

MIT Open Access Articles

Algebraic curves, rich points, and doubly-ruled surfaces

The MIT Faculty has made this article openly available. **Please share** how this access benefits you. Your story matters.

Citation: Guth, Larry and Joshua Zahl. "Algebraic curves, rich points, and doubly-ruled surfaces." *American Journal of Mathematics* 140, 5 (October 2018): 1187-1229 ©2018 Project MUSE

As Published: <http://dx.doi.org/10.1353/ajm.2018.0028>

Publisher: Project Muse

Persistent URL: <https://hdl.handle.net/1721.1/122976>

Version: Original manuscript: author's manuscript prior to formal peer review

Terms of use: Creative Commons Attribution-Noncommercial-Share Alike



Algebraic curves, rich points, and doubly-ruled surfaces

Larry Guth*

Joshua Zahl†

July 11, 2018

Abstract

We study the structure of collections of algebraic curves in three dimensions that have many curve-curve incidences. In particular, let k be a field and let \mathcal{L} be a collection of n space curves in k^3 , with $n \ll (\text{char}(k))^2$ or $\text{char}(k) = 0$. Then either A) there are at most $O(n^{3/2})$ points in k^3 hit by at least two curves, or B) at least $\Omega(n^{1/2})$ curves from \mathcal{L} must lie on a bounded-degree surface, and many of the curves must form two “rulings” of this surface.

We also develop several new tools including a generalization of the classical flecnode polynomial of Salmon and new algebraic techniques for dealing with this generalized flecnode polynomial.

1 Introduction

If \mathcal{L} is a collection of n lines in the plane, then there can be as many as $\binom{n}{2}$ points that are incident to at least two lines. If instead \mathcal{L} is a collection of n lines in \mathbb{R}^3 , there can still be $\binom{n}{2}$ points that are incident to two or more lines; for example, this occurs if we choose n lines that all lie in a common plane in \mathbb{R}^3 , with no two lines parallel. A similar number of incidences can be achieved if the lines are arranged into the rulings of a regulus. This leads to the question: if we have a collection of lines in \mathbb{R}^3 such that many points are incident to two or more lines, must many of these lines lie in a common plane or regulus?

This question has been partially answered by the following theorem of Guth and Katz:

Theorem 1.1 (Guth-Katz [6]). *Let \mathcal{L} be a collection of n lines in \mathbb{R}^3 . Let $A \geq 100n^{1/2}$ and suppose that there are $\geq 100An$ points $p \in \mathbb{R}^3$ that are incident to at least two points of \mathcal{L} . Then there exists a plane or regulus $Z \subset \mathbb{R}^3$ that contains at least A lines from \mathcal{L} .*

In this paper, we will show that a similar result holds for more general curves in k^3 :

Theorem 1.2. *Fix $D > 0$. Then there are constants c_1, C_1, C_2 so that the following holds. Let k be a field and let \mathcal{L} be a collection of n irreducible curves in k^3 of degree at most D . Suppose that $\text{char}(k) = 0$ or $n \leq c_1(\text{char}(k))^2$. Then for each $A \geq C_1n^{1/2}$, either there are at most C_2An points in k^3 incident to two or more curves from \mathcal{L} , or there is an irreducible surface Z of degree $\leq 100D^2$ that contains at least A curves from \mathcal{L} .*

In fact, more is true. If all the curves in \mathcal{L} lie in a particular family of curves, then the surface Z described above is “doubly ruled” by curves from this family. For example, if all the curves in \mathcal{L} are circles, then Z is doubly ruled by circles; this means that there are (at least) two circles passing through a generic point of Z . In order to state this more precisely, we will first need to say what it means for a finite set \mathcal{L} of curves to lie in a certain family of curves. We will do this in Section 3 and state a precise version of the stronger theorem at the end of that section.

*Massachusetts Institute of Technology, Cambridge, MA, lguth@math.mit.edu.

†Massachusetts Institute of Technology, Cambridge, MA, jzahl@math.mit.edu.

1.1 Proof sketch and main ideas

As in the proof of Theorem 1.1, we will first find an algebraic surface Z that contains the curves from \mathcal{L} . A “degree reduction” argument will allow us to find a surface of degree roughly $n/A \ll n^{1/2}$ with this property. In [6], the first author and Katz consider the flecnode polynomial, which describes the local geometry of an algebraic surface $Z \subset \mathbb{R}^3$. This polynomial is adapted to describing surfaces that are ruled by lines. In the present work, we construct a generalization of this polynomial that lets us measure many geometric properties of a variety $Z \subset K^3$. In particular, we will find a generalized flecnode polynomial that tells us when a surface is doubly ruled by curves from some specified family.

We will also explore a phenomena that we call “sufficiently tangent implies trapped.” If a curve is “sufficiently tangent” to a surface, then the curve must be contained in that surface. More precisely, if we fix a number $D \geq 1$, then for any surface $Z \subset K^3$ we can find a Zariski open subset $O \subset Z$ so that any irreducible curve of degree $\leq D$ that is tangent to Z at a point $z \in O$ to order $\Omega_D(1)$ must be contained in Z ; the key point is that the necessary order of tangency is independent of the degree of Z . This will be discussed further in Section 8. The result is analogous to the Cayley-Monge-Salmon theorem, which says that if there is a line tangent to order at least three at every smooth point of a variety, then this variety must be ruled by lines (see [13], or [10, 8] for a more modern treatment).

Finally, we will prove several structural statements about surfaces in K^3 that are doubly ruled by curves. A classical argument shows that any algebraic surface in K^3 that is doubly ruled by lines must be of degree one or two. We will prove an analogous statement that any surface that is doubly ruled curves of degree $\leq D$. This will be done in Section 11.

