is irreducible. Let I be the homogeneous ideal of δ, and consider $I = \bigoplus_e I^{(e)}$, where $I^{(e)}$ is the set of polynomials of I of degree e. We show that each $I^{(e)}$ can be generated by real polynomials, whence so can I. A polynomial is an element of $I^{(e)}$ if and only if the hypersurface it defines contains δ, which occurs if and only if the hypersurface contains more than $e\deg(\delta)$ points of δ by Bézout's theorem (Theorem 2.9). Since δ is real and contains infinitely many real points, the coefficients of each polynomial in $I^{(e)}$ satisfy a linear system of (at least) $e\deg(\delta)+1$ real equations in $\binom{d+e}{d}$ variables. Solving this linear system then shows that $I^{(e)}$, considered as a vector space, has a basis of real polynomials. □

As a consequence, we obtain the following basic fact on odd-degree polynomials in real projective space.

Lemma 3.5. *Let δ be a non-degenerate curve of odd degree in $\mathbb{RP}^d$. Then any hyperplane of $\mathbb{RP}^d$ intersects δ in at least one point of $\mathbb{RP}^d$.*

Proof. By Lemma 3.4, the homogeneous ideal of δ is generated by real polynomials. The lemma then follows from the fact that roots of real polynomials come in complex conjugate pairs. Since δ has odd degree, any real hyperplane thus intersects δ in at least one real point. □

3.1 Elliptic curves

Elliptic curves (in any dimension) and their group structure are well-studied, going back to Clifford [16] and Klein [38].

Definition 3.6. An *elliptic normal curve* is an irreducible non-degenerate smooth curve of degree $d+1$ and genus 1 in $\mathbb{CP}^d$.

The following proposition shows that all elliptic normal curves have a similar group structure.

Proposition 3.7 ([57, Corollary 2.3.1; 58, Exercise 3.11 and Corollary 5.1.1])**.** *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.

3.2 Rational curves

The facts collected in this section are well-known, especially in the $d = 3$ case, in the sense that they were discovered in the 19th century (see [15, 22, 53, 62, 63, 66]). However, it is not easy to find recent references (or in some cases, any reference at all), and so we include some of the proofs. Our main goal is to describe when an irreducible non-degenerate rational curve (defined below) 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.

Definition 3.8. 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, and the q_i's share no common factor.

A *rational normal curve* in $\mathbb{FP}^d$ is an irreducible non-degenerate rational curve of degree d.

Rational normal curves in $\mathbb{FP}^d$ are unique up to projective transformations [29, Example 1.14], and turn out to be smooth [29, Exercise 14.14]. In fact, the rational normal curve is the unique irreducible non-degenerate curve of degree d in $\mathbb{FP}^d$ [29, Proposition 18.9]. We write ν_{d+1} for the rational normal curve in $\mathbb{CP}^{d+1}$ parametrised 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

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

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 $p = [p_0, p_1, \ldots, p_{d+1}] \in \mathbb{CP}^{d+1}$ 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. Noting that if δ_p is real then $p \in \mathbb{RP}^{d+1}$, we summarise the above discussion in the following proposition that will be implicitly used in the remainder of this thesis.

Proposition 3.9. *An irreducible non-degenerate rational curve of degree $d+1$ in $\mathbb{FP}^d$ is projectively equivalent to δ_p for some $p \in \mathbb{FP}^{d+1} \setminus \nu_{d+1}$.*

We use the projection point p to define a binary form and a multilinear form associated to δ_p.

Definition 3.10. The *fundamental binary form* associated to an irreducible non-degenerate rational curve δ_p of degree $d+1$ in $\mathbb{FP}^d$ 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 $F_p\colon (\mathbb{F}^2)^{d+1} \to \mathbb{F}$ [18, 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

$$P_i(x_0,y_0,x_1,y_1,\ldots,x_d,y_d) := \sum_{I\in\binom{\{0,1,\ldots,d\}}{i}} \prod_{j\in\bar{I}} x_j \prod_{j\in I} y_j \tag{3.1}$$

for each $i = 0, \dots, d+1$. Here the sum is taken over all subsets I of $\{0, 1, \dots, d\}$ of size i, and $\overline{I}$ denotes the complement of I in $\{0, 1, \dots, d\}$. It is easy to see that the binary form f_p is the *restitution* of G_p, namely [18, Section 1.2]

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

Since the polarisation of the restitution of a multilinear form is itself [18, Section 1.2], we must thus have $F_p = G_p$. (This can also be checked directly.)

Lemma 3.11. *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 $\delta_p[x_i, y_i]$, $i = 0, \dots, d$, counting multiplicity, if and only if $F_p(x_0, y_0, x_1, y_1, \dots, x_d, y_d) = 0$.*

Proof. By Bertini's theorem [30, Theorem II.8.18 and Remark II.8.18.1], the set of hyperplanes that intersect δ_p in $d+1$ distinct points form an open dense subset of all hyperplanes. It is thus sufficient to 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

$$D := \det \begin{pmatrix} \nu_{d+1}[x_0, y_0] \\ \vdots \\ \nu_{d+1}[x_d, y_d] \\ p \end{pmatrix} = F_p(x_0, y_0, x_1, y_1, \dots, x_d, y_d) \prod_{0 \leqslant j < k \leqslant d} \begin{vmatrix} x_j & x_k \\ y_j & y_k \end{vmatrix}, \tag{3.2}$$

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

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

$$= (-1)^{\lfloor \frac{d+2}{2} \rfloor} \begin{vmatrix} y_0^{d+1} & x_0 y_0^d & x_0^2 y_0^{d-1} & \dots & x_0^d y_0 & x_0^{d+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ y_d^{d+1} & x_d y_d^d & x_d^2 y_d^{d-1} & \dots & x_d^d y_d & x_d^{d+1} \\ p_0 & -p_1 & p_2 & \dots & (-1)^d p_d & (-1)^{d+1} p_{d+1} \end{vmatrix}. \quad (3.3)$$

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 (3.3) and obtain the Vandermonde determinant

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

Finally, note that $(-1)^{\lfloor \frac{d+2}{2} \rfloor} (-1)^{\binom{d+2}{2}} = 1$ 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 (3.1). It follows that the coefficient of p_i in (3.3) is P_i, and (3.2) follows. □

We define the *secant variety* $\mathrm{Sec}_{\mathbb{C}}(\nu_{d+1})$ of the rational normal curve ν_{d+1} in $\mathbb{CP}^{d+1}$ to be 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 $\delta_p[x_0, y_0]$, $\delta_p[x_1, y_1]$, $\delta_p[x_2, y_2], \ldots, \delta_p[x_d, y_d]$ are on a hyperplane in $\mathbb{FP}^d$ for all $[x_i, y_i] \in \mathbb{FP}^1$, $i = 2, \ldots, d$. 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 $[x_0x_1, x_0y_1 + y_0x_1, y_0y_1] M_2(p) = 0$. 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 $c_0 = x_0x_1$, $c_1 = x_0y_1 + y_0x_1$, $c_2 = y_0y_1$, and we have $c_0x^2 + 2c_1xy + c_2y^2 = (x_0x + y_0y)(x_1x + y_1y)$. 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 $c_0x^2 + 2c_1xy + c_2y^2$. 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 thesis, we make the following definitions.

Definition 3.12. 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 with a cusp, crunode, or acnode respectively.

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

Proposition 3.13 ([29, 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 3.14. *Let $d \geqslant 3$. For any $k = 2, \ldots, d-1$ 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* $\mathrm{rank}(M_k(p)) \leqslant 2$.

We next use Corollary 3.14 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 space quartic of the second species in 3-space. (The union of the trisecants form the unique quadric on which the curve lies [29, Exercise 8.13].)

Lemma 3.15. *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

$[x_3, y_3], \ldots, [x_d, y_d] \in \mathbb{CP}^1$, the points $\delta_p[x_i, y_i]$, $i = 0, \ldots, d$ are on a hyperplane, so by Lemma 3.11, $F_p(x_0, y_0, \ldots, x_d, y_d)$ is identically zero as a polynomial in $x_3, y_3, \ldots, x_d, y_d$. 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 $i = 0, \ldots, d-2$. 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 3.14, and so the cubic form is unique up to scalar multiplication. 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 now 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 ν_{d+1}. 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 $\delta_p \circ \varphi[x_i, y_i]$, $i = 0, \ldots, d$, 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 3.11 that

$$F_p(\varphi(x_0, y_0), \ldots, \varphi(x_d, y_d))$$

is a multiple of

$$F_{\psi^{-1}(p)}(x_0, y_0, \ldots, x_d, y_d),$$

hence $f_p \circ \varphi = f_{\psi^{-1}(p)}$ up to a scalar multiple. Thus, we obtain the same reparametrisation of the fundamental binary form f_p.

Recall from Definition 3.2 that a space quartic in $\mathbb{FP}^3$ is of the first species if it is contained in at least two linearly independent quadrics, and is of the second species if it is contained in a unique quadric. We can now prove the following result, which when combined with Corollary 3.14 shows that a rational space quartic in $\mathbb{FP}^3$ is of the first species if and only if it is singular.

Lemma 3.16. *A rational space quartic δ_p in $\mathbb{FP}^3$ is of the first species if and only if* $\operatorname{cat}(f_p) := \det(M_2(p))$ *vanishes.*

Proof. After a reparametrisation of δ_p if necessary, we can assume $\delta_p[x, y] = \nu_{d+1}[x, y]A$, where

$$A = \begin{pmatrix} p_1 & -p_2 & p_3 & -p_4 \\ -p_0 & 0 & 0 & 0 \\ 0 & p_0 & 0 & 0 \\ 0 & 0 & -p_0 & 0 \\ 0 & 0 & 0 & p_0 \end{pmatrix}$$

and $p_0 \neq 0$. Working in the affine charts $y = 1$ in $\mathbb{FP}^1$ and $p_0 = 1$ in $\mathbb{FP}^4$, δ_p thus has the parametrisation

$$[x + p_1, x^2 - p_2, x^3 + p_3, x^4 - p_4],$$

where $p_2 \neq p_1^2$, $p_3 \neq p_1^3$, or $p_4 \neq p_1^4$.

Consider the equations of quadrics Q that contain δ_p. If Q contains δ_p, substituting the four polynomials $x + p_1, x^2 - p_2, x^3 + p_3, x^4 - p_4$ for the homogeneous coordinates of v into the equation $v^T A_Q v = 0$, where $A_Q = (a_{i,j})$ is the 4×4 symmetric matrix defining Q, gives a degree 8 polynomial in x that has to be identically zero.

This gives nine equations in ten variables (the entries of A_Q). The first few equations, corresponding to the coefficients of x^8, x^7, x^6, x^5, are $a_{44} = 0, a_{34} = 0, 2a_{24} + a_{33} = 0, a_{14} + a_{23} = 0$. So in fact we only have five equations

in six variables:

$$\begin{pmatrix} -2p_2 & 2p_1 & 2 & 1 & 0 & 0 \\ -2p_3 & p_2 & p_1 & 0 & 1 & 0 \\ -2p_4 & -2p_3 & 0 & -2p_2 & 2p_1 & 1 \\ 0 & -p_4 & p_3 & 0 & -p_2 & p_1 \\ 2(p_2p_4 - p_3^2) & -2(p_1p_4 - p_2p_3) & 2p_1p_3 & p_2^2 & -2p_1p_2 & p_1^2 \end{pmatrix} \begin{pmatrix} a_{24} \\ a_{14} \\ a_{13} \\ a_{22} \\ a_{12} \\ a_{11} \end{pmatrix} = 0.$$

There is always a non-trivial solution to this system, but we want to show that there are always at least two linearly independent solutions if and only if $\operatorname{cat}(f_p) = p_2p_4 - p_3^2 - p_1^2p_4 + 2p_1p_2p_3 - p_2^3 = 0$.

The nullity of the matrix is at least 2 if and only if its rank is at most 4, which in turn happens if and only if the six 5×5 minors all vanish. These six minors are

$$\begin{aligned} &-4\operatorname{cat}(f_p)(p_3^2 - p_2p_4), && 2\operatorname{cat}(f_p)(p_2p_3 - p_1p_4), && -4\operatorname{cat}(f_p)(p_1p_3 - p_4), \\ &2\operatorname{cat}(f_p)(p_2^2 - 2p_1p_3 + p_4), && 2\operatorname{cat}(f_p)(p_1p_2 - p_3), && -2\operatorname{cat}(f_p)(p_1^2 - p_2), \end{aligned}$$

and it is impossible for all of the last factors to be equal to zero, otherwise we have $p_2 = p_1^2$, $p_3 = p_1^3$, and $p_4 = p_1^4$. Thus the six minors all vanish if and only if $\operatorname{cat}(f_p) = 0$, as desired. □

The polynomial $\operatorname{cat}(f_p)$ defined above is known as the *catalecticant* of the binary quartic form f_p. It was discovered by Boole [67] and generalised to binary forms of even degree by Sylvester [62], who coined the term. Sylvester [62] also showed that a generic binary form f_p of degree d is the sum of two d-th powers of linear forms if and only if $M_2(p)$ does not have full rank. We need a version of this statement that is valid for all binary forms, not only generic ones, to determine the natural group structure on rational singular curves. Reznick [52] gives an elementary proof of the generic case where p does not lie on the tangent variety. (See also Kanev [36, Lemma 3.1] and Iarrobino and Kanev [32, Section 1.3].) We provide a very elementary proof that includes the non-generic case.

Theorem 3.17 (Sylvester [62])**.** *Let* $d \geqslant 2$.

(*i*) *If* $p \in \mathrm{Tan}_{\mathbb{C}}(\nu_{d+1})$*, 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* $p \in \mathrm{Sec}_{\mathbb{C}}(\nu_{d+1}) \backslash \mathrm{Tan}_{\mathbb{C}}(\nu_{d+1})$*, 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* $p \in \mathbb{RP}^{d+1} \setminus \mathrm{Sec}_{\mathbb{R}}(\nu_{d+1})$ *then* L_1 *and* L_2 *are complex conjugates, while if* $p \in \mathrm{Sec}_{\mathbb{R}}(\nu_{d+1})$ *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

$$f_p(x,y) = \sum_{i=0}^{d+1} p_i \binom{d+1}{i} x^{d+1-i} y^i = (\alpha_2 x - \alpha_1 y)^d (\beta_2 x - \beta_1 y) \tag{3.4}$$

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 (3.4), 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

$$p_i = \left(1 - \frac{i}{d+1}\right) \alpha_2^{d-i} (-\alpha_1)^i \beta_2 - \frac{i}{d+1} \alpha_2^{d-i+1} (-\alpha_1)^{i-1} \beta_1. \tag{3.5}$$

Since we are working projectively, we can fix the value of β_1 from the instance $i = d+1$ of (3.5) to get

$$p_{d+1} = -(-\alpha_1)^d \beta_1. \tag{3.6}$$

If $p_{d+1} \neq 0$, we can divide (3.5) by (3.6). 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 $\beta \in \mathbb{F}$,

$$a_i = -\left(1 - \frac{i}{d+1}\right)(-\alpha)^{d-i}\beta + \frac{i}{d+1}(-\alpha)^{d-i+1} \tag{3.7}$$

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 (3.7) 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 $\alpha_2 x - \alpha_1 y$ and $\beta_2 x - \beta_1 y$ 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

$$p_i = \left(1 - \frac{i}{d+1}\right)\alpha_2^{d-i}(-\alpha_1)^i\beta_2 \tag{3.8}$$

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

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

again giving (3.8) as required. Note that since $\alpha_1 \neq 0$ but $\beta_1 = 0$, $\alpha_2 x - \alpha_1 y$ and $\beta_2 x - \beta_1 y$ are linearly independent. Note also that since $\lambda \neq 0$, we have $\beta_2 \neq 0$ and $p \neq [1, 0, \ldots, 0]$, hence $p \notin \nu_{d+1}$.

(ii): Let $p = [p_0, \ldots, p_{d+1}] \in \mathrm{Sec}_{\mathbb{C}}(\nu_{d+1}) \setminus \mathrm{Tan}_{\mathbb{C}}(\nu_{d+1})$, 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 $p = \mu_1 p_1 + \mu_2 p_2$. This means that for $i = 0, \ldots, d+1$, 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

$$\begin{aligned} f_p(x,y) &= \sum_{i=0}^{d+1} p_i \binom{d+1}{i} x^{d+1-i} y^i \\ &= \mu_1 \sum_{i=0}^{d+1} \binom{d+1}{i} (\alpha_2 x)^{d+1-i} (-\alpha_1 y)^i \\ &\qquad + \mu_2 \sum_{i=0}^{d+1} \binom{d+1}{i} (\beta_2 x)^{d+1-i} (-\beta_1 y)^i \\ &= \mu_1 (\alpha_2 x - \alpha_1 y)^{d+1} + \mu_2 (\beta_2 x - \beta_1 y)^{d+1} \\ &= L_1(x,y)^{d+1} - L_2(x,y)^{d+1} \end{aligned}$$

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 $\overline{L_1(x,y)} = L_2(\overline{x}, \overline{y})$.

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. For a detailed account of the $d = 3$ case, including group laws on non-irreducible rational space quartics, see [47].

Proposition 3.18. *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 3.17, $f_p = L_1^d L_2$ for some linearly independent linear forms L_1 and L_2. Reparametrising δ_p if necessary, 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 $p = [0,1,0,\ldots,0]$, with the cusp of δ_p at $\delta_p[0,1]$. It follows that the polarisation of f_p is $F_p(x_0, y_0, \ldots, x_d, y_d) = P_1 = x_0 x_1 \cdots x_d \sum_{i=0}^d y_i/x_i$. For $[x_i, y_i] \neq [0,1]$, $i = 0, \ldots, d$, 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 3.17, $f_p = L_1^{d+1} - L_2^{d+1}$ for some linearly independent linear forms L_1 and L_2. Again by reparametrising δ_p if necessary, 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 $p = [1,0,\ldots,0,-1]$, with the node of δ_p at $\delta_p[0,1] = \delta_p[1,0]$. The polarisation of f_p is $F_p(x_0, y_0, \ldots, x_d, y_d) = P_0 - P_{d+1} = x_0 x_1 \cdots x_d - y_0 y_1 \cdots y_d$. Therefore, $\delta_p[x_i, y_i]$, $i = 0, \ldots, d$, 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 3.17 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 $F_p(x_0,y_0,\ldots,x_d,y_d) = \prod_{j=0}^{d}(x_j+iy_j) - \prod_{j=0}^{d}(x_j-iy_j)$, and it follows that $\delta_p[x_0,y_0],\ldots,\delta_p[x_d,y_d]$ 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 $\delta_p[x_i,y_i]$, $i = 0,\ldots,d$ 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. □

3.3 Circular and spherical curves

In this section, we introduce the curves that appear in Theorems 1.11 and 1.12, our structure theorems for sets spanning few ordinary circles and hyperspheres. These are special classes of curves that are closed under inversion. We also define group laws on these curves so that $d+2$ points are contained in a hypersphere if and only if they sum to some constant.

Recall from Section 1.4 that the imaginary sphere at infinity Σ_∞ in $\mathbb{CP}^d$ is defined as the intersection of the unit hypersphere $\overline{\mathbb{S}^{d-1}}$ and the hyperplane at infinity Π_∞. As remarked, Σ_∞ is also the intersection of Π_∞ and the Zariski closure of any hypersphere in $\mathbb{C}^d$. In fact, any real quadric containing Σ_∞ is either a hypersphere, or the degenerate case of the union of a real hyperplane and Π_∞. If $d = 2$, note that Σ_∞ is just a set of two points, which we denote by

$$\alpha = [0,i,1],\ \beta = [0,-i,1],$$

and refer to them as the *circular points*.

Definition 3.19. An *ℓ-spherical curve* in $\mathbb{R}^d$ is a real curve in $\mathbb{CP}^d$ that contains exactly ℓ pairs of complex conjugate points, counting multiplicity,

on Σ_∞.

An ℓ-spherical curve in $\mathbb{R}^2$ is called an *ℓ-circular curve*, and contains both α and β with multiplicity ℓ.

We sometimes refer to 1-spherical or 1-circular curves as just spherical or circular curves. By abuse of notation, we also refer to ℓ-spherical or ℓ-circular curves for all $\ell \geqslant 1$ as spherical or circular curves. A classical reference for circular curves is Johnson [34], while a more modern one is Werner [65]. While our notion of spherical curves is a natural generalisation of circular curves, we could not find it in the literature. Let us now make the definition more explicit by considering some examples of circular curves.

In the simplest case, a *circular conic* is just a circle or the union of a line and the line at infinity. Equivalently, it is a real curve in $\mathbb{CP}^2$ defined by a homogeneous polynomial of the form

$$t(x^2 + y^2) + \ell(x, y, z)z,$$

where $t \in \mathbb{R}$, and $\ell \in \mathbb{R}[x, y, z]$ is a non-trivial linear form. If $t \neq 0$, then the curve is a circle, while if $t = 0$, the curve is the union of a line with the line at infinity. Ellipses, parabolas, and hyperbolas are thus non-circular conics.

A *circular cubic* is a curve of degree 3 that contains α and β; equivalently, it is any real curve in $\mathbb{CP}^2$ defined by a homogeneous polynomial of the form

$$(ux + vy)(x^2 + y^2) + q(x, y, z)z, \tag{3.9}$$

where $u, v \in \mathbb{R}$, and $q \in \mathbb{R}[x, y, z]$ is a non-trivial homogeneous quadratic polynomial. Note that we do not require a circular cubic to be irreducible or smooth. For instance, the union of a circle and a line is a circular cubic, and so is the union of any conic with the line at infinity (take $u = v = 0$ in (3.9)).

A *bicircular quartic* is an algebraic curve of degree 4 that is 2-circular; equivalently, it is any real curve in $\mathbb{CP}^2$ defined by a homogeneous polynomial of the form

$$t(x^2 + y^2)^2 + (ux + vy)(x^2 + y^2)z + q(x, y, z)z^2, \tag{3.10}$$

where $t, u, v \in \mathbb{R}$, and $q \in \mathbb{R}[x, y, z]$ is a non-trivial homogeneous quadratic polynomial (see [65, Section 8.2] for a proof that a quartic is 2-circular if and only if its equation has the form (3.10)). A noteworthy example of a bicircular quartic is a union of two circles, for which it is easy to see that the curve has double points at α and β, since both circles contain those points.

Every circular cubic is contained in a bicircular quartic, since for $t = 0$ in (3.10) we get a union of a circular cubic and the line at infinity. A non-circular conic is also contained in a bicircular quartic, since for $t = u = v = 0$ in (3.10) we get a union of a conic and $z^2 = 0$, which is a double line at infinity.

In higher even dimensions, we have similar analogues of non-circular conics, circular cubics, and bicircular quartics. If $d = 2k$, these are the $(k-1)$-spherical curves of degree d, k-spherical curves of degree $d+1$ (which are either elliptic or rational by Proposition 3.1), and $(k+1)$-spherical curves of degree $d+2$. This prompts the following definition.

Definition 3.20. The *spherical degree* of an ℓ-spherical curve of degree e is $e - \ell$. We also refer to the spherical degree of curves in the plane as the *circular degree*.

We thus have the following classification of curves of low circular degree.

- *Circular degree* 1: lines and circles;
- *Circular degree* 2: non-circular conics, circular cubics, and bicircular quartics;
- *Circular degree* 3: non-circular cubics, circular quartics, 2-circular quintics, and 3-circular sextics.

Similarly, $(k-1)$-spherical curves of degree d, k-spherical curves of degree $d+1$, and $(k+1)$-spherical curves of degree $d+2$ all have spherical degree 2. This classification is important to us, because spherical (and circular) degree is invariant under inversion, which we now show.

Proposition 3.21. *Let $\delta \subset \mathbb{RP}^d$ be a real curve of spherical degree k. Then $\delta' := \overline{\pi^{-1}(\overline{\delta} \setminus \Sigma_\infty)}$ is a real curve of degree $2k$ contained in $\overline{\mathbb{S}^d} \subset \mathbb{CP}^{d+1}$ that intersects Π_N in finitely many points.*

Proof. Let δ be ℓ-spherical of degree e, where $k = e - \ell$. Then the intersection of the cone over $\overline{\delta} \subset \mathbb{CP}^d \subset \mathbb{CP}^{d+1}$ with vertex N and $\overline{\mathbb{S}^d}$ is exactly the union of the curve δ' and the lines Nx for each $x \in \overline{\delta} \cap \Sigma_\infty$. By Bézout's theorem (Theorem 2.10), the intersection has total degree $2e$, hence $\deg(\delta') = 2e - 2\ell = 2k$. Since $\overline{\delta}$ intersects Σ_∞ in only finitely many points and π^{-1} takes real points to real points, it follows that δ' is real. Also, since δ' consists of all irreducible components of $\pi^{-1}(\overline{\delta})$ not contained in Π_N, δ' intersects Π_N in finitely many points. □

Recall from Definition 2.22 that ρ is the orthogonal reflection map in the hyperplane $\{x_{d+1} = 0\}$.

Proposition 3.22. *Let δ' be a real curve of degree $2k$ contained in $\overline{\mathbb{S}^d} \subset \mathbb{CP}^{d+1}$. If δ' intersects Π_N in finitely many points, then $\delta := \overline{\pi \circ \rho(\delta')}$ is a $(k-m)$-spherical curve of degree $2k-m$, where $m \geqslant 0$ is the multiplicity of $\rho^{-1}(N)$ on δ'. In particular, the spherical degree of δ is k.*

Proof. Since π is one-to-one on $\overline{\mathbb{S}^d} \setminus \Pi_N$, we have $\deg(\delta) = 2k - m$. Let Π be a generic hyperplane in $\mathbb{CP}^{d+1}$. Then $|\delta' \cap \Pi| = 2k$. Since δ' intersects Π_N in finitely many points, without loss of generality, $\delta' \cap \Pi$ is disjoint from Π_N. Then the hypersphere $\pi(\Pi \cap \overline{\mathbb{S}^d})$ intersects δ in $2k$ distinct points in $\mathbb{C}^d$. However, $|\delta \cap \pi(\Pi \cap \overline{\mathbb{S}^d})| = 2(2k - m)$ by Bézout's theorem (Theorem 2.10). So $|\delta \cap \Sigma_\infty| = 2(2k - m) - 2k = 2(k - m)$, and these points must come in complex conjugate pairs as δ is real. This means that δ is $(k-m)$-spherical, hence its spherical degree is $(2k - m) - (k - m) = k$ as claimed. □

We obtain the following corollaries almost immediately. They summarise and extend the discussion above on circular and spherical curves and inversion.