1.2 Previous work

In [6], the first author and Katz show that given a collection of n lines in \mathbb{R}^3 with at most $n^{1/2}$ lines lying in a common plane or regulus, there are at most $n^{3/2}$ points in \mathbb{R}^3 that are incident to two or more lines. This result was a major component of their proof of the Erdős distinct distance problem in the plane.

In [9], Kollár extends this result to arbitrary fields (provided the characteristic is 0 or larger than \sqrt{n}). Kollár’s techniques differ from the ones in the present paper. In particular, Kollár traps the lines in a complete intersection of two surfaces, and then uses tools from algebraic geometry to control the degree of this complete intersection variety. In [15], Sharir and Solomon consider a similar point-line incidence problem, and they provide a new proof of some of the incidence results in [6].

In [4], the first author showed that given a collection of n lines in \mathbb{R}^3 and any $\epsilon > 0$, there are $O_\epsilon(n^{3/2+\epsilon})$ points that are incident to two or more lines, provided at most $n^{1/2-\epsilon}$ lines lie in any algebraic surface of degree $O_\epsilon(1)$. This proof also applies to bounded-degree curves in place of lines. However, the proof is limited to the field $k = \mathbb{R}$, and unlike the present work, it does not say anything about the structure of the surfaces containing many curves.

1.3 Thanks

The first author was supported by a Sloan fellowship and a Simons Investigator award. The second author was supported by a NSF mathematical sciences postdoctoral fellowship.

2 Constructible sets

Definition 2.1. Let K be an algebraically closed field. A constructible set $Y \subset K^N$ is a finite boolean combination of algebraic sets. This means the following:

- There is a finite list of polynomials $f_j : K^N \rightarrow K$, $j = 1, \dots, J(Y)$.
- Define $v(f_j)$ to be 0 if $f_j = 0$ and 1 if $f_j \neq 0$. The vector $v(f_j) = (v(f_1), \dots, v(f_j), \dots)$ gives a map from K^N to the boolean cube $\{0, 1\}^{J(Y)}$.
- There is a subset $B_Y \subset \{0, 1\}^J$ so that $x \in Y$ if and only if $v(f_j(x)) \in B_Y$.

The constructible sets form a Boolean algebra. This means that finite unions and intersections of constructible sets are constructible, and the compliment of a constructible set is constructible.

Definition 2.2. If Y is a constructible set, we define the complexity of Y to be $\min(\deg f_1 + \dots + \deg f_{J(Y)})$, where the minimum is taken over all representations of Y , as described in Definition 2.1.

Remark 2.3. This definition of complexity is not standard. However, we will only be interested in constructible sets of “bounded complexity,” and the complexity of a constructible set will never appear in any bounds in a quantitative way. Thus any other reasonable definition of complexity would work equally well.

The crucial result about constructible sets is Chevalley’s theorem.

Theorem 2.4 (Chevalley; see [7], Theorem 3.16 or [11], Chapter 2.6, Theorem 6). Let $X \subset K^{M+N}$ be a constructible set of complexity $\leq C$. Let π be the projection from $K^M \times K^N$ to K^M . Then $\pi(X)$ is a constructible set in K^M of complexity $O_C(1)$.

Here is an illustrative example. Suppose that X is the zero-set of $z_1 z_2 - 1$ in $\mathbb{C}^2 = \mathbb{C} \times \mathbb{C}$. The set X is an algebraic set, and it is certainly constructible. When we project X to the first factor, we get $\mathbb{C} \setminus \{0\}$. This projection is not an algebraic set, but it is constructible.

We will also need to define constructible sets in projective space.

Definition 2.5. A (projective) constructible set $Y \subset K\mathbf{P}^N$ is a finite boolean combination of projective algebraic sets. This means the following:

- There is a finite list of homogeneous polynomials $f_j : K^{N+1} \rightarrow K$, $j = 1, \dots, J(Y)$.
- Define $v(f_j)$ to be 0 if $f_j = 0$ and 1 if $f_j \neq 0$. The vector $v(f_j) = (v(f_1), \dots, v(f_j), \dots)$ gives a map from $K\mathbf{P}^N$ to the boolean cube $\{0, 1\}^{J(Y)}$.
- There is a subset $B_Y \subset \{0, 1\}^J$ so that $x \in Y$ if and only if $v(f_j(x)) \in B_Y$.

3 The Chow variety of algebraic curves

The set of all degree D curves in 3-dimensional space turns out to be algebraic object in its own right, and this algebraic structure will play a role in our arguments. This object is called a Chow variety.

The (projective) Chow variety $\hat{\mathcal{C}}_{3,D}$ of degree D irreducible curves in $K\mathbf{P}^3$ is a quasi-projective variety, which is contained in some projective space $K\mathbf{P}^N$, $N = N(D)$. Each irreducible degree D curve $\gamma \in K\mathbf{P}^3$ corresponds to a unique point in the Chow variety, called the “chow point” of γ . Here is a fuller description of the properties of the Chow variety.

Proposition 3.1 (Properties of the (projective) Chow variety). *Let $D \geq 1$. Then there is a number $N = N(D)$ and sets $\hat{\mathcal{C}}_{3,D} \subset \mathbf{KP}^N$, $\hat{\mathcal{C}}_{3,D}^* \subset \mathbf{KP}^3 \times \mathbf{KP}^N$ with the following properties*

- $\hat{\mathcal{C}}_{3,D}$ and $\hat{\mathcal{C}}_{3,D}^*$ are (projective) constructible sets of complexity $O_D(1)$. To clarify, $\hat{\mathcal{C}}_{3,D}$ is defined by a Boolean combination of equalities and not-equalities of homogeneous polynomials in $K[x_0, \dots, x_N]$, while $\hat{\mathcal{C}}_{3,D}^*$ is defined by a Boolean combination of equalities and not-equalities of polynomials that are homogeneous in $K[x_0, \dots, x_N]$ and in $K[y_0, \dots, y_3]$.
- For each irreducible curve $\gamma \subset \mathbf{KP}^3$, there is a unique point $z_\gamma \in \hat{\mathcal{C}}_{3,D}$ so that $\{z_\gamma\} \times \gamma \subset \hat{\mathcal{C}}_{3,D}^*$.
- Conversely, if $z \in \hat{\mathcal{C}}_{3,D}$, then $\hat{\mathcal{C}}_{3,D}^* \cap (\{z\} \times \mathbf{KP}^3) = \{z\} \times \gamma$ for some irreducible curve γ . Furthermore, $z = z_\gamma$.

See e.g. [3] for further details. For a friendlier introduction, one can also see [7, Chapter 21] (in the notation used in [7], $\hat{\mathcal{C}}_{3,D}$ is called the “open” Chow variety). [7] works over \mathbb{C} rather than over arbitrary fields, but the arguments are the same (at least provided $\text{char } K > D$, which will always be the case for us).

For our purposes, it will be easier to work with affine varieties, so we will identify K^N with the set $\mathbf{KP}^N \setminus H$, where H is a generic hyperplane. In Theorem 3.8, we are given a finite collection \mathcal{L} of irreducible curves of degree $\leq D$. Thus the choice of hyperplane H does not matter, provided that none of the curves correspond to points in the Chow variety that lie in H .

Finally, we will fix a coordinate chart and only consider those curves in the Chow variety that do not lie in the plane $\{[x_0 : x_1 : x_2 : x_3] : x_0 = 0\}$ (this corresponds to the coordinate chart $(x_1, x_2, x_3) \mapsto [1 : x_1 : x_2 : x_3]$). Since no curves from \mathcal{L} correspond to curves that lie in $\{[x_0 : x_1 : x_2 : x_3] : x_0 = 0\}$, this restriction will not pose any difficulties. Let $\tilde{\mathcal{C}}_{3,D}$ be the “modified” Chow variety, which consists of all projective curves $\gamma \subset \mathbf{KP}^3$ that do not lie in the plane $\{[x_0 : x_1 : x_2 : x_3] : x_0 = 0\}$, and for which the Chow point in \mathbf{KP}^N corresponding to γ does not lie in the hyperplane H .

$\tilde{\mathcal{C}}_{3,D}$ is a constructible set that parameterizes (almost all) irreducible degree D algebraic curves in K^3 . Of course our definition of $\tilde{\mathcal{C}}_{3,D}$ depends on the choice of hyperplane H , but we will suppress this dependence, since the choice of H will not matter for our results.

Lemma 3.2 (Properties of the (affine) Chow variety of degree D curves). *Let $D \geq 1$ and fix a hyperplane $H \subset \mathbf{KP}^N$, where $N = N(D)$ (as in Proposition 3.1). Then there are sets $\tilde{\mathcal{C}}_{3,D} \subset K^N$, $\tilde{\mathcal{C}}_{3,D}^* \subset K^N \times K^3$ with the following properties*

- $\tilde{\mathcal{C}}_{3,D}$ and $\tilde{\mathcal{C}}_{3,D}^*$ are constructible sets of complexity $O_D(1)$.
- For each irreducible degree D curve $\gamma \subset K^3$ whose projectivization does not correspond to a chow point in H , there is a unique point $z_\gamma \in \tilde{\mathcal{C}}_{3,D}$ so that $\{z_\gamma\} \times \gamma \subset \tilde{\mathcal{C}}_{3,D}^*$.
- Conversely, if $z \in \tilde{\mathcal{C}}_{3,D}$, then $\tilde{\mathcal{C}}_{3,D}^* \cap (\{z\} \times K^3) = \{z\} \times \gamma$ for some irreducible curve γ . Furthermore, $z = z_\gamma$.

The constructible set $\tilde{\mathcal{C}}_{3,D}$ parameterizes the set of irreducible curves of degree (exactly) D . However, Theorem 1.2 is a statement about curves of degree at most D . To deal with this, we will define a constructible set that parameterizes the set of curves of degree at most D . Recall that for $j = 1, \dots, D$, we have constructible sets $\tilde{\mathcal{C}}_{3,j} \subset K^{N_j}$ and $\tilde{\mathcal{C}}_{3,j}^* \subset K^{N_j} \times K^3$. Let $V = K^{N_1} \times \dots \times K^{N_D}$

and let $W = (K^{N_1} \times K^3) \times \dots \times (K^{N_D} \times K^3)$. Each copy of K^{N_j} has a natural embedding into V , given by

$$\begin{aligned} \varphi_j: K^{N_j} &\rightarrow V, \\ x &\mapsto (0, \dots, 0, x, 0, \dots, 0) \in K^{N_1} \times \dots \times K^{N_{j-1}} \times K^{N_j} \times K^{N_{j+1}} \times \dots \times K^{N_D}. \end{aligned}$$

Similarly, there is a natural embedding φ_j^* of $K^{N_j} \times K^3$ into W . Define

$$\begin{aligned} \mathcal{C}_{3,D} &:= \bigcup_{j=1}^D \varphi_j(\tilde{\mathcal{C}}_{3,j}), \\ \mathcal{C}_{3,D}^* &:= \pi \left(\bigcup_{j=1}^D \varphi_j^*(\tilde{\mathcal{C}}_{3,j}^*) \right), \end{aligned}$$

where $\pi: W \rightarrow V \times K^3$ is the projection that identifies each copy of K^3 in the vector space $W = (K^{N_1} \times K^3) \times \dots \times (K^{N_D} \times K^3)$ (note that there are many ways that these copies of K^3 can be identified, since there is no distinguished coordinate system for K^3 . However, it doesn't matter which identification we choose).