Corollary 3.23. *Let γ_k be a real curve of circular degree k. Then:*

(*i*) *The inverse of γ_1 in a point on γ_1 is a line; the inverse of γ_1 in a point not on γ_1 is a circle.*

(*ii*) *The inverse of γ_2 in a singular point on γ_2 is a non-circular conic; the inverse of γ_2 in a smooth point on γ_2 is a circular cubic; the inverse of γ_2 in a point not on γ_2 is a bicircular quartic.*

(*iii*) *The inverse of γ_3 in a singularity of multiplicity 3 is a non-circular cubic; the inverse of γ_3 in a singularity of multiplicity 2 is a circular quartic; the inverse of γ_3 in a smooth point on γ_3 is a 2-circular quintic; the inverse of γ_3 in a point not on γ_3 is a 3-circular sextic.*

Proof. Combine Propositions 3.21 and 3.22. □

One particular subcase of Case (*ii*) will play an important role in the proofs of our results on ordinary and 4-rich circles, and we state it separately in Corollary 3.24. A proof can also be found in [31, p. 202]. As discussed in Section 3.2, a singular rational curve of degree $d+1$ in $\mathbb{RP}^d$ has exactly one singularity, and is in fact isomorphic to a planar singular cubic. When the curve is real, the singularity is an acnode, crunode, or cusp depending on whether the singularity of the real planar cubic is an acnode, crunode, or cusp.

Corollary 3.24. *The inverse of an ellipse in a point on the ellipse is a circular acnodal cubic with the centre of inversion as its singularity; the inverse of a circular acnodal cubic in its singularity is an ellipse through the singularity.*

Proof. By Propositions 3.21 and 3.22, we only have to show that an ellipse inverts into a curve with an acnode as its singularity. If the singularity is not an acnode, then it is a crunode or a cusp, and in either case, there are real points on the curve arbitrarily close to the singularity. Then the inverse of this curve will be unbounded, contrary to assumption. □

The following corollaries are the higher dimensional analogues of Corollaries 3.23 and 3.24 above.

Corollary 3.25. *Let δ be a real curve of spherical degree $k+1$. Then the inverse of δ in a singular point of multiplicity 2 on δ is a $(k-1)$-spherical curve of degree $2k$; the inverse of δ in a smooth point on δ is a k-spherical curve of degree $2k+1$; and the inverse of δ in a point not on δ is a $(k+1)$-spherical curve of degree $2k+2$.*

Proof. Combine Propositions 3.21 and 3.22. □

Note that by Lemma 3.5, all real rational normal curves in $\mathbb{R}^d$ are unbounded when d is odd. On the other hand, when d is even, there exist bounded real rational normal curves. In the plane they are exactly the ellipses.

Corollary 3.26. *Let $d = 2k$. The inverse of a bounded $(k-1)$-spherical rational normal curve in $\mathbb{R}^d$ in a point on the curve is a non-degenerate k-spherical rational curve of degree $d+1$, with an acnode in the point of inversion and no other singularities; the inverse of a non-degenerate k-spherical rational curve of degree $d+1$ in $\mathbb{R}^d$, with an acnode and no other singularities, in its acnode is a bounded $(k-1)$-spherical rational normal curve.*

Proof. By Propositions 3.21 and 3.22, we only have to show that a bounded rational normal curve inverts into a curve with an acnode as its singularity. If the singularity is not an acnode, then it is a crunode or a cusp, and in either case, there are real points on the curve arbitrarily close to the singularity. Then the inverse of this curve will be unbounded, contrary to assumption. □

The extremal configurations in the circular variants of our structure theorems are all based on group laws on certain circular and spherical curves that describe when points lie on a hypersphere. We first consider the following general case, where the group laws are inherited from the curves considered in Sections 3.1 and 3.2 via stereographic projection. Note that a real k-spherical elliptic normal curve has a unique real point at infinity.

Proposition 3.27. *Let $d = 2k$. A bounded $(k-1)$-spherical rational normal curve or k-spherical elliptic normal curve in $\mathbb{RP}^d$ has a group structure such that $d+2$ points (not including the real point at infinity on an elliptic normal*

curve) lie on a hypersphere if and only if they sum to the identity. In the prior case, this group is isomorphic to $\mathbb{R}/\mathbb{Z}$*; in the latter case, this group is isomorphic to* $\mathbb{R}/\mathbb{Z}$ *or* $\mathbb{R}/\mathbb{Z} \times \mathbb{Z}_2$ *depending on whether it has one or two semi-algebraically connected components.*

Proof. Let $\delta \subset \mathbb{RP}^d \subset \mathbb{CP}^d$ be a curve of spherical degree $k+1$. Then by Proposition 3.21, $\delta' := \overline{\pi^{-1}(\overline{\delta})}$ is a curve in $\mathbb{CP}^{d+1}$ of degree $2(k+1) = d+2$. If δ is a $(k-1)$-spherical bounded rational normal curve, then by Corollary 3.26, δ' is a rational acnodal curve in $\mathbb{CP}^{d+1}$. If δ is a k-spherical elliptic normal curve, then δ' is an elliptic normal curve in $\mathbb{CP}^{d+1}$. In both cases, $\delta' \cap \mathbb{RP}^d$ has a group structure such that $d+2$ real points on δ' lie on a hyperplane if and only if they sum to the identity, and this group is isomorphic to $\mathbb{R}/\mathbb{Z}$ when δ' is acnodal, and isomorphic to $\mathbb{R}/\mathbb{Z}$ or $\mathbb{R}/\mathbb{Z} \times \mathbb{Z}_2$ if δ' is elliptic, depending on whether it has one or two semi-algebraically connected components (Propositions 3.18 and 3.7). Since a generic hyperplane intersects $\overline{\mathbb{S}^d}$ in a $(d-1)$-sphere and stereographic projection takes hyperspheres (not containing the north pole) to hyperspheres in $\mathbb{RP}^d$, π transfers the group to δ in such a way that $d+2$ points on δ lie on a hypersphere if and only if they sum to the identity. □

Let us note that $(k+1)$-spherical curves of degree $d+2$ that are inverses of the curves in Proposition 3.27 can also be given a group structure. However, in our proofs we will handle them by inverting in a point on the curve, which by Corollary 3.25 (and Corollary 3.23) transforms the curve into a bounded $(k-1)$-spherical rational normal curve or a k-spherical elliptic normal curve. For that reason, we do not need to study the group law on $(k+1)$-spherical curves of degree $d+2$ separately.

In the planar case, we can define group laws on irreducible circular cubics and ellipses in a more explicit and geometric way. By Proposition 3.3, the groups obtained in Propositions 3.29 and 3.30 below are isomorphic to those in Proposition 3.27.

Recall that by Propositions 3.7 and 3.18, irreducible cubics have a natural group structure where three points on the curve are collinear if and only if they sum to the identity. For this property to hold, the identity element

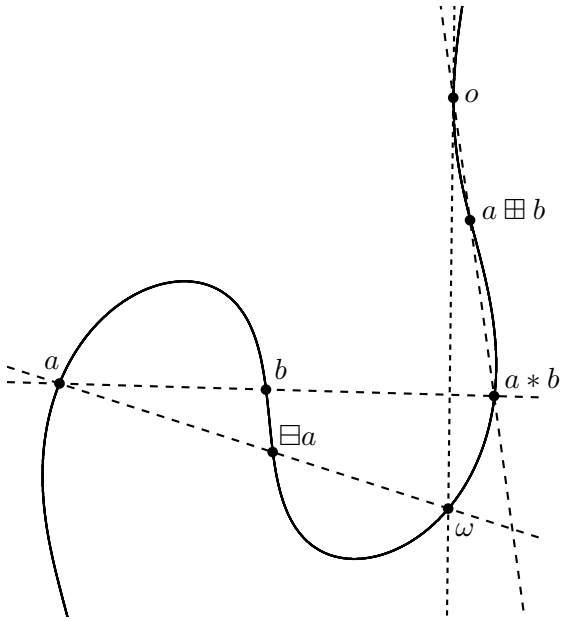

Figure 3.1: Group law on a circular elliptic cubic curve

must be an inflection point (a point with multiplicity 3 on the curve). We now define the group in a slightly different way (described for instance in [59, Section 1.2]), in which the identity is not necessarily an inflection point, and the same collinearity property does not hold. However, for circular cubics, we show that we can choose the identity element so that we get a similar property for concyclicity.

First let γ be any real irreducible cubic in $\mathbb{CP}^2$, write γ^* for its set of smooth points, and pick an arbitrary point $o \in \gamma^*$. We describe an additive group operation $\boxplus$ on the set γ^* for which o is the identity element. The construction is depicted in Figure 3.1. Given $a, b \in \gamma^*$, let $a * b$ be the third intersection point of γ and the line ab, and define $a \boxplus b$ to be $(a * b) * o$, the third intersection point of γ and the line through $a * b$ and o. When $a = b$, the line ab should be interpreted as the tangent line at a; when $a * b = o$, the line through $a * b$ and o should be interpreted as the tangent line to γ at o. We refer to [59] for a more careful definition and a proof that this operation really does give a group.

Now consider a circular cubic γ. Since the circular points α and β lying

on it are conjugate, γ has a unique real point on the line at infinity, which we choose as our identity element o. We define the point ω to be the third intersection point of the tangent line to γ at o (if there is no third intersection point, then o is an inflection point, and we consider o itself to be the third point). Throughout this thesis we will use ω to denote this special point on a circular cubic; note that ω is not fixed like α and β, but depends on γ. Also note that ω is real, since it corresponds to the third root of a real cubic polynomial whose other two roots correspond to the real point o. Observe that

$$\omega = \alpha \boxplus \beta,$$

since $\alpha * \beta = o$, and by definition $o * o = \omega$.

With this group law, we no longer have the property that three points are collinear if and only if they sum to o (unless o happens to be an inflection point). Nevertheless, one can check that three points $a, b, c \in \gamma^*$ are collinear if and only if $a \oplus b \oplus c = \omega$. More important for us, four points of γ^* lie on a circle (or the union of a line and the line at infinity) if and only if they sum to ω. This amounts to a classical fact (see [10, Article 225] for an equivalent statement), but we include a proof for completeness. We use the following version of the Cayley-Bacharach theorem, due to Chasles (see [19]).

Theorem 3.28 (Chasles [19])**.** *Suppose two cubic curves in $\mathbb{CP}^2$ with no common component intersect in nine points, counting multiplicities. If γ is another cubic curve containing eight of these intersection points, counting multiplicities, then γ also contains the ninth.*

Proposition 3.29. *Let γ^* be the set of smooth points of an real irreducible circular cubic $\gamma \subset \mathbb{CP}^2$. There is a group structure on γ^* such that a circle (or the union of a line and the line at infinity) intersects γ^* in four points a, b, c, d (taking into account multiplicity) if and only if $a \boxplus b \boxplus c \boxplus d = \omega$.*

Proof. We first show the forward direction. All statements in the proof should be considered with multiplicity.

Suppose the union of a line ℓ and the line at infinity ℓ_∞ intersects γ in $a, b, c, d, \alpha, \beta$. Since ℓ intersects γ in at most three points, one of the points

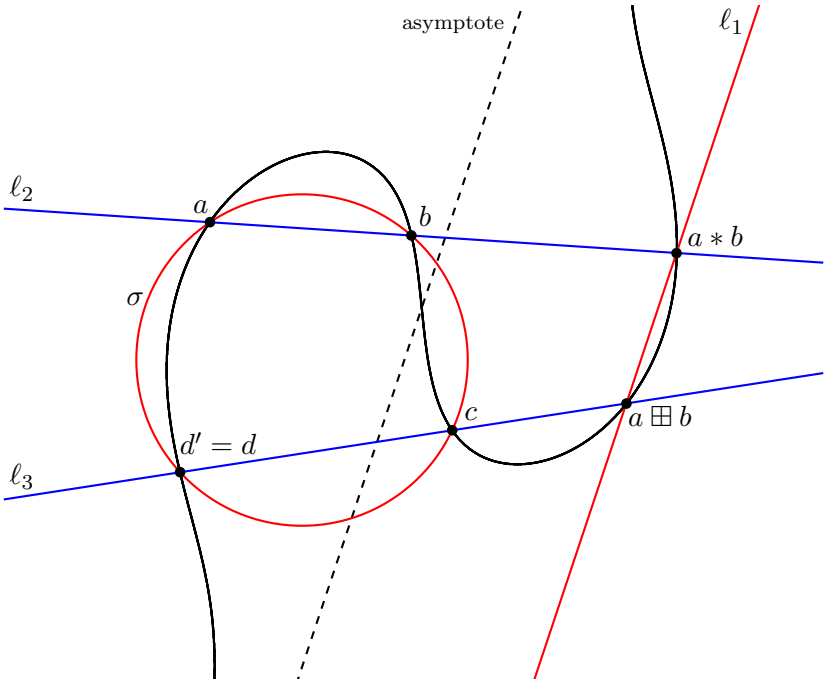

Figure 3.2: Concyclicity of four smooth points on a circular cubic

a, b, c, d must equal o, say $d = o$. Since ℓ_∞ also intersects γ in at most three points, we must have $a, b, c \in \ell$. Thus a, b, c are collinear, and we have $a \boxplus b \boxplus c = \omega$, by the definition of the group law. It then follows from $d = o$ that $a \boxplus b \boxplus c \boxplus d = \omega$.

Suppose next that a circle σ intersects γ in $a, b, c, d, \alpha, \beta$. The construction that follows is depicted in Figure 3.2. Let ℓ_1 be the line through o and $a * b$ (and thus through $a \boxplus b$), ℓ_2 the line through a and b (and thus through $a * b$), and ℓ_3 the line through c and $a \boxplus b$. Note that σ and ℓ_∞ intersect in α and β. Then $\gamma_1 = \sigma \cup \ell_1$ and $\gamma_2 = \ell_2 \cup \ell_3 \cup \ell_\infty$ are two cubic curves that intersect in nine points, of which the eight points a, b, c, $a * b$, $a \oplus b$, o, α, and β certainly lie on γ; the remaining point is the third intersection point of γ_1 and ℓ_3 beside c and $a \boxplus b$, which we denote by d'. By Theorem 3.28, γ contains d'. By the group law on γ, we have $d' = (a \boxplus b) * c$. Moreover, d' must be the sixth intersection point of γ and σ beside a, b, c, α, β, which is d, so $d = d' = (a \boxplus b) * c$. By the definition of the group law, this implies $a \boxplus b \boxplus c = o * d$, so $(a \boxplus b \boxplus c) * d = (o * d) * d = o$, and finally

$a \boxplus b \boxplus c \boxplus d = o * o = \omega$.

For the converse, suppose that $a \boxplus b \boxplus c \boxplus d = \omega$, and let d' be the fourth point where the circle (or the union of a line and the line at infinity) σ through a, b, c intersects γ. Then, by what we have just shown, $a \boxplus b \boxplus c \boxplus d' = \omega$, and it follows that $d = d'$, and a, b, c, d lie on σ. □

This proposition is a consequence of the more general fact that six points on a circular cubic lie on a conic if and only if they sum to 2ω. (In the standard group structure on a cubic, where the identity o is chosen as an inflection point, they would sum to o; see [64, Theorem 9.2].) Since a circle (or the union of a line and the line at infinity) in $\mathbb{RP}^2$ is a conic containing α and β, and $\alpha \boxplus \beta = \omega$, it follows that four points a, b, c, d (possibly including o) lie on a circle (or the union of a line and the line at infinity) if and only if they sum to ω.

Also, as remarked above, we have $(\gamma^*, \boxplus, o) \cong (\gamma^*, \oplus, 0)$, where the latter group is as defined in Proposition 3.27.

We now discuss a group law on ellipses, although we do not actually need it in our proofs, as inversion lets us transform an ellipse into an acnodal cubic (Corollary 3.24), which we have already given a group structure. Nevertheless, we treat the group law on ellipses here because it is especially elementary.

Consider the ellipse σ given by the equation $x^2 + (y/s)^2 = 1$, with $s \neq 0, 1$. For any point $a \in \sigma$, we project a vertically to the point a' on the unit circle around the origin, as in Figure 3.3, and call the angle θ_a from the positive x-axis to the ray from the origin through a' the *eccentric angle* of a. We define the sum of two points $a, b \in \sigma$ to be the point $c = a \boxplus b$ whose eccentric angle is $\theta_c = \theta_a + \theta_b$. This gives σ a group structure isomorphic to $\mathbb{R}/\mathbb{Z}$. The identity element is $o = (1, 0)$, and the inverse of a point is its reflection in the x-axis. We have the following classical fact that describes when four points on an ellipse are concyclic (see [33] for the oldest reference we could find, and [11, Problem 17.2] for two detailed proofs).

Proposition 3.30. *Let σ be an ellipse. There is a group structure on σ such that four points $a, b, c, d \in \sigma$ are concyclic if and only if $a \boxplus b \boxplus c \boxplus d = o$,*

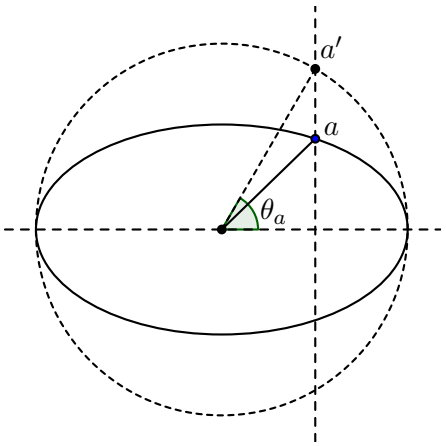

Figure 3.3: Eccentric angle of a point on an ellipse

where $\theta_{p \boxplus q} = \theta_p + \theta_q$ *for* $p, q \in \sigma$*. We may allow two of the points to be equal, in which case the circle through the three distinct points is tangent to the ellipse at the repeated point.*

Another way to look at this group law is that we are parametrising the ellipse using lines through $o = (1, 0)$ (see for instance [59, Section 1.1]). More precisely, each point $a \in \sigma$ corresponds to the line oa' (where a' is as in Figure 3.3); oa' makes an angle $\pi - \theta_a/2$ with the x-axis, and the set of lines through o thus has a group structure equivalent to the one above. This view lets us relate the group on the ellipse to the group on the acnodal cubic. By Corollary 3.24, inverting in o maps the ellipse to a circular acnodal cubic γ, with o becoming the acnode of the cubic. The lines through o now parametrise the cubic, and this parametrisation gives the same group on γ as the line construction that we gave in Proposition 3.29 (see [59, Section 3.7]).

Finally, we define a group on the union of two concentric circles, which can be regarded as a non-irreducible curve of circular degree 2, like irreducible circular cubics and ellipses. Note that the 'aligned' and 'offset' double polygons mentioned in Theorem 1.11, our structure theorem for sets spanning few ordinary circles, are contained in two concentric circles (see Definition 4.4).

Proposition 3.31. *Let* σ_1 *and* σ_2 *be two concentric circles. There is a group structure on* $\sigma_1 \cup \sigma_2$ *such that points* $a, b \in \sigma_1$ *and* $c, d \in \sigma_2$ *lie on a circle or a line if and only if* $a \oplus b \oplus c \oplus d = o$*. If* $a = b$ *or* $c = d$*, then the*

circle or line is tangent at that point.

Proof. For notational convenience, we identify $\mathbb{R}^2$ with $\mathbb{C}$. Without loss of generality, we can assume the circles to be

$$\sigma_1 = \{e^{2\pi it} : t \in [0,1)\},\ \sigma_2 = \{re^{2\pi it} : t \in [0,1)\},$$

with $r > 1$, and we represent each element $p \in \sigma_1 \cup \sigma_2$ as $r^{\varepsilon_p} e^{2\pi i t_p}$ with $\varepsilon \in \mathbb{Z}_2$ (with the obvious convention $r^0 = 1$ and $r^1 = r$). We define a group operation on $\sigma_1 \cup \sigma_2$ by

$$r^{\varepsilon_p} e^{2\pi i t_p} \oplus r^{\varepsilon_q} e^{2\pi i t_q} = r^{(\varepsilon_p + \varepsilon_q) \bmod 2} e^{2\pi i((-1)^{\varepsilon_p} t_p + (-1)^{\varepsilon_q} t_q)},$$

which turns $\sigma_1 \cup \sigma_2$ into a group isomorphic to $\mathbb{R}/\mathbb{Z} \times \mathbb{Z}_2$, with identity element $o = 1 = r^0 e^{2\pi i \cdot 0}$.

It is clear that if $a, b \in \sigma_1$ and $c, d \in \sigma_2$, then $\varepsilon_a + \varepsilon_b + \varepsilon_c + \varepsilon_d \equiv 0 \pmod 2$, so we need only consider the angles. By symmetry, a, b, c, d lie on a circle or a line if and only if $t_a + t_b = t_c + t_d$, if and only if $a \oplus b \oplus c \oplus d = o$. □

By stereographic projection, we also get a group law on the intersection of a sphere and two distinct parallel planes, which contain the prisms and antiprisms (see Definition 4.3) mentioned in Theorem 1.9, our structure theorem for sets spanning few ordinary planes.

Corollary 3.32. *Let σ_1 and σ_2 be two circles given by the intersection of a sphere and two distinct parallel planes in $\mathbb{RP}^3$. There is a group structure on $\sigma_1 \cup \sigma_2$ such that points $a, b \in \sigma_1$ and $c, d \in \sigma_2$ lie on a plane if and only if $a \oplus b \oplus c \oplus d = o$. If $a = b$ or $c = d$, then the plane is tangent at that point.*

Proof. Without loss of generality, we can assume $\sigma_1 = \{x_3 = 0\} \cap \overline{\mathbb{S}^2}$ and $\sigma_2 = \{x_3 = \frac{r^2-1}{r^2+1}\} \cap \overline{\mathbb{S}^2}$ for some $r > 1$. Then projecting (stereographically) from the north pole onto the plane defined by $x_3 = 0$ (the affine part of which we identify with $\mathbb{C}$), we get

$$\pi(\sigma_1) = \{e^{2\pi it} : t \in [0,1)\},\ \pi(\sigma_2) = \{re^{2\pi it} : t \in [0,1)\}.$$

The result then follows from Proposition 3.31, since circles (and lines) are in one-to-one correspondence with planes under stereographic projection. □

Chapter 4

Constructions

In this chapter, we describe constructions that meet, or are close to meeting, the lower and upper bounds mentioned in our extremal theorems stated in Section 1.2.2. These include the trivial construction of all but one point being contained in a hyperplane, prisms and antiprisms, 'aligned' and 'offset' double polygons, and cosets of the curves described in Chapter 3.

4.1 Trivial constructions

We deal with the easy case where all but a bounded number of points of a set is contained in a hyperplane in this section. The following lemma shows that the number of ordinary hyperplanes spanned is minimised when all but one point is contained in the hyperplane, which we call the *trivial construction.*

Lemma 4.1. *Let $d \geqslant 2$, $K \geqslant 1$, and let $n \geqslant 3dK$. 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 $P \setminus \Pi$, $i = 1, \ldots, K$. 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 $\binom{K}{2}\binom{n-K}{d-2}$. Since any d points of P span a hyperplane, any such d-tuple determines a hyperplane containing at least two points of $P \setminus \Pi$ together with a choice of two of these points of $P \setminus \Pi$. (It is possible for different d-tuples with two elements in $P \setminus \Pi$ to have the same intersection with Π.) Therefore,

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

Hence the number of ordinary hyperplanes is at least

$$m_1 \geqslant K\binom{n-K}{d-1} - 2\binom{K}{2}\binom{n-K}{d-2}.$$

We next show that for all $K \geqslant 2$, if $n \geqslant 3dK$ then

$$\begin{aligned}&K\binom{n-K}{d-1} - K(K-1)\binom{n-K}{d-2} \\ &> (K-1)\binom{n-K+1}{d-1} - (K-1)(K-2)\binom{n-K+1}{d-2}. \qquad (4.1)\end{aligned}$$

But this is equivalent to

$$\binom{n-K}{d-1} - 3(K-1)\binom{n-K}{d-2} + (K-1)(K-2)\binom{n-K}{d-3} > 0,$$

so it is therefore sufficient to show that $\binom{n-K}{d-1} > 3(K-1)\binom{n-K}{d-2}$, which is equivalent to $n > 3dK - 2d - 2K + 1$. However, we assumed that $n \geqslant 3dK$, so (4.1) follows, and with it, the lemma. □

Since ordinary hyperspheres spanned by a set $P \subset \mathbb{R}^d$ are in one-to-one correspondence with ordinary hyperplanes spanned by $\pi^{-1}(P) \subset \mathbb{R}^{d+1}$, where π is the stereographic projection map, Lemma 4.1 tells us the trivial construction also minimises the number of ordinary hyperspheres in Case (1)

of Theorems 1.11 and 1.12, our structure theorems for sets spanning few ordinary circles and hyperspheres. We note the following special case in the plane for strict ordinary circles (where we do not count 3-rich lines).

Lemma 4.2. *Let $K \geqslant 1$ and $n \geqslant 2K+4$. If all but K points of a set $P \subset \mathbb{R}^2$ of n points lie on a line, then P spans at least $\binom{n-1}{2}$ strict ordinary circles.*

Proof. Let ℓ be a line such that $|P \cap \ell| = n - K$. For any $p \in P \cap \ell$ and $q \in P \setminus \ell$ there are at most $K-1$ non-ordinary circles through p, q, another point on $P \cap \ell$, and another point in $P \setminus \ell$. Therefore, there are at least $K(n-2K)$ strict ordinary circles through p. This holds for any of the $n-K$ points $p \in P \cap \ell$, and we obtain at least $\frac{1}{2}K(n-2K)(n-K)$ strict ordinary circles. It is easy to see that when $1 \leqslant K \leqslant (n-4)/2$, $\frac{1}{2}K(n-2K)(n-K)$ is minimised when $K = 1$. □

4.2 Constructions on non-irreducible curves

In this section, we consider configurations that differ in at most one point from a prism or an antiprism, or an 'aligned' or 'offset' double polygon, as mentioned in Theorems 1.9 and 1.11, our structure theorems for sets spanning few ordinary planes and circles, respectively. Note that these constructions exist only in 3- and 2-space, as there are no constructions on non-irreducible curves in higher dimensions. In Definitions 4.3 and 4.4 below, $[m]$ denotes the set of integers $\{1, \ldots, m\}$.

Definition 4.3. By a *prism*, we mean a subset of $\mathbb{R}^3$ of the form

$$\left\{\left(\cos\left(\frac{2k\pi}{m}\right), \sin\left(\frac{2k\pi}{m}\right), 0\right) : k \in [m]\right\}$$
$$\cup \left\{\left(\frac{2r}{r^2+1}\cos\left(\frac{2k\pi}{m}\right), \frac{2r}{r^2+1}\sin\left(\frac{2k\pi}{m}\right), \frac{r^2-1}{r^2+1}\right) : k \in [m]\right\},$$

for some $r > 1$, which is projectively equivalent to the vertex set of a prism over a regular m-gon.