Abusing notation slightly, we will call $\mathcal{C}_{3,D}$ the Chow variety of curves of degree (at most) D . From this point onwards, we will never refer to either the (projective) Chow variety or the Chow variety of curves of degree exactly D . The sets $\mathcal{C}_{3,D}$ and $\mathcal{C}_{3,D}^*$ satisfy properties analogous to those of $\tilde{\mathcal{C}}_{3,D}$ and $\tilde{\mathcal{C}}_{3,D}^*$. We will record these properties here.

Lemma 3.3 (Properties of the (affine) Chow variety). *Let $D \geq 1$ and fix hyperplanes $H_1 \subset \mathbf{KP}^{N_1}, \dots, H_D \subset \mathbf{KP}^{N_D}$. Then there are sets $\mathcal{C}_{3,D} \subset K^N$, $\mathcal{C}_{3,D}^* \subset K^N \times K^3$ with the following properties*

- $\mathcal{C}_{3,D}$ and $\mathcal{C}_{3,D}^*$ are constructible sets of complexity $O_D(1)$.
- For each irreducible curve $\gamma \subset K^3$ of degree $j \leq D$ whose projectivization does not correspond to a chow point in H_j , there is a unique point $z_\gamma \in \mathcal{C}_{3,D}$ so that $\{z_\gamma\} \times \gamma \subset \mathcal{C}_{3,D}^*$.
- Conversely, if $z \in \mathcal{C}_{3,D}$, then $\mathcal{C}_{3,D}^* \cap (\{z\} \times K^3) = \{z\} \times \gamma$ for some irreducible curve γ of degree at most D . Furthermore, $z = z_\gamma$.

3.1 Surfaces doubly ruled by curves

In this section we will give some brief definitions that allow us to say what it means for a surface to be doubly ruled by curves.

Definition 3.4. *Let K be an algebraically closed field, let $Z \subset K^3$, let $D \geq 1$, and let $\mathcal{C} \subset \mathcal{C}_{3,D}$ be a constructible set. We say that Z is doubly ruled by curves from \mathcal{C} if there is a Zariski open set $O \subset Z$ so that for every $x \in O$, there are at least two curves from \mathcal{C} passing through x and contained in Z .*

Surfaces that are doubly ruled by curves have many favorable properties. The proposition below details some of them.

Proposition 3.5. *Let K be an algebraically closed field, let $Z \subset K^3$ be an irreducible surface, let $D \geq 1$, and let $\mathcal{C} \subset \mathcal{C}_{3,D}$ be a constructible set. Suppose that Z is doubly ruled by curves from \mathcal{C} . Then*

- $\deg(Z) \leq 100D^2$.
- For any $t \geq 1$, we can find two families of curves from \mathcal{C} , each of size t , so that each curve from the first family intersects each curve from the second family.

Remark 3.6. In our definition of doubly ruled, we did not require that the curves passing through $x \in Z$ vary regularly as the basepoint $x \in Z$ changed. However, we get a version of this statement automatically. More precisely, the set

$$\{(x, \gamma) \in Z \times \mathcal{C} : x \in \gamma, \gamma \subset Z\} \quad (1)$$

is a constructible set. Furthermore, there is a Zariski-open set $O \subset Z$ so that for all $x \in O$, the fiber of $\pi: (1) \rightarrow Z$ contains at least two points. For example, if $K = \mathbb{C}$, this means that we can find a Zariski-open set $O' \subset O \subset Z$ so that as the basepoint $x \in O'$ changes, we can smoothly (in the Euclidean topology) select two distinct curves $\gamma_{1,x}, \gamma_{2,x}$ passing through x that are contained in Z .

Definition 3.7. Let k be a field, and let K be the algebraic closure of k . Let $D \geq 1$ and let $\mathcal{C} \subset \mathcal{C}_{3,D}$ be a constructible set. Let \mathcal{L} be a finite set of irreducible curves of degree at most D in k^3 . Abusing notation, we say that $\mathcal{L} \subset \mathcal{C}$ if $\hat{\gamma}$ is an element of \mathcal{C} for each $\gamma \in \mathcal{L}$. Here $\hat{\gamma}$ is the Zariski closure (in K) of $\iota(\gamma)$, where $\iota: k \rightarrow K$ is the obvious embedding. For example, if $\gamma \subset \mathbb{R}^3$ is a real curve, then $\hat{\gamma}$ is the complexification of γ , i.e. the smallest complex curve whose real locus is γ .

3.2 Statement of the theorem

We are now ready to state a precise version of the theorem alluded to in the paragraph following Theorem 1.2.

Theorem 3.8. Fix $D > 0, C > 0$. Then there are constants c_1, C_1, C_2 so that the following holds. Let k be a field and let K be the algebraic closure of K . Let $\mathcal{C} \subset \mathcal{C}_{3,D}$ be a constructible set of complexity at most C . Let \mathcal{L} be a collection of n irreducible algebraic curves in k^3 , with $\mathcal{L} \subset \mathcal{C}$ (see Definition 3.7). Suppose furthermore that $\text{char}(k) = 0$ or $n \leq c_1(\text{char}(k))^2$.

Then for each number $A > C_1 n^{1/2}$, at least one of the following two things must occur

- There are at most $C_2 A n$ points in k^3 that are incident to two or more curves from \mathcal{L} .
- There is an irreducible surface $Z \subset k^3$ that contains at least A curves from \mathcal{L} . Furthermore, \hat{Z} is doubly ruled by curves from \mathcal{C} . See Definition 3.4 for the definition of doubly ruled, and see Proposition 3.5 for the implications of this statement.

Taking $\mathcal{C} = \mathcal{C}_{3,D}$, we see that Theorem 1.2 is an immediate corollary of Theorem 3.8. It remains to prove Theorem 3.8.

4 Curves and complete intersections

An algebraic curve $\gamma \subset K^3$ is a complete intersection if $\gamma = Z(P) \cap Z(Q)$ for some $P, Q \in K[x_1, x_2, x_3]$. Not every algebraic curve is a complete intersection, but any algebraic curve γ is contained in a complete intersection. Complete intersections are easier to work with in some situations, and we will often study a curve γ using a complete intersection $Z(P) \cap Z(Q) \supset \gamma$. In this subsection, we discuss the space of complete intersections, and we show that any algebraic curve lies in a complete intersection with some convenient properties.

We let $K[x_1, x_2, x_3]_{\leq D} \subset K[x_1, x_2, x_3]$ be the space of polynomials of degree at most D . We will sometimes abbreviate this space as $K[x]_{\leq D}$. The space $K[x]_{\leq D}$ is a vector space of dimension $\binom{D+3}{3}$. We choose an identification of $K[x]_{\leq D}$ with $K^{\binom{D+3}{3}}$.

We use the variable α to denote an element of $K[x]_{\leq D}^2$, and we write

$$\alpha = (P_\alpha, Q_\alpha) \in K[x]_{\leq D}^2 = \left(K^{\binom{D+3}{3}} \right)^2.$$

Given an irreducible curve γ , we look for a choice of $\alpha \in K[x]_{\leq D}^2$ so that $\gamma \subset Z(P_\alpha) \cap Z(Q_\alpha)$ and where P_α and Q_α have some other nice properties.

One useful property has to do with regular points. Recall that a point $x \in \gamma$ is called regular (or smooth) if there are two polynomials $f_1, f_2 \in I(\gamma)$ so that $\nabla f_1(x)$ and $\nabla f_2(x)$ are linearly independent (cf. [7] Chapter 14, page 174.) If x is a regular point, then we will want to choose α so that $\nabla P_\alpha(x)$ and $\nabla Q_\alpha(x)$ are linearly independent. We formalize these properties in a definition.

Definition 4.1. *Let $\gamma \in \mathcal{C}_{3,D}$. We say that a point $\alpha \in \left(K^{\binom{D+3}{3}} \right)^2$ is associated to γ if $\gamma \subset Z(P_\alpha) \cap Z(Q_\alpha)$. If $x \in \gamma$ is a regular point of γ , we say that α is associated to γ at x if α is associated to γ and $\nabla P_\alpha(x)$ and $\nabla Q_\alpha(x)$ are linearly independent.*

Finally, given a surface $Z = Z(T) \subset K^3$, with γ not contained in Z , we would like to choose P_α and Q_α so that $Z \cap Z(P_\alpha) \cap Z(Q_\alpha)$ is 0-dimensional. The following Lemma says that we can choose $\alpha \in K[x]_{\leq D}$ with all these good properties:

Lemma 4.2 (Trapping a curve in a complete intersection). *Let $Z = Z(T) \subset K^3$ be a surface. Let $\gamma \in \mathcal{C}_{3,D}$. If γ is not contained in Z , then there exists $\alpha \in \left(K^{\binom{D+3}{3}} \right)^2$ associated to γ so that $Z \cap Z(P_\alpha) \cap Z(Q_\alpha)$ is 0 dimensional. We say that α is associated to γ and adapted to Z .*

Moreover, if $x \in \gamma$ is a regular point, we can also arrange that α is associated to γ at x .

Proof. Suppose $w \in K^3 \setminus 0$. Let w^\perp be the two-plane passing through 0 orthogonal to w , i.e. w^\perp has the defining equation $\{x \cdot w = 0\}$. Let $\pi_w : K^3 \rightarrow w^\perp$ be the orthogonal projection ($\pi_w(x) = x - (x \cdot w)w$). For $x \in K^3$, let $L_{x,w} = \{x + aw : a \in K\}$ be the line in K^3 passing through the point x and pointing in the direction w . The fibers of the map π_w are lines of the form $L_{x,w}$.

If $\zeta \subset K^3$ is a curve, then $\pi_w(\zeta) \subset w^\perp$ is a constructible set of dimension at most 1. For a generic w , ζ does not contain any line of the form $L_{x,w}$, and in this case, $\pi_w(\zeta)$ is infinite and so $\pi_w(\zeta)$ is a constructible set of dimension 1: a curve with a finite set of points removed.

We can find the polynomials P_1, P_2 in the following way. We pick two vectors $w_1, w_2 \in K^3$, and we consider $\pi_{w_i}(\gamma)$. We let the Zariski-closure of $\pi_{w_i}(\gamma)$ be $Z(p_i)$, where p_i is a polynomial on w_i^\perp . Then we let $P_i = p_i \circ \pi_{w_i}$ be the corresponding polynomial on K^3 . It follows immediately that $\gamma \subset Z(P_1) \cap Z(P_2)$. For a generic choice of w_1, w_2 , we will see that the pair of polynomials (P_1, P_2) has all the desired properties.

First we discuss the degree of P_1 and P_2 . For generic vectors w_i , the degree of each polynomial p_i is equal to the degree of γ . This happens because the degree of p_i is equal to the number of intersection points between $\pi_{w_i}(\gamma)$ with a generic line in w_i^\perp and the degree of γ is equal to the number of intersection points between γ and a generic plane in K^3 . (cf. Chapter 18 of [7], pages 224-225.) But for a line $\ell \subset w_i^\perp$, the number of intersection points between $\pi_{w_i}(\gamma)$ and the line ℓ is equal to the number of intersection points between γ and the plane $\pi_{w_i}^{-1}(\ell)$.