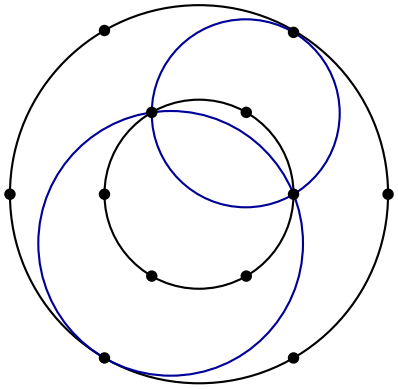

Figure 4.1: 'Aligned' double hexagon

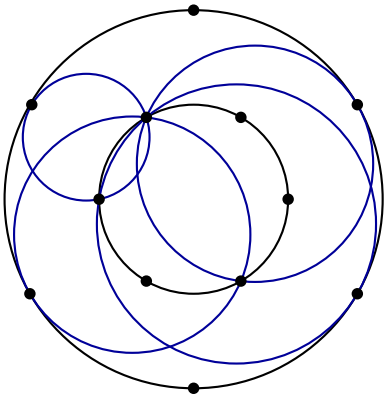

Figure 4.2: 'Offset' double hexagon

By an *antiprism*, we mean a subset of $\mathbb{R}^3$ of the form

$$\left\{\left(\cos\left(\frac{2k\pi}{m}\right),\sin\left(\frac{2k\pi}{m}\right),0\right):k\in[m]\right\}$$
$$\cup\left\{\left(\frac{2r}{r^2+1}\cos\left(\frac{(2k+1)\pi}{m}\right),\frac{2r}{r^2+1}\sin\left(\frac{(2k+1)\pi}{m}\right),\frac{r^2-1}{r^2+1}\right):k\in[m]\right\},$$

for some $r>1$, which is projectively equivalent to the vertex set of an antiprism over a regular m-gon.

Definition 4.4. Identifying $\mathbb{R}^2$ with $\mathbb{C}$, an *'aligned' double polygon* is the set

$$\left\{e^{2\pi ik/m}:k\in[m]\right\}\cup\left\{re^{2\pi ik/m}:k\in[m]\right\},$$

for some $r>1$, which is the vertex set of regular m-gons that are 'aligned' in the sense that their points lie at the same set of angles from the common centre (see Figure 4.1).

An *'offset' double polygon* is the set

$$\left\{e^{2\pi ik/m}:k\in[m]\right\}\cup\left\{re^{-i\pi(2k-1)/m}:k\in[m]\right\},$$

for some $r>1$, which is obtained from an 'aligned' double polygon by rotating the outer set of vertices by a angle of $\pi k/m$ (see Figure 4.2).

Note that projecting the prism and antiprism stereographically gives us the 'aligned' and 'offset' double polygon respectively. Since ordinary and 4-rich

planes spanned by a set $S \subset \mathbb{S}^2 \subset \mathbb{R}^3$ are in one-to-one correspondence with ordinary and 4-rich circles spanned by $\pi(S) \subset \mathbb{R}^2$, we only need to consider one setting in the following constructions. We choose to focus on double polygons for easier geometric intuition, and also because there is the extra case of strict ordinary circles.

Construction 4.5 (Prisms and 'aligned' double polygons)**.** This construction achieves the minimum number of ordinary planes, ordinary circles, and strict ordinary circles as stated in Theorems 1.13, 1.18, and 1.19 respectively, if n is even.

Let $n \geqslant 6$ be even and set $m = n/2$. We identify $\mathbb{R}^2$ with $\mathbb{C}$. Let σ_1 be the circle with centre the origin and radius one, and σ_2 the circle with centre the origin and radius $r > 1$. Let S be an 'aligned' double polygon, let $S_1 = S \cap \sigma_1$, and $S_2 = S \cap \sigma_2$. By Proposition 3.31, the points $a, b \in \sigma_1$, $c, d \in \sigma_2$ are concyclic or collinear if and only if $a \oplus b \oplus c \oplus d = o$. In particular, if $a = b$, then the circle or line through the three points is tangent to σ_1. It follows that if $n \geqslant 8$, the ordinary circles of S are exactly those through $e^{2\pi i k_1/m}$, $re^{-2\pi i k_2/m}$, and $re^{-2\pi i k_3/m}$ or through $re^{-2\pi i k_1/m}$, $e^{2\pi i k_2/m}$, and $e^{2\pi i k_3/m}$, where $2k_1 + k_2 + k_3 \equiv 0 \pmod{m}$ with $k_2 \not\equiv k_3 \pmod{m}$.

For generic $r > 1$, we then obtain that the number of ordinary circles equals

$$\left|\left\{(k_1, k_2, k_3) \in \mathbb{Z}_m^3 : 2k_1 + k_2 + k_3 \equiv 0 \pmod{m}, \quad k_2, k_3 \text{ distinct}\right\}\right|$$

(although k_2 and k_3 are not ordered, we either have two points on σ_1 or two points on σ_2). This equals $m(m-2)$ if m is even and $m(m-1)$ if m is odd. That is, for generic r, we obtain $\frac{1}{4}n^2 - n$ ordinary circles if $n \equiv 0 \pmod{4}$ and $\frac{1}{4}n^2 - \frac{1}{2}n$ ordinary circles if $n \equiv 2 \pmod{4}$.

If we choose $r = (\cos(2\pi k/m))^{-1}$ (there are $\lceil m/4 \rceil - 1$ choices for r), then the tangent lines at points of S_1 pass through two points of S_2, so are ordinary circles. Thus, for these choices of r we lose m strict ordinary circles, and obtain $\frac{1}{4}n^2 - \frac{3}{2}n$ strict ordinary circles if $n \equiv 0 \pmod{4}$ and $\frac{1}{4}n^2 - n$ strict ordinary circles if $n \equiv 2 \pmod{4}$.

Similarly, the number of 4-rich circles spanned by S equals

$$\frac{1}{4}|\{(k_1,k_2,k_3,k_4)\in\mathbb{Z}_m^4 :$$
$$k_1+k_2+k_3+k_4\equiv 0 \pmod m, \quad k_1\neq k_2 \text{ and } k_3\neq k_4\}|,$$

which is $\frac{1}{4}m^3-O(m^2)=\frac{1}{32}n^3-O(n^2)$.

By stereographic projection (or Corollary 3.32), the number of ordinary and 4-rich planes spanned by a prism is equal to the number of ordinary and 4-rich circles spanned by S.

Construction 4.6 (Antiprism and 'offset' double polygons)**.** This construction achieves the minimum number of ordinary planes, ordinary circles, and strict ordinary circles as stated in Theorems 1.13, 1.18, and 1.19 respectively, if $n\equiv 2 \pmod 4$.

Let S be an 'offset' double polygon. As in Construction 4.5, if $n\geqslant 8$, the ordinary circles of S are exactly those through $e^{2\pi ik_1/m}$, $re^{-i\pi(2k_2-1)/m}$, $re^{-i\pi(2k_3-1)/m}$ or through $re^{-i\pi(2k_1-1)/m}$, $e^{2\pi ik_2/m}$, $e^{2\pi ik_3/m}$, where $2k_1+k_2+k_3\equiv 1 \pmod m$ with $k_2\not\equiv k_3 \pmod m$.

For generic $r>1$, we now have to count the number of ordered triples in the set

$$\left\{(k_1,k_2,k_3)\in\mathbb{Z}_m^3 : 2k_1+k_2+k_3\equiv 1 \pmod m, \quad k_2,k_3 \text{ distinct}\right\}.$$

This equals m^2 if m is even and $m(m-1)$ if m is odd. That is, for generic r, we obtain $\frac{1}{4}n^2$ ordinary circles if $n\equiv 0 \pmod 4$, worse than Construction 4.5, and $\frac{1}{4}n^2-\frac{1}{2}n$ ordinary circles if $n\equiv 2 \pmod 4$, the same number as in Construction 4.5.

Again, if we choose $r=(\cos(2\pi k/m))^{-1}$ (there are $\lfloor m/4\rfloor$ choices for r), we lose m ordinary circles. Thus, we obtain $\frac{1}{4}n^2-n$ strict ordinary circles if $n\equiv 2 \pmod 4$, the same number as in Construction 4.5.

As in Construction 4.5, we get $\frac{1}{32}n^3-O(n^2)$ 4-rich circles.

Also as in Construction 4.5, by stereographic projection (or Corollary 3.32), the number of ordinary and 4-rich planes spanned by an antiprism is equal to the number of ordinary and 4-rich circles spanned by S.

Construction 4.7 (Punctured prisms, antiprisms, and double polygons)**.** This construction achieves the minimum number of ordinary planes and circles as stated in Theorems 1.13 and 1.18 respectively, if n is odd.

Let $n = 2m-1 \geqslant 11$ be odd. Take Construction 4.5 with $n+1 = 2m$ points and remove an arbitrary point $p \in S_1$.

First assume that m is odd. Before we remove p, there are $m(m-1)$ ordinary circles. Of these, there are $(m-1)/2$ tangent at p. There are also $m-1$ ordinary circles through p tangent at some point of S_2. Thus, by removing p, we destroy $3(m-1)/2$ ordinary circles and create $\binom{m}{2} - (m-1)/2$ new ones. Therefore, $S \setminus \{p\}$ spans

$$m(m-1) - \frac{3}{2}(m-1) + \binom{m}{2} - \frac{1}{2}(m-1) = \frac{3}{2}m^2 - \frac{7}{2}m + 2$$

ordinary circles. That is, there are $\frac{3}{8}n^2 - n + \frac{5}{8}$ ordinary circles if $n \equiv 1 \pmod 4$.

Next assume that m is even. Before we remove p, there are $m(m-2)$ ordinary circles, of which there are $(m-2)/2$ through two different points of S_2 tangent at p, and there are also $m-2$ ordinary circles through p tangent at a point of S_2. As before, we obtain

$$m(m-2) - \frac{3}{2}(m-2) + \binom{m}{2} - \frac{1}{2}(m-2) = \frac{3}{2}m^2 - \frac{9}{2}m + 4$$

ordinary circles. Thus, we obtain $\frac{3}{8}n^2 - \frac{3}{2}n + \frac{17}{8}$ ordinary circles if $n \equiv 3 \pmod 4$.

Instead of starting with Construction 4.5, we can take the 'offset' Construction 4.6 and remove a point. As in Construction 4.6, if $n \equiv 1 \pmod 4$ we obtain the same number of ordinary circles, while if $n \equiv 3 \pmod 4$ we obtain more.

Since there are no 5-rich circles in Constructions 4.5 and 4.6 when $m \geqslant 6$, removing a point does not add any 4-rich circle, but destroys $O(n^2)$ of them. We thus get $\frac{1}{32}n^3 - O(n^2)$ 4-rich circles, which is asymptotically the same as in Constructions 4.5 and 4.6.

As in Constructions 4.5 and 4.6, by stereographic projection, the number of ordinary and 4-rich planes spanned by a prism or an antiprism with a point

removed is equal to the number of ordinary and 4-rich circles spanned by an 'aligned' or 'offset' double polygon with a point removed respectively.

Construction 4.8 (Inverted double polygons)**.** This construction achieves the minimum number of strict ordinary circles as stated in Theorem 1.19, if n is odd.

Invert Construction 4.7 in the removed point p. The resulting point set has m points on a circle and $m-1$ points on a line disjoint from the circle. Every strict ordinary circle after the inversion corresponds to an ordinary circle not passing through p before the inversion. If m is odd, there are $(m-1)/2$ ordinary circles tangent at p and a further $m-1$ ordinary circles through p tangent to σ_2, so we obtain $m(m-1)-3(m-1)/2 = \frac{1}{2}(m-1)(2m-3)$ strict ordinary circles. For even m we similarly obtain $m(m-2)-3(m-2)/2 = \frac{1}{2}(m-2)(2m-3)$ strict ordinary circles. That is, we have $\frac{1}{4}(n-1)(n-2) = \frac{1}{4}n^2-\frac{3}{4}n+\frac{1}{2}$ strict ordinary circles when $n \equiv 1 \pmod 4$ and $\frac{1}{4}(n-3)(n-2) = \frac{1}{4}n^2-\frac{5}{4}n+\frac{3}{2}$ strict ordinary circles when $n \equiv 3 \pmod 4$.

If we remove another point from this inverted construction, we obtain a set of n points spanning $\frac{3}{8}n^2 - O(n)$ ordinary circles, where n is even.

4.3 Constructions on irreducible curves

We 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 in this section. By Propositions 3.7 and 3.18, 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 $H \cong \mathbb{Z}_n$, or $H \cong \mathbb{Z}_{n/2} \times \mathbb{Z}_2$ when $n \equiv 0 \pmod 4$.

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 k-tuples $(a_1, \ldots, a_k)$ with distinct

$a_i \in H$ that satisfy $m_1 a_1 \oplus \cdots \oplus m_k a_k = c$ by $[m_1, \ldots, m_k; c]$. Then the number of ordinary hyperplanes spanned by $H \oplus x$ is

$$\frac{1}{(d-1)!}[2, \underbrace{1, \ldots, 1}_{d-1 \text{ times}}; c]. \tag{4.2}$$

We show that we can always find a value of c for which (4.2) is at most $\binom{n-1}{d-1}$.

Lemma 4.9. *Let δ^* be an elliptic normal curve or the smooth points of a rational acnodal curve in $\mathbb{RP}^d$, $d \geqslant 2$. There exists a coset $H \oplus x$ of a finite subgroup H of δ^* of order n, with $(d+1)x \in H$, spanning 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 $(a_1, \ldots, a_d) \in H^d$ 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 $i = 2, \ldots, d$. Note that $2a_1 \oplus \cdots \oplus a_d = c$ for a_i distinct (and not equal to a_1) if and only if $b_2 \oplus \cdots \oplus b_d = c \ominus (d+1)a_1$ for b_i distinct and non-zero. Let

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

and let

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

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 $d+1$ and n are coprime, 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 $d+1$ and n are not coprime, 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

$$\begin{aligned}\sum_{c\in H}\sum_{j\in H} |A_{c,j}| &= \gcd(d+1,n)\sum_{c\in H}\sum_{k\in c\ominus(d+1)H} |B_k| \\ &= \gcd(d+1,n)\frac{n}{\gcd(d+1,n)}(n-1)\cdots(n-d+1) \\ &= n(n-1)\cdots(n-d+1).\end{aligned}$$

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 $[2, \overbrace{1,\ldots,1}^{d-1 \text{ times}}; c]$ 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 $[m_1,\ldots,m_k;c]$.

Lemma 4.10. $[m_1,\ldots,m_k;c] \leqslant 2m_k(k-1)!\binom{n}{k-1}$.

Proof. Consider a solution $(a_1,\ldots,a_k)$ of $m_1a_1 \oplus \cdots \oplus m_ka_k = c$ where all the a_i are distinct. We can choose $a_1,\ldots,a_{k-1}$ arbitrarily in $(k-1)!\binom{n}{k-1}$ ways, and then 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 $2m_k$ solutions. $\square$

Lemma 4.11. *We have the recurrence relation*

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

Proof. We can arbitrarily choose distinct values from H for $a_1,\ldots,a_{k-1}$, 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, $i = 1,\ldots,k-1$. $\square$

Lemma 4.12.

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

where

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

Proof. Let the length of $[m_1, \ldots, m_k; c]$ be k, and note that at each stage of the recurrence in Lemma 4.11 (when it applies), there are $(d-1)(d-2)\cdots(d-k)$ terms of length $d-k$. Applying Lemma 4.11 once, we obtain

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

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

$$\begin{aligned} [2, \underbrace{1, \ldots, 1}_{d-1 \text{ times}}; c] &= (d-1)! \left(\binom{n}{d-1} - \binom{n}{d-2} + \cdots \pm \binom{n}{(d+1)/2} \right) \\ &\quad \mp \cdots \mp (d-2)(d-4)\cdots 3 \cdot 1 [\underbrace{2, \ldots, 2}_{\frac{d+1}{2} \text{ times}}; c] \\ &= (d-1)! \left(\binom{n}{d-1} - \binom{n}{d-2} + \cdots \pm \binom{n}{(d+1)/2} \right) \\ &\quad \mp \cdots \mp (d-2)(d-4)\cdots 3 \cdot 1 [\underbrace{1, \ldots, 1}_{\frac{d+1}{2} \text{ times}}; c] \\ &\quad \mp (d-2)(d-4)\cdots 3 \cdot 1 \left([\underbrace{2, \ldots, 2}_{\frac{d+1}{2} \text{ times}}; c] - [\underbrace{1, \ldots, 1}_{\frac{d+1}{2} \text{ times}}; c] \right). \end{aligned}$$

We now bound the terms $A := \cdots + (d-2)(d-4)\cdots 3 \cdot 1[1, \ldots, 1; c]$ and $B := (d-2)(d-4)\cdots 3 \cdot 1([2, \ldots, 2; c] - [1, \ldots, 1; c])$ in the above equation. Note that we can apply Lemma 4.11 to each term in A, after which we obtain $(d-1)(d-2)\cdots(d-(d+1)/2)$ terms of length $(d-1)/2$. Using the

bound in Lemma 4.10, we then have

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

For B, we use the bound in Lemma 4.10 again 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 have

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

where $\varepsilon(d,n) = O\left(2^{-d/2}\binom{n}{(d-1)/2} + \binom{n}{(d-3)/2}\right)$ as claimed.

If d is even, we can continue the recurrence to reach

$$\begin{aligned}[2, \underbrace{1,\ldots,1}_{d-1 \text{ times}}; c] &= (d-1)!\left(\binom{n}{d-1} - \binom{n}{d-2} + \cdots \pm \binom{n}{d/2}\right) \\ &\quad \mp \cdots \mp \Big((d-3)(d-5)(d-7)\cdots 3\cdot 1 \\ &\qquad + 2(d-2)(d-5)(d-7)\cdots 3\cdot 1\end{aligned}$$

$$+ 3(d-2)(d-4)(d-7)\cdots 3\cdot 1 + \cdots$$
$$+ \frac{d}{2}(d-2)(d-4)(d-6)\cdots 2\Bigg)[3, \underbrace{2,\ldots,2}_{\frac{d}{2}-1 \text{ times}}; c],$$

whence we obtain the result in a similar way to the odd d case. □

Using Lemmas 4.9 and 4.12, we get a similar result to Lemma 4.9 for $(d+1)$-rich hyperplanes.

Corollary 4.13. *Let δ^* be an elliptic normal curve or the smooth points of a rational acnodal curve in $\mathbb{RP}^d$, $d \geqslant 2$. There exists a coset $H \oplus x$ of a finite subgroup H of δ^* of order n, with $(d+1)x \in H$, spanning at least*

$$\frac{1}{d+1}\left[\binom{n-1}{d} + O\left(d^2 2^{-d/2}\binom{n}{\lfloor (d-1)/2\rfloor} + \binom{n}{\lfloor (d-3)/2\rfloor}\right)\right]$$

$(d+1)$-rich hyperplanes.

Proof. By Propositions 3.7 and 3.18, the number of $(d+1)$-rich hyperplanes spanned by a coset $H \oplus x$ of δ^* is

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

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

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

so by Lemmas 4.9 and 4.12, there exists a coset spanning at least

$$\frac{1}{d+1}\left[\binom{n}{d} - \binom{n-1}{d-1} + O\left(d2^{-d/2}\binom{n}{\lfloor (d-1)/2\rfloor} + \binom{n}{\lfloor (d-3)/2\rfloor}\right)\right]$$
$$= \frac{1}{d+1}\left[\binom{n-1}{d} + O\left(d2^{-d/2}\binom{n}{\lfloor (d-1)/2\rfloor} + \binom{n}{\lfloor (d-3)/2\rfloor}\right)\right]$$

$(d+1)$-rich hyperplanes. □

As in the previous section, since ordinary and $(d+1)$-rich hyperplanes spanned by a set $S \subset \mathbb{R}^d$ are in one-to-one correspondence with ordinary and $(d+1)$-rich hyperspheres spanned by $\pi(S) \subset \mathbb{R}^{d-1}$, we only need to

consider one setting in the following constructions. We will focus on hyperplanes in this section, since if d is odd the trivial construction minimises the number of ordinary hyperspheres in $\mathbb{R}^d$ (see Theorem 1.21 and its proof in Section 6.4) and we do not know of any non-trivial construction spanning many $(d+2)$-rich hyperspheres.

Construction 4.14 (Elliptic normal curves)**.** This construction achieves the minimum number of ordinary hyperplanes and hyperspheres as stated in Theorems 1.16 and 1.21 respectively. It also achieves the maximum number of 4-rich planes and $(d+1)$-rich hyperplanes as stated in Theorems 1.14 and 1.17 respectively. If d is even, then it achieves the maximum number of 4-rich circles and $(d+2)$-rich hyperspheres as stated in Theorems 1.20 and 1.22 respectively.

Let δ be an elliptic normal curve in $\mathbb{RP}^d$, $d \geqslant 3$. By Proposition 3.7, the group $(\delta, \oplus)$ is isomorphic to $\mathbb{R}/\mathbb{Z}$ if δ has one semi-algebraically connected component, and isomorphic to $\mathbb{R}/\mathbb{Z} \times \mathbb{Z}_2$ if it has two. Summarising the above results, a coset $H \oplus x$ of δ of order n spans

$$\frac{1}{(d-1)!}[2, \underbrace{1, \ldots, 1}_{d-1 \text{ times}}; c] = \binom{n-1}{d-1} \pm O\left(d^2 2^{d/2} \binom{n}{\lfloor (d-1)/2 \rfloor} + \binom{n}{\lfloor (d-3)/2 \rfloor}\right)$$

ordinary hyperplanes and spans

$$\frac{1}{(d+1)!}[\underbrace{1, \ldots, 1}_{d+1 \text{ times}}; c] = \frac{1}{d+1}\left[\binom{n-1}{d} \pm O\left(d^2 2^{d/2} \binom{n}{\lfloor (d-1)/2 \rfloor} + \binom{n}{\lfloor (d-3)/2 \rfloor}\right)\right]$$

$(d+1)$-rich hyperplanes.

To find the exact extremal numbers for ordinary and $(d+1)$-rich hyperplanes spanned by $H \oplus x$, we can continue with the calculation of $[2, 1, \ldots, 1; c]$ in the proof of Lemma 4.12. As seen in the proof of Lemma 4.9, 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 the two cases $H \cong \mathbb{Z}_n$ and $H \cong \mathbb{Z}_{n/2} \times \mathbb{Z}_2$.

If $d = 3$, the number of ordinary planes spanned by $H \oplus x$ is equal to $\frac{1}{2}n^2 - O(n)$, and the maximum number of 4-rich planes is equal to

$$\begin{cases} \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{5}{6}n & \text{if } n \equiv 0 \pmod 8, \\ \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{11}{24}n - \frac{1}{4} & \text{if } n \equiv 1, 3, 5, 7 \pmod 8, \\ \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{7}{12}n - \frac{1}{2} & \text{if } n \equiv 2, 6 \pmod 8, \\ \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{5}{6}n - 1 & \text{if } n \equiv 4 \pmod 8. \end{cases}$$

Note that in the case $n \equiv 0 \pmod 4$, the maximum is attained when $H \cong \mathbb{Z}_{n/2} \times \mathbb{Z}_2$. Note also that both the number of ordinary planes and the maximum number of 4-rich planes are significantly greater than the corresponding numbers in Constructions 4.5, 4.6, and 4.7.

If $d = 4$, the minimum number of ordinary hyperplanes spanned by $H \oplus x$ is equal to

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

and the maximum number of 5-rich hyperplanes is equal to

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

If $d = 5$, the minimum number of ordinary hyperplanes spanned by $H \oplus x$ is equal to

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

and the maximum number of 6-rich hyperplanes is equal to

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

If $d = 6$, the minimum number of ordinary hyperplanes spanned by $H \oplus x$ is equal to

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

and the maximum number of 7-rich hyperplanes is equal to

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

Let $d = 2k$, and let δ' be a k-spherical elliptic normal curve in $\mathbb{R}^d$, $d \geqslant 2$. By stereographic projection (or Propositions 3.29 or 3.27), the extremal numbers for ordinary and $(d+2)$-rich hyperspheres spanned by a coset of δ' of order n is equal to the extremal numbers for ordinary and $(d+1)$-rich hyperplanes spanned by a coset of $\delta \subset \mathbb{R}^{d+1}$. In particular, when $d = 2$, the number of (strict) ordinary circles and 4-rich circles are both much greater than the corresponding numbers in Constructions 4.5, 4.6, 4.7, and 4.8.

Construction 4.15 (Rational acnodal curves and bounded $(k-1)$-spherical rational normal curves)**.** This construction achieves the minimum number of ordinary hyperplanes and hyperspheres as stated in Theorems 1.16 and 1.21 respectively, if $n \not\equiv 0 \pmod 4$. It also achieves the maximum number of 4-rich planes and $(d+1)$-rich hyperplanes as stated in Theorems 1.14 and 1.17 respectively, if $n \not\equiv 0 \pmod 4$. If d is even, then it achieves the maximum number of 4-rich circles and $(d+2)$-rich hyperspheres as stated in Theorems 1.20 and 1.22 respectively, if $n \not\equiv 0 \pmod 4$.

Let δ^* be the set of smooth points of a rational acnodal curve in $\mathbb{RP}^d$, $d \geqslant 3$. By Proposition 3.18, the group $(\delta^*, \oplus)$ is isomorphic to $\mathbb{R}/\mathbb{Z}$. Since we do not have to consider cosets of subgroups of $\mathbb{R}/\mathbb{Z} \times \mathbb{Z}_2$, the minimum number of ordinary hyperplanes spanned by a coset of δ^* is at least the corresponding number in Construction 4.14, and the maximum number of $(d+1)$-rich hyperplanes is at most the corresponding number in Construction 4.14.

Let $d = 2k$, and let δ' be a $(k-1)$-spherical bounded rational normal curve in $\mathbb{R}^d$, $d \geqslant 2$. We get the same situation as in Construction 4.14. If d is even, by stereographic projection (or Propositions 3.30 or 3.27), the extremal

numbers for ordinary and $(d+2)$-rich hyperspheres spanned by a coset of δ' of order n is equal to the extremal numbers for ordinary and $(d+1)$-rich hyperplanes spanned by a coset of $\delta^* \subset \mathbb{R}^{d+1}$, hence at best matching the numbers in Construction 4.14.

Construction 4.16 (Other inverted examples)**.** Let $d = 2k$. If we invert Construction 4.15 in a point on the $(k-1)$-spherical bounded rational normal curve in $\mathbb{R}^d$ that is not in the coset, then by Corollary 3.26, we obtain points on a k-spherical rational acnodal curve of degree $d+1$ (without its acnode) with the same number of ordinary and $(d+2)$-rich hyperspheres.

If we invert a k-spherical elliptic normal curve or rational acnodal curve of degree $d+1$ in a point not on the curve, then we obtain a $(k+1)$-spherical curve of degree $d+2$ by Corollary 3.25, again with the same number of ordinary and $(d+2)$-rich hyperspheres as in Constructions 4.14 and 4.15 respectively.

If $d = 2$, there will again be $\frac{1}{2}n^2 - O(n)$ (strict) ordinary circles and $\frac{1}{24}n^3 - O(n^2)$ 4-rich circles among the inverted points on the bicircular quartic.

Chapter 5

Structure theorems

In this chapter, we prove Theorems 1.9 to 1.12, our structure theorems for sets spanning few ordinary planes, hyperplanes, circles, and hyperspheres. We restate these theorems before their proofs.

5.1 Ordinary planes

We prove Theorem 1.9, our structure theorem for sets spanning few ordinary planes, in this section. First, we prove the weaker Lemma 5.1, using results from Chapter 2. This provides an alternative to Ball's approach in [4] . We then refine Lemma 5.1, replacing the polynomial error terms by linear error terms in Lemma 5.2. Finally, using the properties of space quartics from Chapter 3, we determine the precise characterisation of the possible configurations of sets spanning few ordinary planes as described in Theorem 1.9.

Lemma 5.1. *Let $K \geqslant 1$ and suppose $n \geqslant CK^8$ for some sufficiently large absolute constant $C > 0$. Let P be a set of n points in $\mathbb{RP}^3$ with no three collinear. If P spans at most Kn^2 ordinary planes, then we have one of the following:*

(*i*) *P is contained in the union of a plane and an additional $O(K^6)$ points;*

(*ii*) *P is contained in the union of two irreducible conics lying on distinct*

planes and an additional $O(K^8)$ points, with each conic containing $n/2 \pm O(K^8)$ points of P;

(*iii*) *P is contained in the union of a space quartic curve and an additional $O(K^5)$ points.*

Proof. Let P' denote the set of all points $p \in P$ such that there are at most $9Kn$ ordinary planes through p. Then $|P'| \geqslant 2n/3$, and for any $p \in P'$, the projection $\pi_p(P \setminus \{p\})$ spans at most $9Kn$ ordinary lines. Applying Theorem 2.2 to $\pi_p(P \setminus \{p\})$ for any $p \in P'$, we have one of three cases:

1. $\pi_p(P \setminus \{p\})$ is contained in the union of $O(K)$ lines and an additional $O(K^6)$ points;
2. $\pi_p(P \setminus \{p\})$ lies on the union of a conic σ and an additional $O(K^4)$ lines with $|\pi_p(P \setminus \{p\}) \cap \sigma| = n/2 \pm O(K^5)$;
3. $\pi_p(P \setminus \{p\})$ is contained in the union of an irreducible cubic and an additional $O(K^5)$ points.

This partitions P' into a disjoint union $P'_1 \cup P'_2 \cup P'_3$, depending on which of the above cases we obtain.

If $|P'_1| \geqslant 3$, let p_1, p_2, p_3 be three distinct points in P'_1. Then apart from $O(K^6)$ points, P is contained in the intersection of the union of $O(K)$ planes through p_1, the union of $O(K)$ planes through p_2, and the union of $O(K)$ planes through p_3.

Since p_1, p_2, p_3 are not collinear, if Π_i is a plane through p_i, then $P \cap \Pi_1 \cap \Pi_2 \cap \Pi_3$ is contained in a line, which contains at most two points of P except when $\Pi_1 = \Pi_2 = \Pi_3$ is the plane through p_1, p_2, p_3. Thus we have P lying in a plane except for at most $O(K^6) + O(K^2) = O(K^6)$ points, giving Case (*i*).

Next suppose $|P'_2| \geqslant 3n/5$, and let p_1, p_2, p_3 be three distinct points in P'_2. Then for each $i = 1, 2, 3$, there exist a quadric cone C_i with vertex p_i and planes $\{\Pi_{i,j} : j \in J_i\}$ through p_i with $|J_i| = O(K^4)$, such that $P \subset C_i \cup \bigcup_{j \in J_i} \Pi_{i,j}$ with $|P \cap C_i| = n/2 \pm O(K^5)$. So all but at most $O(K^8)$ points of P lie either on the intersection $C_1 \cap C_2 \cap C_3$, one of the $O(K^4)$ conics $C_i \cap \Pi_{i',j}$ for $i \neq i'$, or the plane Π through p_1, p_2, p_3.

It is well-known (and easy to deduce from Bézout's theorem (Theorem 2.9)) that the intersection of two quadrics is either an irreducible space quartic, a twisted cubic and a line, or conics and lines. We claim that any component δ of the intersection $C_1 \cap C_2 \cap C_3$ that is a twisted cubic or a space quartic cannot contain more than $O(K^4)$ points of P. Choose a point $p \in P_2' \setminus (C_1 \cap C_2 \cap C_3)$ such that the projection π_p restricted to δ is generically one-to-one. Such a p exists since $|P_2' \setminus (C_1 \cap C_2 \cap C_3)| \geqslant 3n/5 - (n/2 + O(K^5))$ and by Lemma 2.17 there are only $O(1)$ exceptional points. Then $\pi_p(\delta)$ is an irreducible planar cubic or quartic containing more than $O(K^4)$ points of P, contradicting $p \in P_2'$. So the components of $C_1 \cap C_2 \cap C_3$ which contain more than $O(K^4)$ points of P must all be conics.

No plane Π' can contain more than $n/2 + O(K^5)$ points of P, otherwise projecting from $p' \in P_2' \cap \Pi'$ would give a line containing more than $n/2 + O(K^5)$ points in the projection, contradicting $p' \in P_2'$. So choose a fourth point $p_4 \in P_2' \setminus \Pi$. As before, P is contained in the union of a quadric cone C_4 with vertex p_4 and $O(K^4)$ planes through p_4. Since $p_4 \notin \Pi$, if Π contains more than $O(K^4)$ points of P, all but at most $O(K^4)$ points of $P \cap \Pi$ must lie on the conic $C_4 \cap \Pi$. We then have that all but at most $O(K^8)$ points of P lie on $O(K^4)$ conics, and without loss of generality we can assume each conic contains more than $O(K^4)$ points. Let Σ be the set of such conics. (Note that the same argument shows that if a plane Π' contains a conic $\sigma \in \Sigma$, then all but at most $O(K^4)$ points of $P \cap \Pi'$ lie on σ.) We show that $|\Sigma| = 2$, and that for each $\sigma \in \Sigma$, $|P \cap \sigma| = n/2 \pm O(K^8)$, thus giving Case (*ii*).

Let σ_1 be the conic in Σ with the most points of P, and let Π_1 be the plane in which σ_1 lies. Since no plane contains more than $n/2 + O(K^5)$ points of P, we have that $|P \setminus \Pi_1| \geqslant n/2 - O(K^5)$. Let σ_2 be the conic in $\Sigma_1 \setminus \{\sigma_1\}$ with the most points of $P \setminus \Pi_1$, and let Π_2 be the plane in which σ_2 lies. Then $|P \cap \sigma_1| \geqslant |P \cap \sigma_2| \geqslant \Omega(n/K^4)$. Note that $\Pi_1 \neq \Pi_2$, as no plane contains more than $n/2 + O(K^5)$ points of P. Suppose there exists $q \in P_2' \setminus (\Pi_1 \cup \Pi_2)$, so that (by Bézout's theorem (Theorem 2.9)) σ_1 and σ_2 must both lie on the same quadric cone C with vertex q. Since $\sigma_1 \cup \sigma_2$ is the intersection of $\Pi_1 \cup \Pi_2$ and C, there can only be at most two such

points by Proposition 2.14. Therefore, all but at most $O(K^4)$ points of P_2' are contained in $\sigma_1 \cup \sigma_2$.

Without loss of generality, suppose $|P_2' \cap \sigma_1| \geqslant 3n/10 - O(K^4) = \Omega(n)$. By Proposition 2.14 again, there exist at most two points in $P_2' \cap \sigma_1$ such that their quadric cones intersect in σ_2 and σ' for some $\sigma' \in \Sigma \setminus \{\sigma_1, \sigma_2\}$. We can then choose a $q' \in P_2' \cap \sigma_1$ such that the only conic in Σ the quadric cone with vertex q' contains is σ_2. In particular, this means that $|P \cap \sigma_2| = n/2 \pm O(K^8)$. But then we also have $|P_2' \cap \sigma_2| = \Omega(n)$. Repeating the argument on σ_2 shows that $|P \cap \sigma_1| = n/2 \pm O(K^8)$ as well.

The remaining case is when $|P_3'| > 2n/3 - 3n/5 - 3 = \Omega(n)$. Let p and p' be two distinct points in P_3'. Then apart from $O(K^5)$ points, we have P lying mostly on the intersection δ of two cubic cones, which is a curve with irreducible components δ_i of total degree 9 by Bézout's theorem (Theorem 2.9).

Let δ_1 be a component for which $|P_3' \cap \delta_i|$ is maximal. Then $|P_3' \cap \delta_1| = \Omega(n)$. Projecting from any $q \in P_3' \cap \delta_1$, we get that $\overline{\pi_q(\delta_1 \setminus \{q\})}$ is an irreducible cubic, and so δ_1 must be non-planar. By Lemma 2.19, all but $O(1)$ points q' on δ_1 are such that the projection $\pi_{q'}$ restricted to $\delta_1 \setminus \{q'\}$ is generically one-to-one. We can thus choose such a $q' \in P_3' \cap \delta_1$ so that $\pi_{q'}$ projects $\delta_1 \setminus \{p_1\}$ generically one-to-one onto an irreducible cubic. The component δ_1 must then be a space quartic.

Now suppose there exists a component δ_2 containing more than $O(K^5)$ points of P. For any $q \in P_3' \cap \delta_1$, the cone $C_q(\delta_1)$ over δ_1 has to contain δ_2 by Bézout's theorem (Theorem 2.9). If δ_2 is non-planar, this contradicts Lemma 2.20, since δ_1 is also non-planar. So suppose δ_2 is planar. By Proposition 2.16, for all but finitely many $q' \in \delta_2 \setminus \delta_1$, $\pi_{q'}(\delta_1)$ is a planar quartic. Since a planar quartic has at most three singularities, all but finitely many $q' \in \delta_2 \setminus \delta_1$ lie on at most three secants or tangents of δ_1. All but finitely many $q' \in \delta_2 \setminus \delta_1$ is thus contained in at most three cones $C_q(\delta_1)$, a contradiction. We thus have all but at most $O(K^5)$ points of P lying on a single space quartic, giving Case (*iii*). □

To get a more precise description of the structure of sets spanning few ordinary planes, we need a more precise description of sets that lie on certain

cubic curves and span few ordinary lines. Using results from Section 2.1, we reduce the polynomial error terms in Lemma 5.1 to linear errors $O(K)$. Since this refinement relies only on Green and Tao's results as stated in Section 2.1, our proof will be similar to Ball's proof in [4].

Lemma 5.2. *Let $K \geqslant 1$ and suppose $n \geqslant CK^8$ for some sufficiently large constant absolute $C > 0$. Let P be a set of n points in $\mathbb{RP}^3$ with no three collinear. If P spans at most Kn^2 ordinary planes, then P differs in at most $O(K)$ points from one of the following:*

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

(*ii*) *a subset of two disjoint irreducible conics lying on distinct planes, with each conic containing $n/2 \pm O(K)$ points;*

(*iii*) *a subset of a space quartic.*

Proof. Let P', P'_1, P'_2, and P'_3 be as in the proof of Lemma 5.1.

If $|P'_1| \geqslant 3$, we are in Case (*i*) of Lemma 5.1, and all but at most $O(K^6)$ points of P lie in a plane Π. Let $k := |P \setminus \Pi|$. Then for a fixed point $p \in P \setminus \Pi$, there are $\binom{n-k}{2}$ planes through p and two points of $P \cap \Pi$, of which at most $k-1$ are not ordinary. Therefore, there are at least $k(\binom{n-k}{2} - k + 1)$ ordinary planes. Since this is at most Kn^2 and $n \geqslant CK^8 > k = O(K^6)$ for sufficiently large C, we obtain that $k = O(K)$.

If $|P'_2| \geqslant 3n/5$, we are in Case (*ii*) of Lemma 5.1, and all but at most $O(K^8)$ points of P lie on the union of two conics $\sigma_1 \cup \sigma_2$. Let $S = P \setminus (\sigma_1 \cup \sigma_2)$. Let Π_i be the plane supporting σ_i, $i = 1, 2$. For any $p \in S \cap \Pi_1$ except at most two points also on Π_2, the projection π_p maps σ_1 to a line and σ_2 to a conic. For any $p \in S \setminus (\Pi_1 \cup \Pi_2)$ except at most two points, the projection π_p maps σ_1 and σ_2 to distinct conics (by Proposition 2.14). Hence, for all but at most four points $p \in S$, there are at most four points $x \in P \cap \sigma_1$ for which $\pi_p(x) \in \pi_p(\sigma_2)$ and at most four points $x \in P \cap \sigma_2$ for which $\pi_p(x) \in \pi_p(\sigma_1)$. Therefore, for any $q \in P'_2 \cap (\sigma_1 \cup \sigma_2)$ except at most $4|S| + 4|S|$ points, we have that $\pi_q(S)$ is disjoint from the line and the conic onto which all but at most $O(K^8)$ points of P map. Such a q exists as $|P'_2| \geqslant 3n/5$. By Lemma 2.3,

the set $\pi_q(P \setminus \{q\})$ differs from a set X projectively equivalent to a regular m-gon and the m points at infinity corresponding to the diagonals of the m-gon in at most $O(K^8)$ points, where $m = n/2 \pm O(K^8)$. By Lemma 2.7, there are at least $n - O(K^8)$ ordinary lines through a fixed point of $\pi_q(S)$ and a point of $\pi_q(P \setminus (S \cup \{q\}))$. Thus, there at least $|S|(n - O(K^8))$ ordinary lines. Since there are at most $9Kn$ ordinary lines and $n \geqslant CK^8$ for sufficiently large C, we obtain that $|S| = O(K)$. The same argument shows that $|\pi_q(P \setminus \{q\}) \setminus X| = O(K)$, hence $|P \cap \sigma_i| \leqslant m + O(K)$, $i = 1, 2$.

It remains to show that $|X \setminus \pi_q(P \setminus \{q\})| = O(K)$. Note that through any point $y \in X$, there are at least $m/2 - 1$ lines through y and two more points of X. By removing a point from X, we thus create at least $m/2 - O(K)$ ordinary lines. Therefore, there are at least $|X \setminus \pi_q(P \setminus \{q\})|(n/4 - O(K^8))$ ordinary lines. Since this is at most $9Kn$ and $n \geqslant CK^8$ for sufficiently large C, we obtain that $|X \setminus \pi_q(P \setminus \{q\})| = O(K)$.

Finally, if $|P_3'| > 2n/3 - 3n/5 - 3 = \Omega(n)$, we are in Case (*iii*) of Lemma 5.1, and all but at most $O(K^5)$ points of P lie on a space quartic δ. By Lemma 2.17, the projection from all but finitely many points $p \in P \setminus \delta$ maps δ generically one-to-one onto a planar quartic, which has at most three singular points. Thus, there are at most six points $x \in \delta$ such that px intersects δ again. Choose a point $q \in P_3' \cap \delta$ that is not one of these at most $6|P \setminus \delta|$ points. Such a q exists as $|P_3'| = \Omega(n)$. Then, if we project from q, each point in $P \setminus \delta$ is projected onto a point not on the cubic $\overline{\pi_q(\delta \setminus \{q\})}$. By Lemma 2.4, $\pi_q(P \setminus \{q\})$ differs in at most $O(K^5)$ points from a coset of a subgroup of an elliptic curve or the smooth points of an acnodal cubic. By Lemma 2.8, there are at least $|P \setminus \delta|(n/1000 - |P \setminus \delta|)$ ordinary lines. Since this is at most $9Kn$ and $n \geqslant CK^8 > |P \setminus \delta| = O(K^5)$ for sufficiently large C, we obtain that $|P \setminus \delta| = O(K)$. □

We now show that if we are in Case (*ii*) of Lemma 5.2, then there is a quadric containing both conics.

Lemma 5.3. *Let $K \geqslant 1$ and suppose $n \geqslant CK^8$ for some sufficiently large absolute constant $C > 0$. Let P be a set of n points in $\mathbb{RP}^3$ with no three collinear, spanning at most Kn^2 ordinary planes. Suppose P has $n/2 \pm O(K)$*

points on each of two disjoint irreducible conics σ_1 and σ_2 lying on two distinct planes Π_1 and Π_2 respectively. Then there exists an irreducible quadric that contains $\sigma_1 \cup \sigma_2$.

Proof. Let P' be as in the proofs of Lemmas 5.1 and 5.2 above. We convert the problem to one in Euclidean geometry, by identifying $\mathbb{RP}^3$ with the Euclidean affine space $\mathbb{R}^3$ together with a projective plane at infinity. We apply a projective transformation such that the planes Π_1 and Π_2 become parallel, and such that σ_1 is a circle. It then suffices to show that σ_2 is a circle as well, as $\sigma_1 \cup \sigma_2$ is then contained in a circular cone or cylinder.

Choose $p_i \in P' \cap \sigma_i$, $i = 1, 2$, and consider the projection $\pi_i := \pi_{p_i}$ to be onto the plane Π_{3-i}. Then by Lemma 5.2, π_1 projects all but at most $O(K)$ points of P onto the line at infinity and a conic on Π_2, which are disjoint by Lemma 2.3. Since the conic $\sigma_2 = \pi_1(\sigma_2)$ is disjoint from the line at infinity, it is an ellipse.

Now let $p_2 \in P' \cap \sigma_2$, and consider the projection π_2. By Lemma 2.3, $\pi_2(P \setminus \{p_2\})$ differs in at most $O(K)$ points from the vertices of a regular m-gon and the m points at infinity corresponding to the diagonals of the m-gon, for some $m = n/2 \pm O(K)$. In particular, $P \cap \sigma_1$ differs in at most $O(K)$ points from a regular m-gon.

Therefore, $\pi_1(P \cap \sigma_1 \setminus \{p_1\})$ differs in at most $O(K)$ points from the points at infinity corresponding to the diagonals of the regular m-gon on σ_1, which are also (if m is even, half of) the points at infinity corresponding to the tangents to σ_1 at the vertices of the m-gon. By Lemma 2.3 again, $\pi_1(P \cap \sigma_2)$ differs in at most $O(K)$ points from an m-gon on the ellipse σ_2, projectively equivalent to a regular m-gon.

It easily follows that all but at most $O(K)$ of the tangent lines to σ_2 at the vertices of the m-gon are ordinary lines and so all but $O(K)$ must be points at infinity of $\pi_1(P \cap \sigma_1 \setminus \{p_1\})$. Let a, b, c be three consecutive vertices of the m-gon on σ_2 such that $a, b, c \in \pi_1(P \cap \sigma_2)$. Then the point d where the tangents at a and c intersect, forms an isosceles triangle with a and c, and we have $|ad| = |cd|$. But this can only happen if d lies on one of the axes of symmetry of σ_2. Since n is sufficiently large depending on K, we can

find many triples of consecutive vertices of the m-gon on σ_2, and we get a contradiction unless σ_2 is a circle. □

The following lemma shows that if we are in Case (*iii*) of Lemma 5.2, then the space quartic is either elliptic or rational of the first species.

Lemma 5.4. *Let $K \geqslant 1$ and suppose $n \geqslant CK^8$ for some sufficiently large absolute constant $C > 0$. Let P be a set of n points in $\mathbb{RP}^3$ with no three collinear, spanning at most Kn^2 ordinary planes. Suppose all but at most $O(K)$ points of P lie on a rational space quartic δ_p. Then δ_p is of the first species.*

Proof. Let $q_\alpha \in \delta_p$ be parametrised by $[\alpha, 1] \in \mathbb{RP}^1$. As before, let P' denote the set of all points $q \in P \cap \delta_p$ with at most $9Kn$ ordinary planes through q. Since P spans at most Kn^2 ordinary planes, we have $|P'| \geqslant 2n/3 - O(K)$. Let π_α be the projection map from q_α. By Lemma 2.19, we can choose $q_\alpha \in P'$ such that all but at most $O(K)$ points of $\pi_\alpha(P \setminus \{q_\alpha\})$ lie on a cubic curve γ_α. By Lemma 2.4, this set differs in at most $O(K)$ points from a coset of γ_α, and γ_α is acnodal (since δ_p is rational). Since n is sufficiently large, there exist three distinct points $q_A, q_B, q_C \in P'$ such that for $\Omega(n)$ many $q_\alpha \in P'$, the projected points $\pi_\alpha(q_A), \pi_\alpha(q_B), \pi_\alpha(q_C)$ are consecutive elements in the coset given by Lemma 2.4.

Let $\oplus_\alpha$ denote the group operation on γ_α so that we have $\pi_\alpha(q_A) \oplus_\alpha \pi_\alpha(q_C) = 2\pi_\alpha(q_B)$. By considering the geometric definition of $\oplus_\alpha$ we obtain that if q_β is the fourth point of intersection between δ_p and the plane through q_A, q_C, q_α, and $q_{\beta'}$ the fourth point of intersection between δ_p and the plane through q_B, q_B, q_α (that is, containing the tangent line of δ_p at q_B and passing through q_α), then $\beta = \beta'$. Equivalently, by Lemma 3.11, we have

$$F(A, 1, C, 1, \alpha, 1, \beta, 1) = 0 = F(B, 1, B, 1, \alpha, 1, \beta, 1).$$

Since F is a polynomial and the above is true for sufficiently many α (since n is sufficiently large), it holds for all $\alpha \in \mathbb{R}$.

Note that

$$F(A,1,C,1,\alpha,1,\beta,1) = \begin{pmatrix}\alpha\beta, & \alpha+\beta, & 1\end{pmatrix}\begin{pmatrix}p_0 & p_1 & p_2\\ p_1 & p_2 & p_3\\ p_2 & p_3 & p_4\end{pmatrix}\begin{pmatrix}AC\\ A+C\\ 1\end{pmatrix},$$

with a similar expression for $F(B,1,B,1,\alpha,1,\beta,1)$. Since $\begin{pmatrix}AC, & A+C, & 1\end{pmatrix}$ and $\begin{pmatrix}B^2, & 2B, & 1\end{pmatrix}$ are linearly independent, the set of vectors

$$\left\{\begin{pmatrix}\alpha\beta, & \alpha+\beta, & 1\end{pmatrix}\begin{pmatrix}p_0 & p_1 & p_2\\ p_1 & p_2 & p_3\\ p_2 & p_3 & p_4\end{pmatrix} : \alpha\in\mathbb{R}\right\}$$

lie in a 1-dimensional linear subspace of $\mathbb{R}^3$. If the catalecticant of the fundamental binary form f_p of δ_p, which is the determinant $p_0p_2p_4 - p_0p_3^2 - p_1^2p_4 + 2p_1p_2p_3 - p_2^3$ of the above 3×3 matrix, is non-zero, then

$$\left\{\begin{pmatrix}\alpha\beta, & \alpha+\beta, & 1\end{pmatrix} : \alpha\in\mathbb{R}\right\}$$

also lies in a 1-dimensional subspace of $\mathbb{R}^3$, in which case both $\alpha\beta$ and $\alpha+\beta$ are constants depending only on δ_p, say $\alpha\beta = c_1$ and $\alpha+\beta = c_2$. But then α is a root of the fixed quadratic equation $x^2 - c_2x + c_1 = 0$, a contradiction. Hence, the catalecticant vanishes, and δ_p is of the first species by Lemma 3.16. □

From Lemmas 5.2, 5.3, and 5.4, we see that up to at most $O(K)$ points, the set P lies on a plane, two disjoint conic sections of an irreducible quadric (which by applying a projective transformation if necessary we can assume to be two disjoint circles on a sphere), or a space quartic of the first species. It thus remains to determine the precise structure of P. To do so, we first consider the effect of adding and/or removing $O(K)$ points.

Lemma 5.5. *Let P be a set of n points in $\mathbb{RP}^3$ with no three collinear. Let P' be a set that differs from P in at most K points, also with no three points collinear. If P spans m ordinary planes, then P' spans at most $m + O(Kn^2 + K^2n + K^3)$ ordinary planes.*

Proof. First note that if we add a point to P, we create at most $\binom{n}{2}$ ordinary planes. Secondly, since two planes intersect in a line that contains at most two points, the number of 4-rich planes through a fixed point in P is at most $\frac{1}{3}\binom{n-1}{2}$, so by removing a point we create at most $\frac{1}{3}\binom{n-1}{2} < \binom{n}{2}$ ordinary planes. It follows that by adding and removing K points, we create at most

$$\binom{n}{2} + \binom{n+1}{2} + \cdots + \binom{n+K-1}{2} = O(Kn^2 + K^2 n + K^3)$$

ordinary planes. □

Applying the additive combinatorial Lemma 2.6 from Section 2.1 then gives us the precise structure of P in Cases (*ii*) and (*iii*) of Lemma 5.2.

Lemma 5.6. *Let P be a set of n points in $\mathbb{RP}^3$ with no three collinear, spanning at most Kn^2 ordinary planes, and suppose $n \geqslant CK$ for some sufficiently large absolute constant $C > 0$. Suppose all but at most K points of P lie on two disjoint planar sections of a quadric, with $n/2 \pm O(K)$ points of P on each conic. Then up to a projective transformation, P differs in at most $O(K)$ points from a prism or an antiprism.*

Proof. By a projective transformation, we can assume that all but at most K points of P lie on the two circles $\sigma_1 = \{(\cos(\theta), \sin(\theta), 1) : \theta \in [0, 2\pi)\}$ and $\sigma_2 = \{(\cos(\theta), \sin(\theta), -1) : \theta \in [0, 2\pi)\}$, which we gave a group structure in Corollary 3.32.