For any given surface $Z = Z(T)$, we check that for a generic choice of w_i , $Z(P_i) \cap Z$ is 1-dimensional. Suppose that $Z' \subset Z \cap Z(P_i)$ is a 2-dimensional surface: so Z' is an irreducible component of Z and of $Z(P_i)$. If $x \in Z'$, then the line L_{x,w_i} must lie in Z' also. In particular, w_i must lie in the tangent space $T_x Z'$. But each component Z' of Z must contain a smooth point x ,

and a generic vector w_i does not lie in $T_x Z'$. So for a generic pair of vectors w_1, w_2 , the pairwise intersections $Z \cap Z(P_1)$, $Z \cap Z(P_2)$, and $Z(P_1) \cap Z(P_2)$ are all 1-dimensional.

Next we consider the triple intersection $Z \cap Z(P_1) \cap Z(P_2)$. Let ζ_1 be the curve $Z \cap Z(P_1)$. Suppose γ is not contained in Z . The curve ζ_1 has irreducible components $\zeta_{1,1}, \zeta_{1,2}, \dots, \zeta_{1,\ell}$, none of which is γ . For a generic choice of w_2 , the curves $\pi_{w_2}(\zeta_{1,j})$ and $\pi_{w_2}(\gamma)$ intersect properly (in a 0-dimensional subset of w_2^\perp). Therefore, $Z(P_2)$, the Zariski closure of $\pi_{w_2}(\gamma)$, does not contain any of the images $\pi_{w_2}(\zeta_{1,j})$. Hence $Z(P_2)$ does not contain any of the curves $\zeta_{1,j}$, and so $Z \cap Z(P_1) \cap Z(P_2)$ is 0-dimensional.

Now suppose that $x \in \gamma$ is a smooth point of γ . For a generic choice of w_i , $\pi_{w_i}(x)$ will be a smooth point of $\pi_{w_i}(\gamma)$. In this situation, $\nabla P_i(\pi_{w_i}(x)) \neq 0$, and so $\nabla P_i(x) \neq 0$. Let v be a non-zero vector in $T_x(\gamma)$. The vector $\nabla P_i(x)$ must be perpendicular to v (because $\gamma \subset Z(P_i)$), and it must be perpendicular to w_i (because the line $L_{x,w_i} \subset Z(P_i)$). Therefore, $\nabla P_i(x)$ is a (non-zero) multiple of the cross-product $w_i \times v$. If we also assume that w_1, w_2 and v are linearly independent, then it follows that $\nabla P_1(x)$ and $\nabla P_2(x)$ are linearly independent, and so $\nabla P_1(x) \times \nabla P_2(x) \neq 0$. \square

The choice of α in the Lemma above is not unique, and we also want to keep track of the set of α with various good properties.

Let

$$G := \{(x, \alpha) \in K^3 \times (K^{\binom{D+3}{3}})^2 : P_\alpha(x) = Q_\alpha(x) = 0, \nabla P_\alpha(x) \times \nabla Q_\alpha(x) \neq 0\}. \quad (2)$$

This is a constructible set of complexity $O_D(1)$.

Lemma 4.3. *The sets*

$$\{(\gamma, \alpha) \in \mathcal{C}_{3,D} \times (K^{\binom{D+3}{3}})^2 : \gamma \subset Z(P_\alpha) \cap Z(Q_\alpha)\}, \quad (3)$$

$$\{(x, \gamma, \alpha) \in K^3 \times \mathcal{C}_{3,D} \times (K^{\binom{D+3}{3}})^2 : (x, \alpha) \in G, \gamma \subset Z(P_\alpha) \cap Z(Q_\alpha)\} \quad (4)$$

are constructible and have complexity $O_D(1)$.

Proof. The proof uses the fact that constructible sets are a Boolean algebra as well as Chevalley's theorem, Theorem 2.4.

The following sets are constructible of complexity $O_D(1)$:

$$\begin{aligned} & \{(x, \gamma) \in K^3 \times \mathcal{C}_{3,D} : x \in \gamma\} \quad (\text{by Proposition 3.1}), \\ & \{(x, \alpha) \in K^3 \times (K^{\binom{D+3}{3}})^2 : P_\alpha(x) = Q_\alpha(x) = 0\}, \\ & \{(x, \alpha) \in K^3 \times (K^{\binom{D+3}{3}})^2 : (P_\alpha(x) \neq 0 \text{ or } Q_\alpha(x) \neq 0)\}, \\ & \{(x, \gamma, \alpha) \in K^3 \times \mathcal{C}_{3,D} \times (K^{\binom{D+3}{3}})^2 : x \in \gamma, P_\alpha(x) \neq 0 \text{ or } Q_\alpha(x) \neq 0\}. \end{aligned} \quad (5)$$

Let $\pi: (x, \gamma, \alpha) \mapsto (\gamma, \alpha)$. Then

$$\pi((5)) = \{(\gamma, \alpha) \in \mathcal{C}_{3,D} \times (K^{\binom{D+3}{3}})^2 : \gamma \not\subset Z(P_\alpha) \cap Z(Q_\alpha)\}, \quad (6)$$

so

$$(3) = \left(\mathcal{C}_{3,D} \times (K^{\binom{D+3}{3}})^2 \right) \setminus (6)$$

is constructible of complexity $O_D(1)$.