Let $P_1 = P \cap \sigma_1$ and $P_2 = P \cap \sigma_2$. Then $|P \triangle (P_1 \cup P_2)| = O(K)$, and by Lemma 5.5, $P_1 \cup P_2$ spans at most $O(Kn^2)$ ordinary planes. If $a, b \in \sigma_1$ and $c \in \sigma_2$ with $a \neq b$, then by Corollary 3.32, the plane through a, b, c meets $\sigma_1 \cup \sigma_2$ again in the unique point $d = \ominus(a \oplus b \oplus c)$. This implies $d \in P_2$ for all but at most $O(Kn^2)$ triples (a, b, c) with $a, b \in P_1$ and $c \in P_2$. Applying Lemma 2.6 with $d = 3$, $A_1 = A_2 = P_1$, $A_3 = P_2$, and $A_4 = \ominus P_2$, we get cosets $H \oplus x$ and $H \oplus y$ of a subgroup H of $\sigma_1 \cup \sigma_2$ such that $|P_1 \triangle (H \oplus x)|, |P_2 \triangle (H \oplus y)| = O(K)$ and $2x \oplus 2y \in H$, where $x \in \sigma_1$ and $y \in \sigma_2$. It follows that H is a subgroup of σ_1, hence H is a cyclic group of order $m = n/2 \pm O(K)$, and $H \oplus x$ and $H \oplus y$ are the vertex sets of regular m-gons inscribed in σ_1 and σ_2, respectively, and $\sigma_1 \cup \sigma_2$ is a prism or an antiprism depending on whether $x \oplus y \in H$ or not. □

Lemma 5.7. *Let P be a set of n points in $\mathbb{RP}^3$ with no three collinear, spanning at most Kn^2 ordinary planes, and suppose $n \geqslant CK$ for some sufficiently large absolute constant $C > 0$. Suppose all but at most K points of P lie on a space quartic δ of the first species. Then P differs in at most $O(K)$ points from a coset of a subgroup of δ^*, the smooth points of δ. In particular, δ is either an elliptic or acnodal space quartic.*

Proof. Let $P' = P \cap \delta^*$. Then $|P \triangle P'| = O(K)$, and by Lemma 5.5, P' spans at most $O(Kn^2)$ ordinary planes.

First suppose δ is an elliptic, cuspidal, or acnodal space quartic. If a, b, $c \in \delta^*$ are distinct, then by Propositions 3.7 and 3.18, the plane through a, b, c meets δ again in the unique point $d = \ominus(a \oplus b \oplus c)$. This implies that $d \in P'$ for all but at most $O(Kn^2)$ triples a, b, $c \in P'$, or equivalently $a \oplus b \oplus c \in \ominus P'$. Applying Lemma 2.6 with $d = 3$, $A_1 = A_2 = A_3 = P'$, and $A_4 = \ominus P'$, we obtain a subgroup H of δ^* and a coset $H \oplus x$ such that $|P \triangle (H \oplus x)| = O(K)$ and $|\ominus P' \triangle (H \oplus 3x)| = O(K)$, which is equivalent to $|P \triangle (H \ominus 3x)| = O(K)$. Thus we have $|(H \oplus x) \triangle (H \ominus 3x)| = O(K)$, which implies $4x \in H$. Also, δ cannot be cuspidal, otherwise by Proposition 3.18 we have $\delta^* \cong (\mathbb{R}, +)$, which has no finite subgroup of order greater than 1.

Now suppose δ is a crunodal space quartic. By Proposition 3.18, there is a bijective map $\varphi : (\mathbb{R}, +) \times \mathbb{Z}_2 \to \delta^*$ such that a, b, c, $d \in \delta^*$ lie in a plane 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 3.18 that $\delta^* \cong (\mathbb{R}, +) \times \mathbb{Z}_2$, which has no finite subgroup of order greater than 2. Otherwise, the plane through distinct a, b, $c \in \delta^*$ meets δ again in the unique point $d = \varphi(0, 1) \ominus (a \oplus b \oplus c)$. As before, this implies that $d \in P'$ for all but at most $O(Kn^2)$ triples a, b, $c \in P'$, or equivalently $a \oplus b \oplus c \in \varphi(0, 1) \ominus P'$. Applying Lemma 2.6 with $d = 3$, $A_1 = A_2 = A_3 = P'$, and $A_4 = \varphi(0, 1) \ominus P'$, we obtain a finite subgroup H of δ^*, giving a contradiction as before. □

Theorem 1.9, restated below, then follows easily.

Theorem 1.9 (Ordinary planes)**.** *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 three collinear. If P spans at most Kn^2 ordinary planes, then up to a projective transformation, 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 prism or an antiprism;*

(*iii*) *a coset $H \oplus x$ of a subgroup H of an elliptic space quartic curve or the smooth points of an acnodal space quartic curve, for some x such that $4x \in H$.*

Conversely, every set of these types spans at most $C'Kn^2$ ordinary planes for some absolute constant $C' > 0$.

Proof. The forward statement follows from directly from Lemmas 5.2, 5.6, and 5.7.

For the converse, note that as seen in Chapter 4, a prism or an antiprism spans at most $\frac{1}{4}n^2$ ordinary planes, and a coset of a finite subgroup of an elliptic space quartic or the smooth points of an acnodal space quartic spans at most $\frac{1}{2}n^2$ ordinary planes. It follows from Lemma 5.5 that if we add and/or remove $O(K)$ points, then there will be at most $O(Kn^2)$ ordinary planes. □

5.2 Ordinary hyperplanes

We prove Theorem 1.10, our structure theorem for sets spanning few ordinary hyperplanes, in this section. The main idea is to induct on the dimension d via projection. We first prove the following weaker lemma using results from Chapter 2.

Lemma 5.8. *Let $d \geqslant 4$, $K > 0$, and suppose $n \geqslant C \max\{(dK)^8, d^{12}\}$ 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 $O(d2^dK)$ 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 $n \geqslant C' \max\{(d\prod_{i=1}^{d}(1+\frac{1}{i^2})K)^8, d^{12}\}$, where $C' > 0$ is a sufficiently large absolute constant, all but at most $O(d2^d\prod_{i=1}^{d}(1+\frac{1}{i^2})K) = O(d2^dK)$ 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. We assume that this holds in $\mathbb{RP}^{d-1}$ if $d \geqslant 5$, while Theorem 1.9 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 $(d+\frac{1}{d})K\binom{n-1}{d-2}/(d-1)$ ordinary hyperplanes through p. Then $|P'| \geqslant n/(d^2+1)$. For any $p \in P'$, the projection $\pi_p(P\backslash\{p\})$ is a set of $n-1 \geqslant C' \max\{(\prod_{i=1}^{d-1}(i+\frac{1}{i})K)^8, (d-1)^{12}\}$ points that spans at most $(d+\frac{1}{d})K\binom{n-1}{d-2}/(d-1)$ 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. By induction, for any $p \in P'$, all but at most

$$O\left((d-1)2^{d-1}\prod_{i=1}^{d-1}\left(1+\frac{1}{i^2}\right)\left(d+\frac{1}{d}\right)\frac{K}{d-1}\right) = O\left(d2^{d-1}\prod_{i=1}^{d}\left(1+\frac{1}{i^2}\right)K\right)$$

points of $\pi_p(P\setminus\{p\})$ are contained in a $(d-2)$-flat or an irreducible non-degenerate curve γ_p of degree d in $\mathbb{RP}^{d-1}$, or in the $d=4$ case, two conics with $n/2 \pm O(K)$ points on each.

If there exists a $p \in P'$ such that all but at most $O(d2^{d-1}\prod_{i=1}^{d}(1+\frac{1}{i^2})K)$ points of $\pi_p(P\setminus\{p\})$ are contained in a $(d-2)$-flat, then we are done. Thus we may assume without loss of generality that for all $p \in P'$, the other case (or two cases when $d=4$) occurs.

Let p and p' be two distinct points of P'. Then all but at most $O(2\cdot d2^{d-1}\prod_{i=1}^{d}(1+\frac{1}{i^2})K)$ 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 and irreducible (over $\mathbb{C}$), the two cones are 2-dimensional irreducible complex varieties. Since their vertices p and p' are distinct, the cones are distinct, and so their intersection is a variety of dimension at most 1. By Bézout's theorem (Theorem 2.9), δ has total degree at most d^2. Let $\delta_1, \ldots, \delta_k$ be the

1-dimensional components of δ, where $k \leqslant d^2$. Suppose also that δ_1 contains the most points of P' amongst all the δ_i, so that $|P' \cap \delta_1| = \Omega(n/d^4)$. Choose a $q \in P' \cap \delta_1$ such that π_q is generically one-to-one on δ_1. Such a q exists since by Lemma 2.19 there are at most $O(\deg(\delta_1)^4) = O(d^8)$ exceptional points and $n = \Omega(d^{12})$. By Bézout's theorem (Theorem 2.9), π_q has to map $\delta_1 \setminus \{q\}$ onto γ_q (or, when $d = 4$, possibly onto a conic containing $n/2 \pm O(K)$ points of $\pi_q(P \setminus \{q\})$), 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 $d+1$. Since $|P' \cap \delta_1| = \Omega(n/d^4)$ and any δ_i, $i \neq 1$, that contains more than three points is non-planar, by Lemma 2.20, we can 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 $\pi_{q'}^{-1}(\pi_{q'}(\gamma_{q'}))$ does not contain any other δ_i, $i \neq 1$, that contains more than three points. Then by Bézout's theorem (Theorem 2.9), we obtain that

$$|P \setminus \delta_1| \leqslant O(d^3) + O\left(d2^d \prod_{i=1}^{d} \left(1 + \frac{1}{i^2}\right) K\right) = O(d2^d K),$$

since $K = \Omega(1/d)$ by [6, Theorem 2.4].

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 2.17 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 2.9) and Theorem 1.9, $\pi_{q'}(\delta_1 \setminus \{q'\})$ has to be mapped onto a conic, which gives a contradiction.

We have shown that all but $O(d2^d K)$ points of P are contained in a hyperplane or an irreducible non-degenerate curve δ of degree $d+1$. By Proposition 3.1, this curve is either elliptic or rational. It remains to show that if δ is rational, then it has to be singular. As shown above for $\Omega(n/d^4)$ points $p \in \delta$, the projection $\overline{\pi_p(\delta \setminus \{p\})}$ is a rational curve of degree d that is singular by the induction hypothesis. Lemma 3.15 now implies that δ is singular. □

As in the previous section, to get the coset structure on the curves as stated in Theorem 1.10, we use Lemma 2.6. Before that, we again need to know that removing K points from a set does not change the number of ordinary hyperplanes it spans by too much. The following lemma generalises Lemma 5.5.

Lemma 5.9. *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 $m + K\frac{1}{d}\binom{n-1}{d-1}$ ordinary hyperplanes.*

Proof. Fix a point $p \in P$. Since every d points span a hyperplane, there are at most $\binom{n-1}{d-1}$ hyperplanes spanned by points of P through p. Thus, the number of $(d+1)$-rich hyperplanes through p is at most $\frac{1}{d}\binom{n-1}{d-1}$, since these $d+1$ points have 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 $K\frac{1}{d}\binom{n-1}{d-1}$ ordinary hyperplanes. □

The following lemma then translates the additive combinatorial Lemma 2.6 to our geometric setting.

Lemma 5.10. *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 5.9, P' spans at most $K\binom{n-1}{d-1} + O(dK\frac{1}{d}\binom{n-1}{d-1}) = O(K\binom{n-1}{d-1})$ 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 3.7 and 3.18, 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 $(a_1, \ldots, a_d) \in (P')^d$ with all a_i distinct. There are also at most $\binom{d}{2}n^{d-1}$ d-tuples $(a_1, \ldots, a_d) \in (P')^d$ 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 $(a_1, \ldots, a_d) \in (P')^d$. Applying Lemma 2.6 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 of which 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 3.18 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 3.18, 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 3.18 that $\delta^* \cong (\mathbb{R}, +) \times \mathbb{Z}_2$, which has no finite subgroup of order greater than 2. Otherwise, the hyperplane through distinct $a_1, \ldots, a_d \in \delta^*$ 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 $(a_1, \ldots, a_d) \in (P')^d$, or equivalently $a_1 \oplus \cdots \oplus a_d \in \varphi(0, 1) \ominus P'$. Applying Lemma 2.6 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 1.10, restated below.

Theorem 1.10 (Ordinary hyperplanes)**.** *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 $(d+1)x \in H$.

Conversely, every set of these types spans at most $C'2^dK\binom{n-1}{d-1}$ ordinary hyperplanes for some absolute constant $C' > 0$.

Proof. Without loss of generality we may assume that P does not lie on a hyperplane. Then by [6, Theorem 2.4], $K = \Omega(1/d)$, hence $d^3 2^d K = \Omega(d^{12})$, so we can apply Lemma 5.8 to P to obtain that 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 5.10 to obtain Case (ii) of the theorem, proving the forward statement.

Applying Lemma 5.9 to a set contained in a hyperplane (so that it spans no ordinary hyperplanes) for a set of type (i), and to Constructions 4.14 and 4.15 for a set of type (ii), gives the converse statement. □

5.3 Ordinary circles

We prove two structure theorems for sets spanning few ordinary circles in this section. We first prove the weaker Theorem 5.15, which only requires inversion in the plane and Green and Tao's stronger structure theorem for sets spanning few ordinary lines (Theorem 2.1). We then prove Theorem 1.11, which relies on Theorem 1.9, our structure theorem for sets spanning few ordinary planes, and stereographic projection. Note from Section 5.1 that Theorem 1.9 only required Green and Tao's weaker structure theorem (Theorem 2.2).

The following lemma forms the basis of the proof of Theorem 5.15. Recall that 3-rich lines are also ordinary circles.

Lemma 5.11. *Let $K > 0$ and let n be sufficiently large depending on K. If a set P of n points in $\mathbb{R}^2$ spans at most Kn^2 ordinary circles, then all but at most $O(K)$ points of P lie on a (possibly non-irreducible) bicircular quartic.*

Proof. We wish to show that P lies mostly on a bicircular quartic (we will repeatedly use 'mostly' to mean 'for all but $O(K)$ points').

Note that for at least $2n/3$ points p of P, there are at most $9Kn$ ordinary circles through p, hence the set $\iota_p(P \setminus \{p\})$ spans at most $9Kn$ ordinary lines. Let P' be the set of such points. For n sufficiently large depending on K, applying Theorem 2.1 to $\iota_p(P \setminus \{p\})$ for any $p \in P'$ gives that $\iota_p(P \setminus \{p\})$ lies mostly on a line, a line and a conic, or an elliptic or acnodal cubic.

If there exists $p \in P'$ such that $\iota_p(P \setminus \{p\})$ lies mostly on a line, then inverting again in p, we see that P must lie mostly on a line or a circle.

If there exists $p \in P'$ such that $\iota_p(P \setminus \{p\})$ lies mostly on a line ℓ and a disjoint conic σ, we have two cases, depending on whether p lies on ℓ or not.

If $p \in \ell$, we invert again in p to find that P lies mostly on the union of ℓ and $\iota_p(\sigma)$. By Corollary 3.23, $\iota_p(\sigma)$ is either a circle (if σ is a circle) or an irreducible bicircular quartic (if σ is a non-circular conic). Furthermore, p is the only point that could possibly lie on both ℓ and $\iota_p(\sigma)$. Since roughly $n/2$ points of P lie on ℓ, there must be another point $q \in \ell \cap P'$ that does not lie on $\iota_p(\sigma)$. In $\iota_q(P \setminus \{q\})$, the line ℓ remains a line, and by definition of P' the set $\iota_q(P \setminus \{q\})$ spans few ordinary lines, so Theorem 2.1 tells us $\iota_q(\iota_p(\sigma))$ is a conic. It follows from Corollary 3.23 that $\iota_p(\sigma)$ cannot be a quartic, since we inverted in the point q outside $\iota_p(\sigma)$ and did not obtain a quartic. That means $\iota_p(\sigma)$ has to be a circle, and it is disjoint from ℓ. Thus, P lies mostly on the union of a line and a disjoint circle.

If $p \notin \ell$, we invert in p to see that P lies mostly on the union of the circle $\iota_p(\ell)$ and the curve $\iota_p(\sigma)$, which is either a circle or a quartic. Again p is the only point that can lie on both curves. Inverting in another point $q \in \iota_p(\ell) \cap P'$, $\iota_q(\iota_p(\ell))$ becomes a line, so Theorem 2.1 tells us that $\iota_q(\iota_p(\sigma))$ is a conic, so that $\iota_p(\sigma)$ must be a circle disjoint from $\iota_p(\ell)$ as before. Thus, P lies mostly on the union of two disjoint circles.

The case that remains is when for all $p \in P'$, the set $\iota_p(P \setminus \{p\})$ lies mostly on an elliptic or acnodal cubic γ. Fix such a p, and consider $\iota_p(\gamma)$, which mostly contains P. If γ is not a circular cubic, then by the classification in Section 3.3 it has circular degree three, so $\iota_p(\gamma)$ has circular degree three

as well. For any $q \in \iota_p(\gamma) \cap P'$ other than p, the curve $\iota_q(\iota_p(\gamma))$ is also a cubic curve, by the definition of P' and Theorem 2.1. By Case (*iii*) of Corollary 3.23, this can only happen if q is a singularity of $\iota_p(\gamma)$. But $\iota_p(\gamma)$ is an irreducible curve of degree at most 6, and so has at most ten singularities by [64, Chapter III, Theorem 4.4], which is a contradiction. So γ must be a circular cubic that is elliptic or acnodal. If γ is elliptic, then $I_p(\gamma)$ is either a bicircular quartic or a circular elliptic cubic. If γ is acnodal, then $\iota_p(\gamma)$ is either a bicircular quartic (if $p \notin \gamma$), a circular acnodal cubic (if p is a smooth point of γ), or a non-circular conic (if p is the singularity of γ). In the last case, the conic is an ellipse by Corollary 3.24.

We have encountered the following curves that P could mostly lie on: a line, a circle, an ellipse, a disjoint union of a line and a circle, a disjoint union of two circles, a circular cubic, or a bicircular quartic. All of these are subsets of bicircular quartics, which proves the lemma. □

We now prove Theorem 5.15. As explained in Chapter 4, a coset of a finite subgroup of an ellipse or a circular elliptic cubic both span at most $\frac{1}{2}n^2$ ordinary circles, and a double polygon spans at most $\frac{1}{4}n^2$ ordinary circles. It follows from Lemma 5.12 below that if we add and/or remove $O(K)$ points, then there will be at most $O(Kn^2)$ ordinary circles. Note that this is the circular analogue to Lemma 5.5, and is proved almost identically.

Lemma 5.12. *Let P be a set of n points in $\mathbb{R}^2$ spanning m ordinary circles. Let P' be a set that differs from P in at most K points. Then P' spans at most $s + O(Kn^2 + K^2n + K^3)$ ordinary circles.*

Proof. First note that if we add a point to any set of n points, we create at most $\binom{n}{2}$ ordinary circles. Secondly, since two circles intersect in at most two points, the number of 4-rich circles through a fixed point in a set of n points is at most $\frac{1}{3}\binom{n-1}{2}$, so by removing a point we create at most $\frac{1}{3}\binom{n-1}{2} < \binom{n}{2}$ ordinary circles. It follows that by adding and removing $O(K)$ points, we create at most

$$\binom{n}{2} + \binom{n+1}{2} + \cdots + \binom{n+K-1}{2} = O(Kn^2 + K^2n + K^3)$$

ordinary circles. □

Let P be a set of n points spanning at most Kn^2 ordinary circles. From the proof of Lemma 5.11 above, we see that P differs in at most $O(K)$ points from a line, a circle, an ellipse, the union of a line and a disjoint circle, the union of two disjoint circles, a circular cubic, or a bicircular quartic. Moreover, in the proof we saw that the circular cubic must be elliptic or acnodal, and that the bicircular quartic has the property that if we invert in a point on the curve, the resulting circular cubic is elliptic or acnodal.

Using inversions, we can reduce the number of types of curves that we need to analyse further.

- If P lies mostly on a line, then we are in Case (i) of Theorem 5.15, so we are done.
- If P lies mostly on a circle, then inverting in a point on the circle puts us in Case (i) again.
- If P lies mostly on an ellipse, then inverting in a point of the ellipse places P mostly on a circular acnodal cubic.
- If P lies mostly on a bicircular quartic, then inverting in any smooth point on the curve gives us a circular cubic. As mentioned above, this cubic is elliptic or acnodal.
- If P lies mostly on a line and a disjoint circle, then an inversion in a point not on the line or circle places P mostly on two disjoint circles.
- If P lies mostly on the disjoint union of two circles, we can apply an inversion that maps the two disjoint circles to two concentric circles [13, Theorem 1.7].

So, up to inversions, we need only consider the cases when P lies mostly on a circular elliptic or acnodal cubic, or on two concentric circles. We do this in Lemmas 5.13 and 5.14 below, which will complete the proof of Theorem 5.15.

To determine the structure of P, we again use the additive combinatorial Lemma 2.6. Lemmas 5.13 and 5.14 below can be viewed as circular analogues of Lemmas 5.7 and 5.6 respectively.

Lemma 5.13. *Let $K > 0$ and let n be sufficiently large depending on K. Suppose P is a set of n points in $\mathbb{R}^2$ spanning at most Kn^2 ordinary circles, and all but at most K points of P lie on a circular elliptic or acnodal cubic γ. Then P differs in at most $O(K)$ points from a coset $H \oplus x$ of a subgroup H of γ^*, the smooth points of γ, with $4x \in H \boxplus \omega$.*

Proof. Let $P' = P \cap \gamma^*$. Then $|P \triangle P'| = O(K)$, and by Lemma 5.12, P' spans at most $O(Kn^2)$ ordinary circles. If a, b, $c \in \gamma$ are distinct, then by Proposition 3.29, the circle through a, b, c meets γ again in the unique point $d = \omega \boxminus (a \boxplus b \boxplus c)$. This implies that $d \in P'$ for all but at most $O(Kn^2)$ triples a, b, $c \in P'$, or equivalently $a \boxplus b \boxplus c \in \omega \boxminus P'$. Applying Lemma 2.6 with $d = 3$, $A_1 = A_2 = A_3 = P'$, and $A_4 = \omega \boxminus P'$, we obtain a subgroup H of γ^* and a coset $H \boxplus x$ such that $|P \triangle (H \boxplus x)| = O(K)$ and $|(\omega \boxminus P') \triangle (H \boxplus 3x)| = O(K)$, which is equivalent to $|P \triangle (H \boxminus 3x \boxplus \omega)| = O(K)$. Thus we have $|(H \boxplus x) \triangle (H \boxminus 3x \boxplus \omega)| = O(K)$, which implies $4x \in H \boxplus \omega$. □

Lemma 5.14. *Let $K > 0$ and let n be sufficiently large depending on K. Suppose P is a set of n points in $\mathbb{R}^2$ spanning at most Kn^2 ordinary circles. Suppose all but at most K points of P lie on two concentric circles, and that P has $n/2 \pm O(K)$ points on each circle. Then, up to similarity, P differs in at most $O(K)$ points from an 'aligned' or 'offset' double polygon.*

Proof. By scaling and rotating, we can assume that P lies mostly on the two concentric circles $\sigma_1 = \{e^{2\pi it} : t \in [0,1)\}$ and $\sigma_2 = \{re^{2\pi it} : t \in [0,1)\}$, $r > 1$, which we gave a group structure in Proposition 3.31.

Let $P_1 = P \cap \sigma_1$ and $P_2 = P \cap \sigma_2$. Then $|P \triangle (P_1 \cup P_2)| = O(K)$, and by Lemma 5.12, $P_1 \cup P_2$ spans at most $O(Kn^2)$ ordinary circles. If $a, b \in \sigma_1$ and $c \in \sigma_2$ with $a \neq b$, then by Proposition 3.31, the circle or line through a, b, c meets $\sigma_1 \cup \sigma_2$ again in the unique point $d = \ominus(a \oplus b \oplus c)$. This implies $d \in P_2$ for all but at most $O(Kn^2)$ triples (a, b, c) with $a, b \in P_1$ and $c \in P_2$. Applying Lemma 2.6 with $d = 3$, $A_1 = A_2 = P_1$, $A_3 = P_2$, and $A_4 = \ominus P_2$, we get cosets $H \oplus x$ and $H \oplus y$ of a subgroup H of $\sigma_1 \cup \sigma_2$ such that $|P_1 \triangle (H \oplus x)|, |P_2 \triangle (H \oplus y)| = O(K)$ and $2x \oplus 2y \in H$, where

$x \in \sigma_1$ and $y \in \sigma_2$. It follows that H is a subgroup of σ_1, hence H is a cyclic group of order $m = n/2 \pm O(K)$, and $H \oplus x$ and $H \oplus y$ are the vertex sets of regular m-gons inscribed in σ_1 and σ_2, respectively, either 'aligned' or 'offset' depending on whether $x \oplus y \in H$ or not. □

As mentioned in Section 1.2.1, we can take $n \geqslant \exp\exp(CK^C)$ for some sufficiently large absolute constant $C > 0$. This bound is inherited from Green and Tao's structure theorem for sets spanning few ordinary lines (Theorem 2.1).

Theorem 5.15. *Let $K > 0$ and let n be sufficiently large depending on K. If a set P of n points in $\mathbb{R}^2$ spans at most Kn^2 ordinary circles, then up to inversions and similarities, P differs in at most $O(K)$ points from a configuration of one of the following types:*

(*i*) *a subset of a line;*

(*ii*) *a coset $H \boxplus x$ of a subgroup of an ellipse, for some x such that $4x \in H$;*

(*iii*) *a coset $H \boxplus x$ of a subgroup H of a circular elliptic cubic curve, for some x such that $4x \in H \boxplus \alpha \boxplus \beta$;*

(*iv*) *a double polygon that is 'aligned' or 'offset'.*

Conversely, every set of these types spans at most $C'Kn^2$ ordinary circles for some absolute constant $C' > 0$.

Proof. Lemmas 5.11, 5.13, and 5.14 prove the forward statement. It just remains to remark that if P differs in $O(K)$ points from a coset on a circular acnodal cubic, then we apply inversion in its singularity. By Corollary 3.24, we obtain that P differs in $O(K)$ points from a coset $H \boxplus x$ of a finite subgroup H of an ellipse, where $4x = o$. Thus, x is a point of the ellipse with eccentric angle a multiple of $\pi/2$. After a rotation, we can assume that $x = o$, which is Case (*ii*).

The converse statement follows from Lemma 5.12 applied to a coset of a subgroup of an ellipse or a circular elliptic cubic (see Constructions 4.15

and 4.14), or an 'aligned' or 'offset' double polygon (see Constructions 4.5 and 4.6). □

We now prove the stronger Theorem 1.11, restated below. As mentioned at the beginning of this section, the following theorem is a consequence of Theorem 1.9, our structure theorem for sets spanning few ordinary planes, and stereographic projection. Note that in contrast with Theorem 5.15 above, we only need $n \geqslant CK^8$ for some sufficiently large absolute constant $C > 0$.

Theorem 1.11 (Ordinary circles)**.** *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 $\mathbb{R}^2$. If P spans at most Kn^2 ordinary circles, then up to inversions and similarities of the plane, P differs in at most $O(K)$ points from a configuration of one of the following types:*

(*i*) *a subset of a line;*

(*ii*) *a coset $H \oplus x$ of a subgroup H of an ellipse, for some x such that $4x \in H$;*

(*iii*) *a coset $H \oplus x$ of a subgroup H of a circular elliptic cubic curve, for some x such that $4x \in H$;*

(*iv*) *a double polygon that is 'aligned' or 'offset'.*

Conversely, every set of these types spans at most $C'Kn^2$ ordinary circles for some absolute constant $C' > 0$.

Proof. Projecting P stereographically, we obtain a set $P' := \pi^{-1}(P) \subset \overline{\mathbb{S}^2} \subset \mathbb{RP}^3$ of n points with no three collinear, spanning at most Kn^2 ordinary planes. We can thus apply Theorem 1.9 to get that P' differs in at most $O(K)$ points from

(1) a subset of a plane, or

(2) a subset of two planar sections of a quadric, which after a projective transformation is a prism or an antiprism, or

(3) a coset $H \oplus x$ of a subgroup H of an elliptic space quartic or the smooth points of an acnodal space quartic, for some x such that $4x \in H$.

Since P' is contained in a sphere, by Bézout's theorem (Theorem 2.9), the two conics in Case (2) and the space quartic in Case (3) are also contained in the sphere. In particular, the two conics are both circles and the space quartic is bounded.

If we are in Case (1), then projecting back down to the plane, we get that P differs in at most $O(K)$ points from a subset of a circle or a line, which after an inversion we can assume to be a line.

If we are in Case (2), without loss of generality (applying an inversion to P if necessary), we can assume P' differs in at most $O(K)$ points from a prism or an antiprism contained in the intersection of the circular cylinder defined by $\frac{1}{2}x_0^2 = x_1^2 + x_2^2$ and $\overline{\mathbb{S}^2}$. Then, since the north pole is not one of two points that project the prism or antiprism onto a single conic, by Proposition 2.14, P differs in at most $O(K)$ points from a double polygon, which is 'aligned' or 'offset' depending on whether it was a prism or an antiprism respectively.

If we are in Case (3), then all but at most $O(K)$ points of P' lie on a space quartic $\delta' \subset \mathbb{R}^3$, which is either elliptic or acnodal. Projecting (stereographically) back to the plane, we get that all but at most $O(K)$ points of P lie on a curve $\delta \subset \mathbb{R}^2$. By Proposition 3.22, we get one of the following cases, depending on the multiplicity of the north pole N on δ':

(a) N is a double point of δ', which means δ' is acnodal, and thus δ is an ellipse;

(b) N is a smooth point of δ', in which case δ is a circular elliptic or acnodal cubic;

(c) N does not lie on δ', in which case δ is a bicircular quartic.

Note that the group structure mentioned in the statement of the theorem is inherited from that in Theorem 1.9, and is detailed in Propositions 3.29 and 3.30. By Corollary 3.23, the curve from (c) can be inverted to a curve

as in (b), and by Corollary 3.26, the rational curve from (b) can be inverted to an ellipse as in (a).

The converse statement follows from Lemma 5.12 applied to a coset of a subgroup of an ellipse or a circular elliptic curve (see Constructions 4.15 and 4.14), or an 'aligned' or 'offset' double polygon (see Constructions 4.5 and 4.6). □

As mentioned in Section 3.3, the groups obtained in the corresponding cases of Theorems 5.15 and 1.11 are isomorphic by Proposition 3.3. Thus Theorem 5.15 is a strict strengthening of Theorem 5.15.

5.4 Ordinary hyperspheres

We prove Theorem 1.12, our structure theorem for sets spanning few ordinary hyperspheres, in this section.

Since ordinary hyperspheres spanned by $P \subset \mathbb{R}^d$ are in one-to-one correspondence with ordinary hyperplanes in $\pi^{-1}(P) \subset \mathbb{R}^{d+1}$, Theorem 1.12, restated below, is a simple consequence of Theorem 1.10, our structure theorem for sets spanning few ordinary hyperplanes, combined with the results from Section 3.3.

Theorem 1.12 (Ordinary hyperspheres)**.** *Let $d \geqslant 3$, $K > 0$, and suppose $n > C \max\{(dK)^8, d^3 2^d K\}$ for some sufficiently large absolute constant $C > 0$. Let P be a set of n points in $\mathbb{R}^d$ where no $d+1$ points lie on a $(d-2)$-sphere or a $(d-2)$-flat. Suppose P spans at most $K\binom{n}{d}$ ordinary hyperspheres.*

If d is odd, then all but at most $O(d2^d K)$ points of P lie on a hypersphere or a hyperplane.

If $d = 2k$ is even, then up to an inversion, 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 a bounded $(k-1)$-spherical rational normal curve of degree d, for some x such that $(d+2)x \in H$;*

(*iii*) *a coset $H \oplus x$ of a subgroup H of a k-spherical elliptic normal curve of degree $d+1$, for some x such that $(d+2)x \in H$.*

Conversely, every set of these types spans at most $C' 2^d K \binom{n}{d}$ ordinary hyperspheres for some absolute constant $C' > 0$.

Proof. Projecting P stereographically, we obtain a set $P' := \pi^{-1}(P) \subset \overline{\mathbb{S}^d} \subset \mathbb{RP}^{d+1}$ of n points, no $d+1$ of which lie on a hyperplane, spanning at most $K\binom{n}{d}$ ordinary hyperplanes. We can thus apply Theorem 1.10 to get that P' differs in at most $O(d2^d K)$ points from

(1) a subset of a hyperplane, or

(2) 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 $d+2$, for some x such that $(d+2)x \in H$.

In the latter case, since P' is contained in a hypersphere, by Bézout's theorem (Theorem 2.9), the degree $d+2$ curve is also contained in the hypersphere. In particular, it is bounded.

Suppose d is odd (so that $d+2$ is odd). Then Case (2) does not occur, as Lemma 3.5 implies an odd degree curve is always unbounded. Thus projecting Case (1) back down to $\mathbb{R}^d$, we get that P differs in at most $O(d2^d K)$ points from a subset of a hypersphere or a hyperplane.

Now suppose d is even. If we are in Case (1), then we are in the same situation as the odd case. So assume we are in Case (2), and all but at most $O(d2^d K)$ points of P' lie on a degree $d+2$ curve $\delta' \subset \mathbb{R}^{d+1}$, which is either elliptic or acnodal. Projecting (stereographically) back to $\mathbb{R}^d$, we get that all but at most $O(d2^d K)$ points of P lie on a curve $\delta \subset \mathbb{R}^d$. By Proposition 3.22, we get one of the following cases, depending on the multiplicity of the north pole N on δ':

(*a*) N is a double point of δ', which means δ' is acnodal, and thus δ is a bounded $(k-1)$-spherical rational normal curve of degree d;

(*b*) N is a smooth point of δ', in which case δ is a k-spherical elliptic normal curve or rational acnodal curve of degree $d+1$;

(*c*) N does not lie on δ', in which case δ is a $(k+1)$-spherical curve of degree $d+2$.

Note that the group structure mentioned in the statement of the theorem is inherited from that in Theorem 1.10, and is detailed in Proposition 3.27. By Corollary 3.25, the curve from (*c*) can be inverted to a curve as in (*b*), and by Corollary 3.26, the rational curve from (*b*) can be inverted to a curve as in (*a*).

Finally, the converse statement follows directly from stereographic projection (as at the beginning of this proof) and Theorem 1.10. □

Chapter 6

Extremal theorems

In this chapter, we prove our extremal Theorems 1.13 to 1.22. We restate these theorems before their proofs.

6.1 Planes

We prove Theorems 1.13, 1.14, and 1.15 in this section.

Suppose P is a non-coplanar set of n points in $\mathbb{RP}^3$ with no three collinear spanning fewer than $\frac{1}{2}n^2$ ordinary planes. Applying Theorem 1.9, our structure theorem for sets spanning few ordinary planes, we can conclude that, up to projective transformations, P differs in $O(1)$ points from either a subset of a plane, a coset of a subgroup of an elliptic space quartic or the smooth points of an acnodal space quartic, or a prism or an antiprism.

The first type of set is very easy to handle, and spans at least $\binom{n-1}{2} = \frac{1}{2}n^2 - O(n)$ ordinary planes by Lemma 4.1.

Cosets on space quartics are also relatively easy to handle. We again obtain a lower bound on the number of ordinary planes.

Lemma 6.1. *Let δ be an elliptic or acnodal space quartic. Suppose $P \subset \mathbb{RP}^3$ differs in K points from a coset $H \oplus x$ of a subgroup H of δ^*, the smooth points of δ, where $|H| = n \pm O(K)$ and $4x \in H$. Then P spans at least $\frac{1}{2}n^2 - O(Kn)$ ordinary planes.*

Proof. We know from Constructions 4.14 and 4.15 that $H \oplus x$ spans $\frac{1}{2}n^2 - O(n)$ ordinary planes, all of which are tangent to δ. We show that adding or removing K points destroys no more than $O(Kn)$ of these ordinary planes, so that the resulting set P still spans at least $\frac{1}{2}n^2 - O(Kn)$ ordinary planes.

Suppose we add a point $q \notin H \oplus x$. For $p \in H \oplus x$, at most one plane tangent to δ at p can pass through q. Thus, adding q destroys at most n ordinary planes. Now suppose we remove a point $p \in H \oplus x$. Since ordinary planes of $H \oplus x$ correspond to solutions of $2p \oplus q \oplus r = 0$ or $p \oplus 2q \oplus r = 0$ by Propositions 3.7 and 3.18, there are at most $O(n)$ solutions for a fixed p. Thus removing p destroys at most $O(n)$ ordinary planes.

Repeating K times, we see that adding or removing K points to or from $H \oplus x$ destroys at most $O(Kn)$ ordinary planes out of the $\frac{1}{2}n^2 - O(n)$ spanned by $H \oplus x$. This proves that P spans at least $\frac{1}{2}n^2 - O(Kn)$ ordinary planes. □

So there exists an absolute constant $C > 0$ such that a non-coplanar set of n points with no three collinear, spanning at most $\frac{1}{2}n^2 - Cn$ ordinary planes, differs in $O(1)$ points from Case (ii) of Theorem 1.9, our structure theorem for sets spanning few ordinary planes. This case, where P is close to a prism or an antiprism, requires a more careful analysis of the effect of adding and/or removing points.

We first need the following simple application of Theorem 2.25.

Proposition 6.2. *If $P \subset \mathbb{R}^2$ is a set of n points contained in two circles, then the number of lines with at least three points of P is at most $O(n^{11/6})$.*

Proof. Denote the two circles by σ_1 and σ_2. Let $\gamma_1 = \sigma_1$ and $\gamma_2 = \gamma_3 = \sigma_2$, and set $S_i = P \cap \gamma_i$ for $i = 1, 2, 3$. Every line with at least one point of S_1 and two points of $S_2 = S_3$ corresponds to a collinear triple in $S_1 \times S_2 \times S_3$. Since the union of two circles is not a line or a cubic, we can apply Theorem 2.25 to get the bound $O(n^{11/6})$ for the number of collinear triples in P with one point in σ_1 and two points in σ_2. Similarly, the number of collinear triples in P with one point in σ_2 and two points in σ_1 is also $O(n^{11/6})$. Since a line intersects $\sigma_1 \cup \sigma_2$ in at most four points, we also obtain the bound $O(n^{11/6})$

for the number of lines with at least three points. □

Lemma 6.3. *Let S be a prism or an antiprism with $|S| = 2m$. Let $P = (S \setminus A) \cup B$ be a set of n points with no three collinear, where A is a subset of S with $a = O(1)$ points and B is a set disjoint from S with $b = O(1)$ points. Then P spans at least $\frac{1}{8}(2 + a + 4b)n^2 - O(n^{11/6})$ ordinary planes.*

Proof. By a projective transformation, suppose S is given by

$$\left\{\left(\cos\left(\frac{2k\pi}{m}\right), \sin\left(\frac{2k\pi}{m}\right), \pm 1\right) : k \in [m]\right\},$$

if S is a prism, or

$$\left\{\left(\cos\left(\frac{2k\pi}{m}\right), \sin\left(\frac{2k\pi}{m}\right), 1\right) : k \in [m]\right\}$$
$$\cup \left\{\left(\cos\left(\frac{(2k+1)\pi}{m}\right), \sin\left(\frac{(2k+1)\pi}{m}\right), -1\right) : k \in [m]\right\},$$

if S is an antiprism.

We know from Constructions 4.5 and 4.6 that S spans $\frac{1}{4}n^2 - O(n)$ ordinary planes.

Consider first the number of ordinary planes spanned by $S \setminus A$. As we saw in Construction 4.7, removing a point $p \in S$ destroys at most $3m/2$ ordinary planes spanned by S, and adds $\frac{1}{2}m^2 - O(m) = \frac{1}{8}n^2 - O(n)$ ordinary planes. Noting that there are at most m 4-rich planes spanned by S that go through any two given points of A, we thus have by inclusion-exclusion that $S \setminus A$ spans at least $(\frac{1}{4} + \frac{a}{8})n^2 - O(n)$ ordinary planes.

Now consider adding $q \in B$ to S. For any pair of points from $S \setminus A$, adding $q \in B$ creates a new ordinary plane, unless the plane through the pair and q contains three or four points of $S \setminus A$. We already saw that the number of ordinary planes hitting a fixed point is $O(n)$, so it remains to bound the number of 4-rich planes of S that hit q. If q lies on one of the circumscribed circles of the m-gons of S, then no 4-rich planes hit q, so we can assume that q does not. Projecting from q reduces the problem to bounding the number of 4-rich lines spanned by a subset of two conics, unless q is one of two points projecting S onto a single conic by Proposition 2.14. If q is not one of those two points, by Proposition 6.2, this number is bounded by

$O(n^{11/6})$, so q lies on at most $O(n^{11/6})$ of the 4-rich planes spanned by S. If q projects S onto a single conic, then q is either the origin or the point at infinity corresponding to the x_3-axis. In the prior case, q does not lie on any 4-rich planes spanned by S if m is odd and S is a prism or if m is even and S is an antiprism, and adding q would result in three collinear points if m is odd and S is an antiprism or if m is even and S is a prism. In the latter case, q does not lie on any 4-rich planes spanned by S if S is an antiprism, and adding q would result in three collinear points if S is a prism. Adding q to S thus creates at least $\binom{n}{2} - O(n^{11/6})$ ordinary planes. Note that each $p \in A$ that was removed destroys at most n of these planes.

Adding q to $S \setminus A$ also destroys at most $O(n)$ ordinary planes, since for each $p \in S$ there is only one plane tangent at p and going through q, and for each $p \in A$, at most m ordinary planes spanned by $S \setminus A$ go through p. Finally, since there are at most $2m$ planes through two points of B that also go through two points of $S \setminus A$, $P = (S \setminus A) \cup B$ spans at least $(\frac{1}{4} + \frac{a}{8} + \frac{b}{2})n^2 - O(n^{11/6})$ ordinary planes. □

Theorems 1.13 and 1.14, restated below, then follow easily from the lemmas above.

Theorem 1.13 (Ordinary planes)**.**

(*i*) *If n is sufficiently large, the minimum number of ordinary planes spanned by a non-coplanar set of n points in $\mathbb{RP}^3$ with no three collinear is equal to*

$$\begin{cases} \frac{1}{4}n^2 - n & \text{if } n \equiv 0 \pmod 4, \\ \frac{3}{8}n^2 - n + \frac{5}{8} & \text{if } n \equiv 1 \pmod 4, \\ \frac{1}{4}n^2 - \frac{1}{2}n & \text{if } n \equiv 2 \pmod 4, \\ \frac{3}{8}n^2 - \frac{3}{2}n + \frac{17}{8} & \text{if } n \equiv 3 \pmod 4. \end{cases}$$

(*ii*) *Let $C > 0$ be a sufficiently large absolute constant. If a non-coplanar set P of n points in $\mathbb{RP}^3$ with no three collinear spans fewer than $\frac{1}{2}n^2 - Cn$ ordinary planes, then P is contained in a prism or an antiprism.*

Proof. Suppose P is a set of n points in $\mathbb{RP}^3$ with no three collinear spanning

fewer than $\frac{1}{2}n^2 - Cn$ ordinary planes, where $C > 0$ is a sufficiently large absolute constant. Without loss of generality, n is also sufficiently large. By Lemmas 4.1 and 6.1, we need only consider the case where P differs by $O(1)$ points from a prism or antiprism. In the notation of Lemma 6.3, we have $P = (S \setminus A) \cup B$ and $\frac{1}{8}(2 + a + 4b) < \frac{1}{2}$, which implies that $a \leqslant 1$ and $b = 0$. So P is either equal to S, or is obtained from S by removing one point, which are exactly the cases in Constructions 4.5, 4.6, and 4.7. In particular, the minimum number of ordinary planes occurs in Construction 4.5 when $n \equiv 0 \pmod 4$, in Construction 4.7 when $n \equiv 1, 3 \pmod 4$, and in Constructions 4.5 and 4.6 when $n \equiv 2 \pmod 4$. □

Theorem 1.14 (4-rich planes)**.**

(*i*) *If n is sufficiently large, the maximum number of 4-rich planes spanned by a set of n points in $\mathbb{RP}^3$ with no three collinear is equal to*

$$\begin{cases} \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{5}{6}n & \text{if } n \equiv 0 \pmod 8, \\ \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{11}{24}n - \frac{1}{4} & \text{if } n \equiv 1, 3, 5, 7 \pmod 8, \\ \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{7}{12}n - \frac{1}{2} & \text{if } n \equiv 2, 6 \pmod 8, \\ \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{5}{6}n - 1 & \text{if } n \equiv 4 \pmod 8. \end{cases}$$

(*ii*) *Let $C > 0$ be a sufficiently large absolute constant. If a set P of n points in $\mathbb{RP}^3$ with no three collinear spans more than $\frac{1}{24}n^3 - \frac{7}{24}n^2 + Cn$ 4-rich planes, then P lies on an elliptic or acnodal space quartic curve.*

Proof. Let P be a set of n points in $\mathbb{RP}^3$ with no three collinear spanning at least $\frac{1}{24}n^3 - \frac{7}{24}n^2 + O(n)$ 4-rich planes. Let t_i denote the number of i-rich planes ($i \geqslant 3$). By counting unordered triples of points, we have

$$\binom{n}{3} = \sum_{i \geqslant 3} \binom{i}{3} t_i \geqslant t_3 + 4t_4,$$

hence

$$\frac{1}{6}n^3 - O(n^2) \geqslant t_3 + 4\left(\frac{1}{24}n^3 - O(n^2)\right)$$

and $t_3 = O(n^2)$, so we can apply Theorem 1.9. We next consider each of the cases of that theorem in turn.

If all except $O(1)$ points of P lie on a plane, it is easy to see that P spans only $O(n^2)$ 4-rich planes, contrary to assumption.

If all except $O(1)$ are vertices of a prism or antiprism, then we know from Constructions 4.5, 4.6, and 4.7 that P spans at most $\frac{1}{32}n^3 + O(n^2)$ 4-rich planes, again contrary to assumption.

Suppose next that $P = ((H \oplus x) \setminus A) \cup B$, where H is a finite subgroup of order $m = n \pm O(1)$ of an elliptic or acnodal space quartic, A is a subset of $H \oplus x$ with $a = O(1)$ points, and B is a set disjoint from $H \oplus x$ with $b = O(1)$ points. Then $n = m - a + b$. The number of 4-rich planes spanned by $H \oplus x$ is $\frac{1}{24}m^3 - \frac{1}{4}m^2 + O(m)$. We next determine an upper bound for the number of 4-rich planes in P.

For each $p \in A$, let Π_p be the set of 4-rich planes spanned by $H \oplus x$ that pass through p. Then $|\Pi_p| = \frac{1}{6}m^2 - O(m)$ and $|\Pi_p \cap \Pi_q| = O(m)$ for distinct $p, q \in A$. By inclusion-exclusion, we destroy at least $|\bigcup_{p\in A} \Pi_p| \geqslant \frac{1}{6}am^2 - O(m)$ 4-rich planes by removing A, and we still have at most $\frac{1}{24}m^3 - \frac{1}{4}m^2 - \frac{1}{6}am^2 + O(m)$ 4-rich planes in $(H \oplus x) \setminus A$.

For each $p \in B$, the number of ordinary planes spanned by $H \oplus x$ passing through p is at most $O(m)$. This is because each such plane is tangent to the space quartic at one of the points of $H \oplus x$, and there is only one plane through p and tangent at a given point of $H \oplus x$. Also, for each pair of distinct $p, q \in B$, there are at most $O(m)$ planes through p and q and two points of $H \oplus x$; and for any three $p, q, r \in B$ there are at most $O(1)$ planes through p, q, r and one point of $H \oplus x$. Therefore, again by inclusion-exclusion, by adding B we gain at most $O(m)$ 4-rich planes.

It follows that the number of 4-rich planes spanned by P is

$$t_4 \leqslant \frac{1}{24}m^3 - \frac{1}{4}m^2 - \frac{1}{6}am^2 + O(m) = \frac{n^3 - (a + 3b + 6)n^2 + O(n)}{24}.$$

Since we assumed that

$$t_4 \geqslant \frac{n^3 - 7n^2 + O(n)}{24},$$

we obtain $a + 3b < 1$. Therefore, $a = b = 0$ and $P = H \oplus x$. The maximum number of 4-rich planes spanned by a coset has been determined in Constructions 4.14 and 4.15. □

We now turn to coplanar quadruples. As mentioned in [50], certain space quartic curves such as elliptic normal curves contain sets of n points spanning $\Theta(n^3)$ coplanar quadruples. We use Theorem 2.26, a special case of Raz, Sharir, and De Zeeuw's 4-dimensional generalisation of the Elekes-Szabó theorem [50], to prove Theorem 1.15, restated below.

Theorem 1.15 (Coplanar quadruples)**.** *Let δ be a rational space quartic curve in $\mathbb{CP}^3$. If δ is singular, then there exist n points on δ that span $\Theta(n^3)$ coplanar quadruples. If δ is smooth, then any n points on δ span $O(n^{8/3})$ coplanar quadruples.*

Proof. We first show that if an n-point set P on a rational space quartic δ_p in $\mathbb{CP}^3$ spans more than $O(n^{8/3})$ coplanar quadruples, then δ_p is of the first species, hence singular by Lemma 3.16 and Corollary 3.14. We work in the affine charts $y = 1$ in $\mathbb{CP}^1$ and $p_0 = 1$ in $\mathbb{FP}^4$.

Lemma 3.11 says four points parametrised by $[t_1, 1], [t_2, 1], [t_3, 1], [t_4, 1]$ are coplanar if and only if $F_p(t_1, 1, t_2, 1, t_3, 1, t_4, 1) = 0$. It is clear that F_p is not independent of any t_i (otherwise δ_p would be planar). Since P does not span $O(n^{8/3})$ coplanar quadruples, Theorem 2.26 gives the existence of injective analytic $\varphi_1, \varphi_2, \varphi_3, \varphi_4$ such that $F_p = 0$ if and only if $\varphi_1(t_1) + \varphi_2(t_2) + \varphi_3(t_3) + \varphi_4(t_4) = 0$. In particular, on the hypersurface $F_p = 0$, we can express $t_4 = t_4(t_1, t_2, t_3)$ as a function of t_1, t_2, t_3:

$$t_4(t_1, t_2, t_3) = -\frac{p_1 t_1 t_2 t_3 + p_2(t_1 t_2 + t_1 t_3 + t_2 t_3) + p_3(t_1 + t_2 + t_3) + p_4}{t_1 t_2 t_3 + p_1(t_1 t_2 + t_1 t_3 + t_2 t_3) + p_2(t_1 + t_2 + t_3) + p_3}. \tag{6.1}$$

We thus have for all $(t_1, t_2, t_3) \in U_1 \times U_2 \times U_3$ that

$$\varphi_1(t_1) + \varphi_2(t_2) + \varphi_3(t_3) + \varphi_4(t_4(t_1, t_2, t_3)) = 0.$$

Partial differentiation with respect to t_i for $i = 2, 3$ gives

$$\varphi_i'(t_i) + \varphi_4'(t_4)\frac{\partial t_4}{\partial t_i} = 0,$$

and so the quotient $(\partial t_4/\partial t_2) \,/\, (\partial t_4/\partial t_3)$ is independent of t_1. The numerator of the partial derivative of this quotient with respect to t_1 is thus identically zero. If we substitute (6.1) into

$$\frac{\partial}{\partial t_1}\left(\frac{\partial t_4}{\partial t_2}\Big/\frac{\partial t_4}{\partial t_3}\right) = 0,$$

we obtain (with the help of a computer algebra system such as SageMath)

$$\frac{(p_2p_4 - p_3^2 - p_1^2p_4 + 2p_1p_2p_3 - p_2^3)F(t_1, t_1, t_2, t_3)(t_3 - t_2)}{h(t_1, t_2)^2} = 0,$$

where

$$\begin{aligned} h(t_1, t_2) = (p_1^2 - p_2)t_1^2t_2^2 + (p_1p_2 - p_3)t_1t_2(t_1 + t_2) + (p_2^2 - p_1p_3)(t_1^2 + t_2^2) \\ + (p_2^2 - p_4)t_1t_2 + (p_2p_3 - p_1p_4)(t_1 + t_2) + p_3^2 - p_2p_4. \end{aligned}$$

Since t_1, t_2, t_3 are arbitrary in $(U_1 \times U_2 \times U_3) \setminus (Z_{\mathbb{C}}(h) \times \mathbb{C})$, we obtain that the catalecticant $p_2p_4 - p_3^2 - p_1^2p_4 + 2p_1p_2p_3 - p_2^3$ vanishes. By Lemma 3.16, the rational space quartic δ_p is thus of the first species, as desired.