Finally,

$$(4) = \left(K^3 \times (3) \right) \cap \{(x, \gamma, \alpha) \in K^3 \times \mathcal{C}_{3,D} \times (K^{\binom{D+3}{3}})^2 : (x, \alpha) \in G\}$$

is constructible of complexity $O_D(1)$. \square

5 Local Rings, Intersection multiplicity and Bézout

5.1 Local rings

Definition 5.1. For $z \in K^N$, let $\mathcal{O}_{K^N, z}$ be the local ring of K^N at z . This is the ring of rational functions of the form $p(x)/q(x)$, where $q(z) \neq 0$.

There is a natural map $\iota: K[x_1, \dots, x_N] \rightarrow \mathcal{O}_{K^N, z}$ which sends $f \mapsto f/1$. This map is an injection.

Definition 5.2. If $I \subset K[x_1, \dots, x_N]$ is an ideal, let $I_z \subset \mathcal{O}_{K^N, z}$ be the localization of I at z ; this is the ideal in $\mathcal{O}_{K^N, z}$ generated by $\iota(I)$.

Lemma 5.3. If $Z \subset K^N$ is an affine variety and if $z \notin Z$, then $I(Z)_z = \mathcal{O}_{K^N, z}$.

Proof. Since $z \notin Z$, there is a function $f \in I(Z)$ which is non-zero at z . Then the element $f/1 \in I(Z)_z$ is a unit. \square

Lemma 5.4. Let $Z \subset K^N$ be an affine variety. Suppose that Y is an irreducible component of Z and $z \in Y$ is a regular point of Z . Then $I(Y)_z = I(Z)_z$.

Proof. Write $Z = Y \cup Z_1 \cup \dots \cup Z_\ell$ as a union of irreducible components. We get a corresponding decomposition $I(Z)_z = I(Y)_z \cap I(Z_1)_z \cap \dots \cap I(Z_\ell)_z$. Since z is a regular point of Z , for each index j we have $z \notin Z_j$ and thus by Lemma 5.3, $I(Z_j)_z = \mathcal{O}_{K^N, z}$. Thus $I(Z)_z = I(Y)_z$. \square

5.2 The Bézout theorem

In the paper, we will need a few variations of the Bézout theorem. One of the versions involves the multiplicity of the intersection of hypersurfaces $Z(f_1) \cap \dots \cap Z(f_N)$. We start by defining this multiplicity.

Given polynomials f_1, \dots, f_N , we define the (length) intersection multiplicity of f_1, \dots, f_N at z to be

$$\text{mult}_z(f_1, \dots, f_N) = \dim_K (\mathcal{O}_{K^N, z} / (f_1, \dots, f_N)_z). \quad (7)$$

Let us understand (7).

- $\mathcal{O}_{K^N, z}$ is the local ring of K^N at z .
- $(f_1, \dots, f_N)_z$ is the ideal in $\mathcal{O}_{K^N, z}$ generated by (f_1, \dots, f_N) . I.e. it is the set of elements of $\mathcal{O}_{K^N, z}$ which can be written $a_1 f_1 + \dots + a_N f_N$, with $a_1, \dots, a_N \in \mathcal{O}_{K^N, z}$.
- $\mathcal{O}_{K^N, z} / (f_1, \dots, f_N)_z$ is the set of equivalence classes of elements in $\mathcal{O}_{K^N, z}$ where $\bar{g} \sim \bar{g}'$ if $g - g' \in (f_1, \dots, f_N)_z$. This set of equivalence classes forms a ring.
- $\dim_K(\cdot)$ is the dimension of the ring $\mathcal{O}_{K^N, z} / (f_1, \dots, f_N)_z$ when it is considered as a K -vector space. Later, $\dim(\cdot)$ (without the subscript) will be used to denote the dimension of an algebraic variety or constructible set.

If $z \in Z(f_1) \cap \dots \cap Z(f_N)$, then the multiplicity $\text{mult}_z(f_1, \dots, f_N)$ is always at least 1. Later, we will show that the multiplicity of certain intersections is large. To do this, we need to find many linearly independent elements of $\mathcal{O}_{K^N, z} / (f_1, \dots, f_N)_z$. Polynomials $g_1(x), \dots, g_\ell(x)$ are linearly dependent in $\mathcal{O}_{K^N, z} / (f_1, \dots, f_N)_z$ if we can write

$$\sum_{i=1}^{\ell} c_i g_i(x) = a_1(x) f_1(x) + \dots + a_N(x) f_N(x), \quad (8)$$

where $c_1, \dots, c_\ell \in K$; at least one c_i is non-zero; and $a_1(x), \dots, a_N(x) \in \mathcal{O}_{K^N, z}$, i.e. $a_1(x), \dots, a_N(x)$ are rational functions of the form $p(x)/q(x)$ with $q(z) \neq 0$.

If no expression of the form (8) holds for g_1, \dots, g_ℓ , then g_1, \dots, g_ℓ are *linearly independent*.

We can now state the first version of Bézout's theorem that we will use.

Theorem 5.5 (Bézout's theorem for surfaces in K^3). *Let $Z_1 = Z(f_1), Z_2 = Z(f_2), Z_3 = Z(f_3)$ be surfaces in K^3 . Suppose that $Z_1 \cap Z_2 \cap Z_3$ is zero-dimensional (i.e. finite). Then*

$$\sum_{z \in Z_1 \cap Z_2 \cap Z_3} \text{mult}_z(f_1, f_2, f_3) \leq (\deg f_1)(\deg f_2)(\deg f_3). \quad (9)$$

This is a special case of [2, Proposition 8.4]. Specifically, see Equation (3) on p145.

We will also need a version of Bézout's theorem that bounds the number of (distinct) intersection points between a curve and a surface in K^3 .