For the converse, suppose that δ_p is singular, hence of the first species (again by Corollary 3.14 and Lemma 3.16). Then, as is well-known (and explicitly demonstrated in the proof of Proposition 3.18), the smooth points δ_p^* carry a group structure such that four points are coplanar if and only if their sum in the group is the identity. If δ_p is nodal, then the group is isomorphic to the non-zero complex numbers under multiplication $(\mathbb{C}^*, \cdot)$. If δ_p is cuspidal, then the group is isomorphic to the complex numbers under addition $(\mathbb{C}, +)$. In both groups it is trivial to find n elements such that there are $\Theta(n^3)$ quadruples of distinct elements that sum to 0. In the multiplicative case, we can take the n-th roots of unity, and in the additive case, we can take the n integers closest to 0. □

For a rational space quartic $\delta \in \mathbb{CP}^3$ that is singular, the proof of Proposition 3.18 gives the φ_i's in Theorem 2.26 explicitly. Recall that δ has a unique singularity that is either a cusp or a node. For convenience, let us identify $\mathbb{CP}^1$ with the affine line $\mathbb{C}$ together with a point ∞ at infinity. If δ has a cusp, then there exists a parametrisation $\varphi\colon \mathbb{CP}^1 \to \delta$ such that $\varphi(\infty)$ is the cusp of δ, and any four points $\varphi(t_1), \varphi(t_2), \varphi(t_3), \varphi(t_4)$ on $\delta \setminus \{\varphi(\infty)\}$ are coplanar if and only if $t_1 + t_2 + t_3 + t_4 = 0$. If δ has a node, then there exists a parametrisation $\varphi\colon \mathbb{CP}^1 \to \delta$ such that $\varphi(0) = \varphi(\infty)$ is the node of δ, and any four points $\varphi(t_1), \varphi(t_2), \varphi(t_3), \varphi(t_4)$ on $\delta \setminus \{\varphi(0)\}$ are coplanar if and only if $t_1t_2t_3t_4 = 1$.

6.2 Hyperplanes

We prove Theorems 1.16 and 1.17 in this section. It turns out that minimising the number of ordinary hyperplanes spanned by a set is equivalent to maximising the number of $(d+1)$-rich planes, thus we can apply Theorem 1.10, our structure theorem for sets spanning few ordinary hyperplanes, 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 at least $\binom{n-1}{d-1}$ ordinary hyperplanes by Lemma 4.1.

The second case needs more work. Let δ^* be an elliptic normal curve or the smooth points of a rational acnodal curve in $\mathbb{RP}^d$. By Lemma 4.9, there always exists a coset of δ^* that spans at most $\binom{n-1}{d-1}$ ordinary hyperplanes. 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 6.4, while Lemma 6.5 covers the case where the point is off the curve. We then obtain a more general lower bound in Lemma 6.6.

Lemma 6.4. *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 $p_1, \ldots, p_{d-1} \in H \oplus x$, and note that for the hyperplane through $p, p_1, \ldots, p_{d-1}$ to not contain any other point of $H \oplus x$, we must have $\ominus(p \oplus p_1 \oplus \cdots \oplus p_{d-1}) \notin H \oplus x$ by Propositions 3.7 and 3.18. Suppose otherwise. Then we have $\ominus p \ominus (d-1)x \in H \oplus x$, in which case we also have $p \oplus (d+1)x \in H \oplus x$. But this contradicts $p \notin H \oplus x$ as $(d+1)x \in H$.

Next we show that if $\{p_1, \ldots, p_{d-1}\} \neq \{p'_1, \ldots, p'_{d-1}\}$, where $p'_1, \ldots, p'_{d-1} \in H \oplus x$, then they 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. □

Lemma 6.5. *Let δ be an elliptic normal curve or a rational acnodal curve in $\mathbb{RP}^d$, $d \geqslant 3$, and let δ^* be its set of smooth points. Let $K > 0$, and suppose $H \oplus x$ is a coset of a finite subgroup of δ^* of order n, where $n \geqslant Cd^2 2^d d! K$ for some sufficiently large absolute constant $C > 0$. Let $p \in \mathbb{RP}^d \setminus \delta^*$ be such that p lies on at most $K 2^d \binom{n}{d-3}$ $(d-2)$-flats through exactly $d-1$ points of $H \oplus x$. Then there are at least $\frac{c}{d2^d}\binom{n}{d-1}$ hyperplanes through p that meet $H \oplus x$ in exactly $d-1$ points, for some sufficiently small absolute constant $c > 0$.*

Proof. We first consider the case $d = 3$. 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 3 in $\mathbb{RP}^2$ (otherwise its degree would be at most 1, but it has to have degree at least 2 because it is non-degenerate). 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 will be the single point in $\overline{\pi_q(\delta \setminus \{q\})} \setminus \pi_q(\delta \setminus \{q\})$.) The cubic curve $\pi_q(\delta)$ is either elliptic or rational and acnodal, hence it has a group operation $\boxplus$ such that three points are collinear in $\mathbb{RP}^2$ if and only if they sum to the identity.

Observe that any three points $\pi_q(p_1), \pi_q(p_2), \pi_q(p_3) \in \pi_q(\delta^*)$ lie on a line in $\mathbb{RP}^2$ if and only if $p_1 \oplus p_2 \oplus p_2 \oplus q = 0$. By Proposition 3.3 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.

If $\pi_q(p) \notin \pi_q(\delta^*)$, then there are at least $n/1000$ lines in $\mathbb{RP}^2$ through $\pi_q(p)$ and exactly one point of $H' \boxplus x'$ by Lemma 2.8. At most one of these lines go through $\pi_q(q)$, and thus there are at least $n/1000 - 1$ planes in $\mathbb{RP}^3$ that pass through p and exactly two points of $H \oplus x$.

If $\pi_q(p) \in \pi_q(\delta^*) \setminus (H' \boxplus x')$, then there are at least n lines in $\mathbb{RP}^2$ through $\pi_q(p)$ and exactly one point of $H' \boxplus x'$ by Lemma 6.4. Again, at most one of these lines go through $\pi_q(q)$, and thus there are at least $n-1$ planes in $\mathbb{RP}^3$ that pass through p and exactly two points of $H \oplus x$.

Since p lies on at most $8K$ lines through exactly two points of $H \oplus x$, there are at most $16K$ points $q \in H \oplus x$ for which $\pi_q(p) \in H' \boxplus x'$. Therefore, the total number of planes through p and exactly two points of $H \oplus x$ is at least

$$\frac{1}{2}(n-16K)\left(\frac{n}{1000}-1\right) \geqslant c_1\left(1-\frac{c_2K}{n}\right)\binom{n}{2},$$

where c_1, c_2 are some absolute constants.

Next, we use induction on d to show that for $n \geqslant C' \prod_{i=4}^{d} \frac{i-1}{i-3} 2^d d! K$ where $C' > 0$ is a sufficiently large absolute constant, there are at least

$$c' \prod_{i=4}^{d} \frac{i-1}{i} 2^{-d}\left(1-\frac{1}{n}\prod_{i=4}^{d}\frac{i-1}{i-3}2^d d!K\right)\binom{n}{d-1} =: f(n,d,k)\binom{n}{d-1}$$

hyperplanes through p and exactly $d-1$ points of $H \oplus x$ for some sufficiently small absolute constant $c' > 0$. Note that $n \geqslant C' \prod_{i=4}^{d} \frac{i-1}{i-3} 2^d d! K$ implies $f(n,d,K) \geqslant \frac{3c'}{d2^d}(1-\frac{1}{C'}) \geqslant \frac{c}{d2^d}$ for $c > 0$ a sufficiently small absolute constant.

Assume $d \geqslant 4$, and assume the above statement holds for $d-1$. As in the $d=3$ case, if $q \in H \oplus x$, then $\pi_q(\delta)$ is a degree d curve in $\mathbb{RP}^{d-1}$ that is either elliptic or rational and acnodal, with 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. Again as in the $d=3$ case, it follows from Proposition 3.3 that $\pi_q(H \oplus x) = H' \boxplus x'$ for some subgroup H' of $(\pi_q(\delta^*), \boxplus)$ of order n.

We know that p lies on at most $K 2^d \binom{n}{d-1}$ $(d-2)$-flats containing exactly $d-1$ points of $H \oplus x$. Thus, through at least $(1-\frac{1}{d})n$ points $q \in H \oplus x$, there are at most $\left(\frac{d-1}{d-3}2dK\right) 2^{d-1}\binom{n}{d-4}$ $(d-2)$-flats through p, q, and exactly $d-2$ other points of $H \oplus x$. Since $n \geqslant C' \prod_{i=4}^{d} \frac{i-1}{i-3} 2^d d! K = C' \prod_{i=4}^{d-1} \frac{i-1}{i-3} 2^{d-1}(d-1)! \left(\frac{d-1}{d-3}2dK\right)$, we can apply induction if $\pi_q(p) \notin \delta^*$.

Note that for all $p \in \mathbb{RP}^d \setminus \delta^*$, the projection π_p is generically one-to-one on δ. Suppose otherwise, and let p be such a projection point. Choose points $q_1, \ldots, q_{d-1} \in \delta^*$ such that $p, q_1, \ldots, q_{d-1}$ span a hyperplane Π in $\mathbb{RP}^d$, which

is possible since δ is non-degenerate. Then each line pq_i intersects δ again in q_i'. So Π intersects δ in at least $2(d-1)$ points. Since $\deg(\delta) = d+1$, we have $d \leqslant 3$, contradicting $d \geqslant 4$. We thus have that every point $p \in \mathbb{RP}^d \setminus \delta$ lies on at most $O(d^2)$ secants or tangents (or lines through two points of δ^* if p is the acnode of δ) of δ (this follows from projection and [64, Chapter III, Theorem 4.4]), in which case there are at most $O(d^2)$ points $q \in H \oplus x$ for which $\pi_q(p) \in \delta^*$.

For each of the at least $(1-\frac{1}{d})n - O(d^2)$ points of $q \in H \oplus x$ for which $\pi_q(p) \notin \delta^*$, by the induction hypothesis, there are at least $f(n, d-1, \frac{d-1}{d-3}2dK)\binom{n}{d-2}$ hyperplanes Π in $\mathbb{RP}^{d-1}$ through $\pi_q(p)$ and exactly $d-2$ points of $H' \uplus x'$. 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 $\pi_q(q)$. Since each hyperplane is counted $d-1$ times, the total number of such hyperplanes is at least

$$\begin{aligned}
&\frac{\left(1-\frac{1}{d}\right)n - O(d^2)}{d-1}\left(f\left(n, d-1, \frac{d-1}{d-3}2dK\right)\binom{n}{d-2} - \binom{n-1}{d-3}\right)\\
&\geqslant \left(\frac{d-1}{d} - \frac{O(d^2}{n}\right)\left(f\left(n, d-1, \frac{d-1}{d-3}2dK\right) - \frac{d-2}{n-d+2}\right)\binom{n}{d-1}\\
&\geqslant \frac{d-1}{2d}f\left(n, d-1, \frac{d-1}{d-3}2dK\right)\binom{n}{d-1} \quad \text{if } n \geqslant C'\prod_{i=4}^{d}\frac{i-1}{i-3}2^d d!K\\
&= f(n,d,K)\binom{n}{d-1}. \qquad \square
\end{aligned}$$

Lemma 6.6. *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^*. Let $A \subseteq H \oplus x$ and $B \subset \mathbb{RP}^d \setminus (H \oplus x)$ with $|A| = a$, $|B| = b$, and $a, b = O(d2^d)$. 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 $n \geqslant Cd^3 2^d d!$ for some sufficiently large absolute constant $C > 0$, then P spans at least $(1 + \frac{c}{d2^d})\binom{n-1}{d-1}$ 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

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

and it can be shown in the same way as in the proof of Lemma 4.12 that this is at least $\binom{n-b}{d-1} - \varepsilon(d, n-b)$, where $\varepsilon(d,n)$ is as defined in Lemma 4.12.

To obtain an upper bound on the number of these hyperplanes that pass through a point $q \in B$, we choose $p \in (H \oplus x) \setminus A$ and a further $d-3$ distinct points from $(H \oplus x) \setminus A$. Then p, the tangent line of δ at p, q, and the $d-3$ points span a unique hyperplane, unless the tangent line passes through q. It follows from [48, Corollary 2.5] and projection that there are at most $d(d+1)$ tangent lines from a given point $q \notin \delta$ to the curve δ of degree $d+1$. It follows that there are at most $b(n-b+d(d+1))\binom{n-b-1}{d-3}$ of these hyperplanes that pass through some point of B.

The number of ordinary hyperplanes of $(H \oplus x) \setminus A$ that contain a point from A is at least $a\left(\binom{n-b}{d-1} - a\binom{n-b}{d-2} - (n-b)\binom{n-b-1}{d-3}\right)$, 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

$$\begin{aligned}\binom{n-b}{d-1} - \varepsilon(d,n-b) - b(n-b+d(d+1))\binom{n-b-1}{d-3} \\ + a\binom{n-b}{d-1} - a^2\binom{n-b}{d-2} - a(n-b)\binom{n-b-1}{d-3} - ab\binom{n-b}{d-2}. \quad (6.2)\end{aligned}$$

Next we find a lower bound to the number of ordinary hyperplanes through exactly one point of B and exactly $d-1$ points of $(H \oplus x) \setminus A$. Note that if $p \in B$ does not lie on a line through two points of $H \oplus x$, then p, a fixed point $q \in A$, and $d-3$ points of $H \oplus x$ span a $(d-2)$-flat, so p lies on at most $\frac{1}{d-2}\binom{n-1}{d-3}$ $(d-2)$-flats through q and exactly $d-2$ other points of $H \oplus x$. Now suppose p lies on a line through two points of $H \oplus x$ including $q \in A$.

Let the other point be q'. Then p lies on at most $\binom{n-2}{d-3}$ $(d-2)$-flats through q, q', and exactly $d-3$ other points of $H \oplus x$. Since p lies on at most $O(d^2)$ secants or tangents (or lines through two points of δ^* if p is the acnode of δ) of δ (as in the proof of Lemma 6.5), we have that p lies on at most

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

$(d-2)$-flats through exactly $d-1$ points of $H \oplus x$.

The number of hyperplanes through at least one point of B and exactly $d-1$ points of $(H \oplus x) \setminus A$ is then at least $b\frac{c'}{d2^d}\binom{n-b}{d-1} - ab\binom{n-b}{d-2}$ by Lemmas 6.4 and 6.5 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 $b\frac{c'}{d2^d}\binom{n-b}{d-1} - \left(ab + \binom{b}{2}\right)\binom{n-b}{d-2}$ ordinary hyperplanes passing though a point of B.

Combining this with (6.2), P spans at least

$$\begin{aligned}\binom{n-b}{d-1} - \varepsilon(d, n-b) - b(n-b+d(d+1))\binom{n-b-1}{d-3} \\ + a\binom{n-b}{d-1} - a^2\binom{n-b}{d-2} - a(n-b)\binom{n-b-1}{d-3} - ab\binom{n-b}{d-2} \\ + b\frac{c'}{d2^d}\binom{n-b}{d-1} - \left(ab + \binom{b}{2}\right)\binom{n-b}{d-2} =: f(a,b)\end{aligned}$$

ordinary hyperplanes. Since

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

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 $a = 0$. Then for $n > b + d - 2$, we have that $f(0, b+1) - f(0,b)$ is at least

$$\begin{aligned}\frac{\frac{c'}{d2^d}(n-b-d+1) - \left(1 + b\frac{c'}{d2^d}\right)(d-1)}{n-b}\binom{n-b}{d-1} \\ - b\binom{n-b}{d-2} - (n-b-1+d(d+1))\binom{n-b-1}{d-3},\end{aligned}$$

which is positive for all $b \geqslant 1$ if $n \geqslant C(b+d)d^2 2^d$ for C sufficiently large. Finally, we have $f(0,1) = (1 + \frac{c'}{d2^d})\binom{n-1}{d-1} - O(d^2\binom{n-2}{d-3}) \geqslant (1 + \frac{c}{d2^d})\binom{n-1}{d-1}$, completing the proof. □

We are now ready to prove Theorems 1.16 and 1.17, restated below.

Theorem 1.16 (Ordinary hyperplanes)**.** *Let $d \geqslant 4$ and let $n \geqslant Cd^3 2^d d!$ 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*

$$\binom{n-1}{d-1} - O\left(d^2 2^{-d/2}\left(\binom{n}{\lfloor (d-1)/2 \rfloor} + \binom{n}{\lfloor (d-3)/2 \rfloor}\right)\right).$$

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.

Proof. Let P be the set of n points. By Lemma 4.9, we may assume that P has at most $\binom{n-1}{d-1}$ ordinary hyperplanes. Since $n \geqslant Cd^3 2^d d!$, we may apply Theorem 1.10 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 4.1, since $n \geqslant Cd^3 2^d d!$, 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 6.6, again since $n \geqslant Cd^3 2^d d!$, 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 4.9 and 4.12 then complete the proof. □

Thus, by Section 4.3, we have a recursive method to compute the exact minimum number of ordinary hyperplanes for a given d and $n \geqslant Cd^3 2^d d!$ for some sufficiently large absolute constant $C > 0$. This is demonstrated in Construction 4.14 (and Construction 4.15) for $d = 4, 5, 6$.

Theorem 1.17 ($(d+1)$-rich hyperplanes)**.** *Let $d \geqslant 4$ and let $n \geqslant Cd^3 2^d d!$ for some sufficiently large absolute constant $C > 0$. The maximum number of $(d+1)$-rich hyperplanes spanned by a set of n points in $\mathbb{RP}^d$ where every*

d points span a hyperplane is

$$\frac{1}{d+1}\left[\binom{n-1}{d}+O\left(d^2 2^{-d/2}\binom{n}{\lfloor (d-1)/2\rfloor}+\binom{n}{\lfloor (d-3)/2\rfloor}\right)\right].$$

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 $d+1$.

Proof. Note that by Corollary 4.13, there exist sets of n points, with every d points spanning a hyperplane, spanning at least

$$\frac{1}{d+1}\left[\binom{n-1}{d}+O\left(d^2 2^{-d/2}\binom{n}{\lfloor (d-1)/2\rfloor}+\binom{n}{\lfloor (d-3)/2\rfloor}\right)\right]$$

$(d+1)$-rich hyperplanes.

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 $(d+1)$-rich hyperplanes. Without loss of generality, we can thus assume P spans at least $\frac{1}{(d+1)}\left[\binom{n-1}{d}+O\left(d^2 2^{-d/2}\binom{n}{\lfloor (d-1)/2\rfloor}+\binom{n}{\lfloor (d-3)/2\rfloor}\right)\right]$ $(d+1)$-rich hyperplanes. Let m_i denote the number of i-rich 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

$$\begin{aligned} m_d &\leqslant \binom{n}{d}-\binom{n-1}{d}-O\left(d^2 2^{-d/2}\binom{n}{\lfloor (d-1)/2\rfloor}+\binom{n}{\lfloor (d-3)/2\rfloor}\right) \\ &= O\left(\binom{n-1}{d-1}\right), \end{aligned}$$

and we can apply Theorem 1.10.

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 $O(d2^d\binom{n}{d-1})$ $(d+1)$-rich 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 1.16 and Lemma 6.6, we know that

$$m_d \geqslant \binom{n-1}{d-1} - O\left(d^2 2^{-d/2}\binom{n}{\lfloor (d-1)/2 \rfloor} + \binom{n}{\lfloor (d-3)/2 \rfloor}\right)$$

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

$$\begin{aligned}\sum_{i \geqslant d+2} \binom{i}{d} m_i &= \binom{n}{d} - m_d - (d+1)m_{d+1} \\ &= \binom{n}{d} - \binom{n-1}{d-1} - \binom{n-1}{d} \\ &\quad + O\left(d^2 2^{-d/2}\binom{n}{\lfloor (d-1)/2 \rfloor} + \binom{n}{\lfloor (d-3)/2 \rfloor}\right) \\ &= O\left(d^2 2^{-d/2}\binom{n}{\lfloor (d-1)/2 \rfloor} + \binom{n}{\lfloor (d-3)/2 \rfloor}\right),\end{aligned}$$

we can conclude that m_{d+1} is maximised when P is exactly a coset of a subgroup of δ^*, in which case Corollary 4.13 completes the proof. □

As above, Section 4.3 gives a recursive method to compute the exact maximum number of $(d+1)$-rich hyperplanes for a given d and $n \geqslant Cd^3 2^d d!$ for some sufficiently large absolute constant $C > 0$. This is again demonstrated in Construction 4.14 (and Construction 4.15) for $d = 4, 5, 6$.

6.3 Circles

We prove Theorems 1.18, 1.19, and 1.20 in this section. Note that the proofs of Theorems 1.18 and 1.20 are very similar to the proofs of their planar analogues Theorems 1.13 and 1.14 respectively, but with some subtle differences. This is due to how they are related via stereographic projection, as seen in Section 5.3, and we remark more on this at the end of the section. We first consider ordinary circles, including 3-rich lines.

Suppose P is an n-point set in $\mathbb{R}^2$ spanning fewer than $\frac{1}{2}n^2$ ordinary circles, and that P is not contained in a circle or a line. Applying Theorem 1.11, we can conclude that, up to inversions, P differs in $O(1)$ points from either a

subset of a line, a coset of a subgroup of a circular elliptic or acnodal cubic, or a double polygon.

The first type of set is very easy to handle, and spans at least $\binom{n-1}{2} = \frac{1}{2}n^2 - O(n)$ strict ordinary circles (and thus ordinary circles) by Lemma 4.2.

Cosets on cubics are also relatively easy to handle. We again obtain a lower bound on the number of strict ordinary circles, not including 3-rich lines.

Lemma 6.7. *Suppose $P \subset \mathbb{R}^2$ differs in K points from a coset $H \oplus x$ of a subgroup H of a circular elliptic or acnodal cubic, where $|H| = n \pm O(K)$ and $4x \ominus \omega \in H$. Then P spans at least $\frac{1}{2}n^2 - O(Kn)$ strict ordinary circles.*

Proof. Suppose that P differs in K points from $H \oplus x$. We know from Constructions 4.14 and 4.15 that $H \oplus x$ spans $\frac{1}{2}n^2 - O(n)$ strict ordinary circles, all of which are tangent to γ. We show that adding or removing K points destroys no more than $O(Kn)$ of these strict ordinary circles, so that the resulting set P still spans at least $\frac{1}{2}n^2 - O(Kn)$ strict ordinary circles.

Suppose we add a point $q \notin H \oplus x$. For $p \in H \oplus x$, at most one circle tangent to γ at p can pass through q. Thus, adding q destroys at most n strict ordinary circles. Now suppose we remove a point $p \in H \oplus x$. Since strict ordinary circles of $H \oplus x$ correspond to solutions of $2p \oplus q \oplus r = \omega$ or $p \oplus 2q \oplus r = \omega$, there are at most $O(n)$ solutions for a fixed p. Thus removing p destroys at most $O(n)$ strict ordinary circles.

Repeating K times, we see that adding or removing K points to or from $H \oplus x$ destroys at most $O(Kn)$ strict ordinary circles out of the $\frac{1}{2}n^2 - O(n)$ spanned by $H \oplus x$. This proves that P spans at least $\frac{1}{2}n^2 - O(Kn)$ strict ordinary circles. □

So there exists an absolute constant $C > 0$ such that a set of n points, not all collinear or concyclic, spanning at most $\frac{1}{2}n^2 - Cn$ ordinary circles, differs in $O(1)$ points from Case (iv) of Theorem 1.18, our structure theorem for sets spanning few ordinary circles. This case, where P is close to an 'aligned' or 'offset' double polygon, requires a more careful analysis of the effect of adding and/or removing points.

Lemma 6.8. *Let S be an 'aligned' or 'offset' double polygon with $|S| = 2m$. Let $P = (S \setminus A) \cup B$ be a set of n points, where A is a subset of S with $a = O(1)$ points and B is a set disjoint from S with $b = O(1)$ points. Then P spans at least $\frac{1}{8}(2 + a + 4b)n^2 - O(n^{11/6})$ ordinary circles.*

Proof. We know from Constructions 4.5 and 4.6 that S spans $\frac{1}{4}n^2 - O(n)$ ordinary circles.

Consider first the number of ordinary circles spanned by $S \setminus A$. As we saw in Construction 4.7, removing a point $p \in S$ destroys at most $3m/2$ ordinary circles spanned by S, and adds $\frac{1}{2}m^2 - O(m) = \frac{1}{8}n^2 - O(n)$ ordinary circles. Noting that there are at most m 4-rich circles spanned by S that go through any two given points of A, we thus have by inclusion-exclusion that $S \setminus A$ spans at least $(\frac{1}{4} + \frac{a}{8})n^2 - O(n)$ ordinary circles.

Now consider adding $q \in B$ to S. For any pair of points from $S \setminus A$, adding $q \in B$ creates a new ordinary circle, unless the circle or line through the pair and q contains three or four points of $S \setminus A$. We already saw that the number of ordinary circles hitting a fixed point is $O(n)$, so it remains to bound the number of 4-rich circles of S that hit q. If q lies on one of the concentric circles, then no 4-rich circles hit q, so we can assume that q does not. Applying inversion in q reduces the problem to bounding the number of 4-rich lines spanned by a subset of two circles. By Proposition 6.2, this number is bounded by $O(n^{11/6})$, so p lies on at most $O(n^{11/6})$ of the 4-rich circles spanned by S. Adding q to S thus creates at least $\binom{n}{2} - O(n^{11/6})$ ordinary circles. Note that each $p \in A$ that was removed destroys at most n of these circles or lines.

Adding q to $S \setminus A$ also destroys at most $O(n)$ strict ordinary circles, since for each $p \in S$ there is only one circle tangent at p and going through q, and for each $p \in A$, at most m strict ordinary circles spanned by $S \setminus A$ go through p. Finally, since there are at most $2m$ circles through two points of B that also go through two points of $S \setminus A$, $P = (S \setminus A) \cup B$ spans at least $(\frac{1}{4} + \frac{a}{8} + \frac{b}{2})n^2 - O(n^{11/6})$ ordinary circles. □

Theorem 1.18, restated below, then follows easily from the lemmas above.

Theorem 1.18 (Ordinary circles)**.**

(*i*) *If n is sufficiently large, the minimum number of ordinary circles spanned by a non-concyclic and non-collinear set of n points in $\mathbb{R}^2$ is equal to*

$$\begin{cases} \frac{1}{4}n^2 - n & \text{if } n \equiv 0 \pmod 4, \\ \frac{3}{8}n^2 - n + \frac{5}{8} & \text{if } n \equiv 1 \pmod 4, \\ \frac{1}{4}n^2 - \frac{1}{2}n & \text{if } n \equiv 2 \pmod 4, \\ \frac{3}{8}n^2 - \frac{3}{2}n + \frac{17}{8} & \text{if } n \equiv 3 \pmod 4. \end{cases}$$

(*ii*) *Let $C > 0$ be a sufficiently large absolute constant. If a set P of n points in $\mathbb{R}^2$ spans fewer than $\frac{1}{2}n^2 - Cn$ ordinary circles, then P lies on the union of two disjoint circles, or the union of a circle and a disjoint line.*

Proof. Suppose that P is a set of n points in $\mathbb{R}^2$ spanning fewer than $\frac{1}{2}n^2 - Cn$ ordinary circles, where C is sufficiently large. Without loss of generality, n is also sufficiently large. By Lemmas 4.2 and 6.7, we need only consider the case where P differs by $O(1)$ points from a double polygon. In the notation of Lemma 6.8, we have $P = (S \setminus A) \cup B$ and $\frac{1}{8}(2+a+4b) < \frac{1}{2}$, which implies that $a \leqslant 1$ and $b = 0$. So P is either equal to S, or is obtained from S by removing one point, which are exactly the cases in Constructions 4.5, 4.6, and 4.7. In particular, the minimum number of ordinary circles occurs in Construction 4.5 when $n \equiv 0 \pmod 4$, in Construction 4.7 when $n \equiv 1, 3 \pmod 4$, and in Constructions 4.5 and 4.6 when $n \equiv 2 \pmod 4$. □

We now consider what happens if we do not count 3-rich lines as ordinary circles, and prove Theorem 1.19, restated below. We first prove the following lemma, which is basically an exercise in Euclidean geometry.

Lemma 6.9. *Let S be a double polygon ('aligned' or 'offset') with m points on each circle. Then a point $q \notin S$ lies on at most m ordinary circles spanned by S.*

Proof. Denote the inner circle by σ_1 and the outer circle by σ_2, both with centre o. We proceed by case analysis on the position of q with respect to σ_1

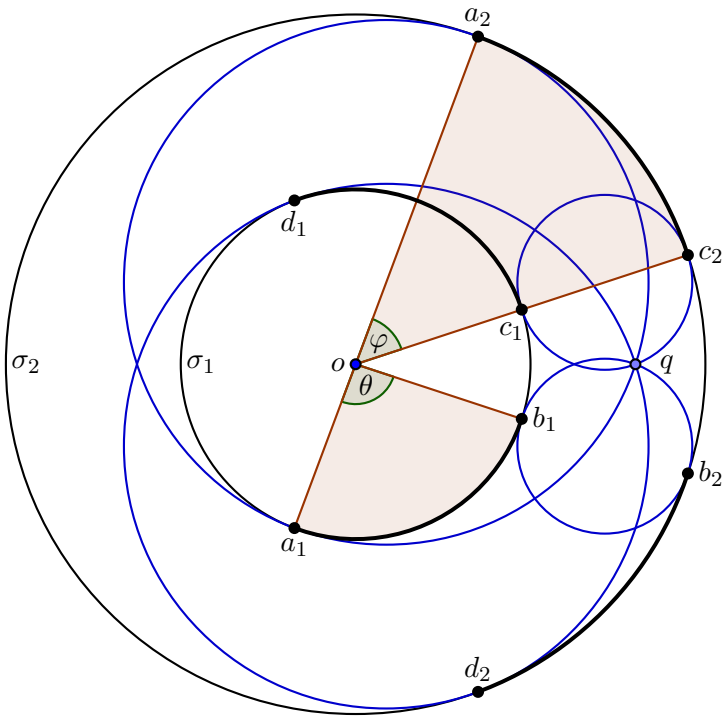

Figure 6.1: Bitangent circles through q

and σ_2. Note that for each point $p \in S$, at most one of the ordinary circles tangent at p can go through q.

If q lies on either σ_1 or σ_2, then q does not lie on any ordinary circle spanned by S.

If q lies inside σ_1, then q lies on at most m ordinary circles spanned by S, since ordinary circles tangent to σ_1 cannot pass through q. Similarly, if q lies outside σ_2, it lies on at most m ordinary circles, since ordinary circles tangent to σ_2 lie inside σ_2.

The remaining case to consider is when q lies in the annulus bounded by σ_1 and σ_2. Consider the subset $S' \subset S$ of points p such that there exists an ordinary circle tangent at p going through q. Consider the four circles passing through q and tangent to both σ_1 and σ_2. They touch σ_1 at a_1, b_1, c_1, d_1 and σ_2 at a_2, b_2, c_2, d_2 as in Figure 6.1. Any circle through q tangent to σ_1 and intersecting σ_2 in two points, must touch σ_1 on one of the open arcs a_1b_1 or c_1d_1. Similarly, any circle through q tangent to σ_2 and intersecting σ_1 in

two points, must touch σ_2 on one of the open arcs a_2c_2 or b_2d_2. It follows that S' must be contained in the relative interiors of one of these four arcs. Since S consists of m equally spaced points on each of σ_1 and σ_2,

$$|S'| < \left\lceil \frac{2m(\angle a_1ob_1 + \angle c_1od_1 + \angle b_2od_2 + \angle a_2oc_2)}{4\pi} \right\rceil = \left\lceil \frac{m(\theta+\varphi)}{\pi} \right\rceil,$$

where θ and φ are as indicated in Figure 6.1. In order to show that $|S'| \leqslant m$, it suffices to show that the angle sum $\theta + \varphi$ is strictly less than π. This is clear from Figure 6.1 (note that a_1, o, a_2 are collinear with a_1 and a_2 on opposite sides of o). □

Theorem 1.19 (Strict ordinary circles)**.**

(*i*) *If n is sufficiently large, the minimum number of strict ordinary circles spanned by a non-concyclic and non-collinear set of n points in $\mathbb{R}^2$ is equal to*

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

(*ii*) *Let $C > 0$ be a sufficiently large absolute constant. If a set P of n points in $\mathbb{R}^2$ spans fewer than $\frac{1}{2}n^2 - Cn$ strict ordinary circles, then P lies on the union of two disjoint circles, or the union of a circle and a disjoint line.*

Proof. Let P be a set of n points not all on a circle or a line, spanning at most $\frac{1}{2}n^2 - Cn$ strict ordinary circles for some sufficiently large absolute constant $C > 0$. By a simple double counting argument, there are at most $\frac{1}{6}n^2$ 3-rich lines, so there are at most $\frac{2}{3}n^2 - O(n)$ ordinary circles. By Theorem 1.11, up to inversions and up to $O(1)$ points, P lies on a line, an ellipse, a circular elliptic cubic, or two concentric circles. By Lemmas 4.2 and 6.7, the first three cases give us at least $\frac{1}{2}n^2 - O(n)$ strict ordinary circles, contrary to assumption. Therefore, we only need to consider the case where, when P is transformed by an inversion to P', we have $P' = (S \setminus A) \cup B$, where S is a double polygon ('aligned' or 'offset'), and $|A| = a$, $|B| = b$.

By Lemma 6.8, P' has at least $\frac{1}{8}(2+a+4b)n^2 - O(n^{11/6})$ ordinary circles, which gives us the inequality $\frac{1}{8}(2+a+4b) < \frac{2}{3}$, which in turn gives us $a \leqslant 3$ and $b = 0$. Therefore, P' lies on two concentric circles, and P lies on the disjoint union of two circles or the disjoint union of a line and a circle.

Suppose that $a = 3$ (and $b = 0$). Then P' has $\frac{5}{8}n^2 - O(n)$ ordinary circles. Those passing through the centre of the inversion that transforms P to P', are inverted back to straight lines passing through three points of P. As in the proof of Lemma 6.8, there are $\frac{1}{8}n^2 - O(n)$ ordinary circles that pass through any point of A. Also, we can use Lemma 6.9 to show that there are at most $O(n)$ ordinary circles spanned by $S \setminus A$ that intersect in the same point not in S. Indeed, by Lemma 6.9, there are at most $n/2$ ordinary circles of S that intersect in the same point $p \notin S$. Furthermore, for each point $q \in A$ there are $O(n)$ circles or lines through p, q, and two more points of S. It follows that there are $O(n)$ ordinary circles spanned by $S \setminus A$ through p.

Thus, if the centre of inversion is in A, P has $\frac{1}{2}n^2 - O(n)$ strict ordinary circles, which is a contradiction if C is chosen large enough. On the other hand, if the centre of inversion is not in A, then P has $\frac{5}{8}n^2 - O(n)$ strict ordinary circles, also a contradiction.

Therefore, we have $a \leqslant 2$, which means that P' is a set of n points as in Constructions 4.5, 4.6, 4.7, or 4.8.

Next, suppose that n is even. If $a = 2$, then there are $\frac{1}{2}n^2 - O(n)$ ordinary circles and through both points of A there are $\frac{1}{8}n^2 - O(n)$ ordinary circles. If we invert in one of these points in A, we obtain a set with $\frac{3}{8}n^2 - O(n)$ strict ordinary circles (as in Construction 4.8), which is not extremal. Otherwise, $a = 0$, P' is as in Constructions 4.5 or 4.6, and there are at least $\frac{1}{4}n^2 - n$ ordinary circles if $n \equiv 0 \pmod 4$ and $\frac{1}{4}n^2 - \frac{1}{2}n$ if $n \equiv 2 \pmod 4$. Let p be the centre of the inversion that transforms P to P'. Then all the 3-rich lines of P are inverted to strict ordinary circles in the double polygon P', all passing through p. By Lemma 6.9, there are at most $n/2$ ordinary circles that intersect in the same point not in P'. Thus, in P there at most $n/2$ 3-rich lines, and the number of strict ordinary circles is at least $\frac{1}{4}n^2 - \frac{3}{2}n$ if $n \equiv 0 \pmod 4$ and $\frac{1}{4}n^2 - n$ if $n \equiv 2 \pmod 4$, which match the constructions described in Construction 4.5 (and Construction 4.6 if $n \equiv 2 \pmod 4$), if

the radii are chosen so that each vertex of the inner polygon has an ordinary circle that is a straight line tangent to it.

Finally, suppose that n is odd. Then $a = 1$ and P' is as described in Construction 4.7, with $\frac{3}{8}n^2 - O(n)$ strict ordinary circles. It follows that P must be as described in Construction 4.8, with $\frac{1}{4}n^2 - \frac{3}{4}n + \frac{1}{2}$ strict ordinary circles if $n \equiv 1 \pmod 4$ and $\frac{1}{4}n^2 - \frac{5}{4}n + \frac{3}{2}$ strict ordinary circles if $n \equiv 3 \pmod 4$. □

Finally, we prove Theorem 1.20, restated below. As mentioned in Section 1.2.2, by inversion, the following theorem remains true whether we count 4-rich lines as 4-rich circles or not.

Theorem 1.20 (4-rich circles)**.**

(*i*) *If n is sufficiently large, the maximum number of 4-rich circles spanned by a set of n points in $\mathbb{R}^2$ is equal to*

$$\begin{cases} \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{5}{6}n & \text{if } n \equiv 0 \pmod 8, \\ \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{11}{24}n - \frac{1}{4} & \text{if } n \equiv 1, 3, 5, 7 \pmod 8, \\ \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{7}{12}n - \frac{1}{2} & \text{if } n \equiv 2, 6 \pmod 8, \\ \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{5}{6}n - 1 & \text{if } n \equiv 4 \pmod 8. \end{cases}$$

(*ii*) *Let $C > 0$ be a sufficiently large absolute constant. If a set P of n points in $\mathbb{R}^2$ spans more than $\frac{1}{24}n^3 - \frac{7}{24}n^2 + Cn$ 4-rich circles, then up to an inversion, P lies on a ellipse or a circular elliptic cubic curve.*

Proof. Let P be a set of n points in $\mathbb{R}^2$ with at least $\frac{1}{24}n^3 - \frac{7}{24}n^2 + O(n)$ 4-rich circles. Let t_i denote the number of i-rich lines ($i \geqslant 2$) and s_i the number of i-rich circles ($i \geqslant 3$) in P. By counting unordered triples of points, we have

$$\binom{n}{3} = \sum_{i \geqslant 3} \binom{i}{3}(t_i + s_i) \geqslant t_3 + s_3 + 4(t_4 + s_4),$$

hence

$$\frac{1}{6}n^3 - O(n^2) \geqslant t_3 + s_3 + 4\left(\frac{1}{24}n^3 - O(n^2)\right)$$

and $t_3 + s_3 = O(n^2)$, so we can apply Theorem 1.11. We next consider each of the cases of that theorem in turn.

If all except $O(1)$ points of P lie on a line, it is easy to see that P spans only $O(n^2)$ 4-rich circles, contrary to assumption.

If all except $O(1)$ are vertices of two regular m-gons on concentric circles where $m = n/2 \pm O(1)$, then we know from Constructions 4.5, 4.6, and 4.7 that P spans at most $\frac{1}{32}n^3 + O(n^2)$ 4-rich circles, again contrary to assumption.

Suppose next that $P = ((H \oplus x) \setminus A) \cup B$, where H is a finite subgroup of order $m = n \pm O(1)$ of a circular elliptic cubic, A is a subset of $H \oplus x$ with $a = O(1)$ points, and B is a set disjoint from $H \oplus x$ with $b = O(1)$ points. Then $n = m - a + b$. The number of 4-rich circles in $H \oplus x$ is $\frac{1}{24}m^3 - \frac{1}{4}m^2 + O(m)$. We next determine an upper bound for the number of 4-rich circles in P.

For each $p \in A$, let C_p be the set of 4-rich circles of $H \oplus x$ that pass through p. Then $|C_p| = \frac{1}{6}m^2 - O(m)$ and $|C_p \cap C_q| = O(m)$ for distinct $p, q \in A$. By inclusion-exclusion, we destroy at least $|\bigcup_{p\in A} C_p| \geqslant \frac{1}{6}am^2 - O(m)$ 4-rich circles by removing A, and we still have at most $\frac{1}{24}m^3 - \frac{1}{4}m^2 - \frac{1}{6}am^2 + O(m)$ 4-rich circles in $(H \oplus x) \setminus A$.

For each $p \in B$, the number of ordinary circles spanned by $H \oplus x$ passing through p is at most $O(m)$. This is because each such circle or line is tangent to the cubic at one of the points of $H \oplus x$, and there is only one circle or line through p and tangent at a given point of $H \oplus x$. Also, for each pair of distinct $p, q \in B$, there are at most $O(m)$ circles or liens through p and q and two points of $H \oplus x$; and for any three $p, q, r \in B$ there are at most $O(1)$ circles or lines through p, q, r and one point of $H \oplus x$. Therefore, again by inclusion-exclusion, by adding B we gain at most $O(m)$ 4-rich circles.

It follows that the number of 4-rich circles spanned by P is

$$t_4 + s_4 \leqslant \frac{1}{24}m^3 - \frac{1}{4}m^2 - \frac{1}{6}am^2 + O(m) = \frac{n^3 - (a + 3b + 6)n^2 + O(n)}{24}.$$

Since we assumed that

$$t_4 + s_4 \geqslant \frac{n^3 - 7n^2 + O(n)}{24},$$

we obtain $a + 3b < 1$. Therefore, $a = b = 0$ and $P = H \oplus x$. The maximum number of 4-rich circles in a coset has been determined in Constructions 4.15 and 4.14.

The final case, when all but $O(1)$ points of P lie on an ellipse, can be reduced to the previous case. Indeed, by Corollary 3.24, if we invert the ellipse in a point on the ellipse, we obtain a circular acnodal cubic, and then the above analysis holds verbatim for the group of smooth points on this cubic. □

We note that Theorems 1.18 and 1.20 can be proved via stereographic projection and applying their planar analogues Theorem 1.13 and 1.14 respectively. This is illustrated in the next section for the extremal theorems for ordinary and $(d+2)$-rich hyperspheres.

6.4 Hyperspheres

We prove Theorem 1.21 and 1.22 in this section, which follow from their hyperplanar analogues Theorems 1.16 and 1.17 respectively.

Theorem 1.21 (Ordinary hyperspheres)**.** *Let $d \geqslant 3$ and let $n \geqslant Cd^4 2^d d!$ for some sufficiently large absolute constant $C > 0$. Let P be a set of n points in $\mathbb{R}^d$ where no $d+1$ points lie on a $(d-2)$-sphere or a $(d-2)$-flat. If P is not contained in a hypersphere or a hyperplane, then the minimum number of ordinary hyperspheres spanned by P is exactly $\binom{n-1}{d}$ if d is odd and is*

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

if d is even.

If d is odd, this minimum is attained by $n-1$ points in a hypersphere or a hyperplane together with a point not in the hypersphere or hyperplane.

If $d = 2k$ is even, this minimum is attained by a coset of a subgroup of a bounded $(k-1)$-spherical rational normal curve of degree d or a k-spherical elliptic normal curve of degree $d+1$, and when $d+1$ and n are coprime, by $n-1$ points in a hypersphere or a hyperplane together with a point not in the hypersphere or hyperplane.

Proof. By Constructions 4.15 and 4.14, we may assume P spans at most $\binom{n-1}{d}$ ordinary hyperspheres, so that Theorem 1.12 applies. Projecting P stereographically, we obtain a set $P' := \pi^{-1}(P) \subset \overline{\mathbb{S}^d} \subset \mathbb{RP}^{d+1}$ of n points, no $d+1$ of which lie on a hyperplane. By Theorem 1.12 and Proposition 3.21, P' differs in at most $O(d2^d)$ points from

(1) a subset of a hyperplane, or

(2) 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 $d+2$, for some x such that $(d+2)x \in H$.

Note that if d is odd, then only Case (1) occurs. The theorem then follows from Lemma 4.1 in the odd-dimensional case, and Theorem 1.16 in the even-dimensional case. □

For odd d, by stereographic projection and Lemma 4.1, the minimum number of ordinary hyperspheres is thus exactly $\binom{n-1}{d}$ for $n \geqslant Cd^4 2^d d!$, where $C > 0$ is some sufficiently large absolute constant. For even d, as with hyperplanes in Section 6.2, we can compute the exact minimum number of ordinary hyperspheres for $n \geqslant Cd^4 2^d d!$, where $C > 0$ is some sufficiently large absolute constant, using the recursive method described in Section 4.3. The minimum when $d = 4$ is given in Construction 4.14 (and Construction 4.15).

Theorem 1.22 ($(d+2)$-rich hyperspheres)**.** *Let $d \geqslant 3$ and let $n \geqslant Cd^4 2^d d!$ for some sufficiently large absolute constant $C > 0$. Let P be a set of n points in $\mathbb{R}^d$ where no $d+1$ points lie on a $(d-2)$-sphere or a $(d-2)$-flat. Then the maximum number of $(d+2)$-rich hyperspheres spanned by P is bounded above by*

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

and this bound is tight when d is even.

If $d = 2k$ is even, this maximum is attained by a coset of a subgroup of a bounded $(k-1)$-spherical rational normal curve of degree d or a k-spherical elliptic normal curve of degree $d+1$.

Proof. This theorem follows from stereographic projection and Theorem 1.17. Note that in the case when d is odd, the extremal configurations in Theorem 1.17 lying on an algebraic curve of degree $d+2$ do not exist, as this curve has to lie on $\overline{\mathbb{S}^d}$, hence is bounded, contradicting Lemma 3.5. □

As above, if d is even, we can compute the exact maximum number of $(d+2)$-rich hyperplanes for $n \geqslant Cd^4 2^d d!$, where $C > 0$ is some sufficiently large absolute constant, using the recursive method described in Section 4.3. The maximum when $d = 4$ is again given in Construction 4.14 (and Construction 4.15). On the other hand, if d is odd, we do not have any lower bound that is superlinear in n, nor can we show an upper bound of the form $\frac{c}{d+2}\binom{n}{d+1}$ for some $c < 1$.

Bibliography

[1] E. Arbarello, M. Cornalba, P. A. Griffiths, and J. Harris, *Geometry of Algebraic Curves. Vol. I*, Grundlehren der Mathematischen Wissenschaften, vol. 267, Springer, 1985.

[2] M. Artebani and I. Dolgachev, *The Hesse pencil of plane cubic curves*, Enseign. Math. (2) **55** (2009), no. 3-4, 235–273.

[3] A. Bálintová and V. Bálint, *On the number of circles determined by n points in the Euclidean plane*, Acta Math. Hungar. **63** (1994), no. 3, 283–289.

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

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

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

[7] E. Ballico, *Special projections of projective varieties*, Int. Math. J. **3** (2003), no. 1, 11–12.

[8] E. Ballico, *Special inner projections of projective varieties*, Ann. Univ. Ferrara Sez. VII (N.S.) **50** (2004), no. 1, 23–26.

[9] P. Le Barz, *Formules multisécantes pour les courbes gauches quelconques*, Enumerative geometry and classical algebraic geometry (Nice, 1981), Progr. Math., vol. 24, Birkhäuser, Boston, Mass., 1982, pp. 165–197.

[10] A. B. Basset, *An Elementary Treatise on Cubic and Quartic Curves*, Deighton, Bell & Co., 1901.

[11] M. Berger, R. Pansu, J.-P. Berry, and X. Saint-Raymond, *Problems in Geometry*, Springer, 1984.

[12] M.-A. Bertin, *On the singularities of the trisecant surface to a space curve*, Matematiche (Catania) **53** (1998), no. suppl., 15–22 (1999).

[13] D. Blair, *Inversion Theory and Conformal Mappings*, American Mathematical Society, 2000.

[14] P. Brass, W. Moser, and J. Pach, *Research Problems in Discrete Geometry*, Springer, 2005.

[15] A. Brill, *Ueber die Doppelpunkte von Curven im Raume, deren Geschlecht Null ist*, Math. Ann. **3** (1871), no. 3, 456–458.

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

[17] J. Csima and E. T. Sawyer, *There exist* $6n/13$ *ordinary points*, Discrete Comput. Geom. **9** (1993), no. 2, 187–202.

[18] I. Dolgachev, *Lectures on Invariant Theory*, Cambridge University Press, 2003.

[19] D. Eisenbud, M. Green, and J. Harris, *Cayley-Bacharach theorems and conjectures*, Bull. Amer. Math. Soc. (N.S.) **33** (1996), no. 3, 295–324.

[20] P. D. T. A. Elliott, *On the number of circles determined by n points*, Acta Math. Acad. Sci. Hungar. **18** (1967), 181–188.

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

[22] A. R. Forsyth, *On twisted quartics of the second species*, The Quarterly Journal of Pure and Applied Mathematics **27** (1895), 247–269.

[23] W. Fulton, *Introduction to Intersection Theory in Algebraic Geometry*, CBMS Regional Conference Series in Mathematics, vol. 54, American Mathematical Society, 1984.

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

[25] B. Green and T. Tao, *On sets defining few ordinary lines*, Discrete Comput. Geom. **50** (2013), no. 2, 409–468.

[26] L. Gruson and C. Peskine, *Courbes de l'espace projectif: variétés de sécantes*, Enumerative geometry and classical algebraic geometry (Nice, 1981), Progr. Math., vol. 24, Birkhäuser, Boston, Mass., 1982, pp. 1–31 (French).

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

[28] S. Hansen, *On configurations of* 3*-space without elementary planes and on the number of ordinary planes*, Math. Scand. **47** (1980), 181–194.

[29] J. Harris, *Algebraic Geometry: A First Course*, Springer, 1992.

[30] R. Hartshorne, *Algebraic Geometry*, Springer, 1977.

[31] H. Hilton, *Plane Algebraic Curves*, Oxford University Press, 1920.

[32] A. Iarrobino and V. Kanev, *Power Sums, Gorenstein Algebras, and Determinantal Loci*, Lecture Notes in Mathematics, vol. 1721, Springer, 1999. Appendix C by Iarrobino and Steven L. Kleiman.

[33] F. Joachimsthal, *Démonstration d'un théorème de Mr. Steiner*, J. Reine Angew. Math. **36** (1848), 95–96.

[34] W. W. Johnson, *Classification of plane curves with reference to inversion*, The Analyst **4** (1877), no. 2, 42–47.

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

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

[37] V. Klee and S. Wagon, *Old and New Unsolved Problems in Plane Geometry and Number Theory*, Mathematical Association of America, 1991.

[38] 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.

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

[40] 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.

[41] A. Lin and K. Swanepoel, *Ordinary planes, coplanar quadruples, and space quartics*, J. Lond. Math. Soc. (2) (2019). doi:10.1112/jlms.12251.

[42] A. Lin and K. Swanepoel, *On sets defining few ordinary hyperplanes*. arXiv:1808.10849.

[43] A. Lin and K. Swanepoel, *Ordinary hyperspheres and spherical curves*. arXiv:1905.09639.

[44] E. Melchior, *Über Vielseite der projektiven Ebene*, Deutsche Math. **5** (1941), 461–475.

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

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

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

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

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

[50] O. E. Raz, M. Sharir, and F. de Zeeuw, *Polynomials vanishing on Cartesian products: The Elekes-Szabó Theorem revisited*, Duke Math. J. **165** (2016), no. 18, 3517–3566.

[51] O. E. Raz, M. Sharir, and F. de Zeeuw, *The Elekes-Szabó Theorem in four dimensions*, Israel J. Math. **227** (2018), no. 2, 663–690.

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

[53] H. Richmond, *Rational space-curves of the fourth order*, Trans. Camb. Phil. Soc. **19** (1900), 132–150.

[54] B. Segre, *On the locus of points from which an algebraic variety is projected multiply*, Proc. Phys.-Math. Soc. Japan (3) **18** (1936), 425–426.

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

[56] F. Severi, *Vorlesungen über algebraische Geometrie: Geometrie auf einer Kurve, Riemannsche Flächen, Abelsche Integrale*, Bibliotheca Mathematica Teubneriana, Band 32, Teubner, 1921.

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

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

[59] J. H. Silverman and J. T. Tate, *Rational Points on Elliptic Curves*, Second Edition, Springer, 1992.

[60] D. M. Y. Sommerville, *Analytic Geometry of Three Dimensions*, Cambridge University Press, 1939.

[61] J. J. Sylvester, *Mathematical question 11851*, Educational Times **46** (1893), 156.

[62] J. J. Sylvester, *On a remarkable discovery in the theory of canonical forms and of hyperdeterminants*, Philosophical Magazine **2** (1951), 391–410. Paper 41 in The Collected Mathematical Papers of James Joseph Sylvester, Cambridge University Press, 1904.

[63] H. G. Telling, *The Rational Quartic Curve in Space of Three and Four Dimensions*, Cambridge University Press, 1936. Re-issued 2015.

[64] R. J. Walker, *Algebraic Curves*, Springer, 1978.

[65] T. R. Werner, *Rational families of circles and bicircular quartics*, Ph.D. Dissertation, Friedrich-Alexander-Universität Erlangen-Nürnberg, 2011.

[66] E. Weyr, *Ueber rationale Curven vierter Ordnung*, Math. Ann. **4** (1871), no. 2, 243–244.

[67] P. R. Wolfson, *George Boole and the origins of invariant theory*, Historia Math. **35** (2008), no. 1, 37–46.

[68] R. Zhang, *On the number of ordinary circles determined by n points*, Discrete Comput. Geom. **46** (2011), no. 2, 205–211.