Theorem 5.6 (Bézout's theorem for curves and surfaces in K^3 ; see [2], Theorem 12.3). *Let $Z \subset K^3$ be a surface and let $\gamma \subset K^3$ be an irreducible curve. Then either $\gamma \subset Z$ or γ intersects Z in at most $(\deg \gamma)(\deg Z)$ distinct points.*

Finally, we will need a version of Bézout's theorem that bounds the number of curves in the intersection between two surfaces in K^3 .

Theorem 5.7. *Suppose that $f_1, f_2 \in K[x_1, x_2, x_3]$. If f_1 and f_2 have no common factor, then the number of irreducible curves in $Z(f_1) \cap Z(f_2)$ is at most $(\deg f_1)(\deg f_2)$.*

Proof. We will prove this result using Theorem 5.5. Suppose that $\{\gamma_i\}_{i=1, \dots, M}$ is a finite set of irreducible curves in $Z(f_1) \cap Z(f_2)$. We want to show that $M \leq (\deg f_1)(\deg f_2)$. If π is a generic plane in K^3 , then π will intersect each of the curves γ_i (cf. [7] Corollary 3.15). There are only finitely many points that lie in at least two of the curves γ_i , and a generic plane π will avoid all of those points. Therefore, $|\pi \cap Z(f_1) \cap Z(f_2)| \geq M$. Let f_3 be a polynomial of degree 1 with $Z(f_3) = \pi$.

Since f_1 and f_2 have no common factor, $Z(f_1) \cap Z(f_2)$ must have dimension 1. Then for a generic plane π , $Z(f_1) \cap Z(f_2) \cap Z(f_3)$ has dimension zero, so we can apply the Bézout theorem, Theorem 5.5. In this way we see that,

$$\begin{aligned} M \leq |Z(f_1) \cap Z(f_2) \cap Z(f_3)| &\leq \sum_{z \in Z_1 \cap Z_2 \cap Z_3} \text{mult}_z(f_1, f_2, f_3) \leq \\ &\leq (\deg f_1)(\deg f_2)(\deg f_3) = (\deg f_1)(\deg f_2). \end{aligned}$$

□

6 Curve-surface tangency

In this section, we will define what it means for a curve to be tangent to a surface to order r . A precise definition will be given in Section 6.2.

As a warmup, suppose that the curve γ is the x_1 -axis. In this case, we could make the definition that γ is tangent to the surface $Z(T)$ at the origin to order at least r if and only if

$$\frac{\partial^j T}{\partial x_1^j}(0) = 0 \text{ for } j = 0, \dots, r.$$

The definition we give will be equivalent to this one in the special case that γ is the x_1 -axis. One of our goals is to extend this definition to any regular point x in any curve γ . To do so, we define a version of “differentiating along the curve γ ” in Subsection 6.1. In the following subsection, we give two other definitions of being tangent to order r , and we show that all the definitions are equivalent.

Throughout the section, we will restrict to the case that $r < \text{char } K$. To see why, suppose again that γ is the x_1 -axis, and consider the polynomial $T = x_2 - x_1^p$ for $p = \text{char } K$. For this choice of T , $\frac{\partial^j T}{\partial x_1^j}(0) = 0$ for all j . Nevertheless, it does not seem correct to say that the x_1 -axis is tangent to $Z(T)$ to infinite order, and with our other definitions of tangency, the x_1 -axis is not tangent to $Z(T)$ to infinite order. To avoid these issues, we restrict throughout this paper to the case $r < \text{char } K$.

6.1 Differentiating along a curve

Recall the definition of $P_\alpha(x)$ and $Q_\alpha(x)$ from Section 4. Here and throughout this section, $\nabla = \nabla_x = (\partial_{x_1}, \partial_{x_2}, \partial_{x_3})$ denotes the gradient in the x variable.

We define a differential operator D_α . For any f , we define

$$D_\alpha f(x) := (\nabla P_\alpha(x) \times \nabla Q_\alpha(x)) \cdot \nabla f(x). \quad (10)$$

This is well-defined for $f \in K[x_1, x_2, x_3]$, and in this case, $D_\alpha f \in K[x_1, x_2, x_3]$. The operator D_α also makes sense a little more generally: if f is a rational function, then $D_\alpha f$ is a rational function as well.

The intuition behind D_α is the following. If $\gamma \subset Z(P_\alpha) \cap Z(Q_\alpha)$, and $x \in \gamma$ is a point where $\nabla P_\alpha(x) \times \nabla Q_\alpha(x) \neq 0$, then $\nabla P_\alpha(x) \times \nabla Q_\alpha(x)$ is tangent to γ , and so $D_\alpha f(x)$ is a derivative of f in the tangent direction to γ .

We let $D_\alpha^2 f$ be shorthand for $D_\alpha(D_\alpha f)$, and we define the higher iterates $D_\alpha^j f$ in a similar way.

Note that $D_\alpha P_\alpha$ and $D_\alpha Q_\alpha$ are identically 0 (as functions of α and x). Thus $(D_\alpha^j P_\alpha)(x) = 0$ and $(D_\alpha^j Q_\alpha)(x) = 0$ for all $j \geq 1$. If $P_\alpha(x) = 0$ and $Q_\alpha(x) = 0$, then $(D_\alpha^j P_\alpha)(x) = 0$ and $(D_\alpha^j Q_\alpha)(x) = 0$ for all $j \geq 0$.

We also observe that $D_\alpha(x)$ obeys the Leibniz rule. In particular, if $f(x)$, $g(x)$ are polynomials or rational functions, then

$$D_\alpha(fg)(x) = (D_\alpha f)(x) g(x) + f(x) (D_\alpha g)(x). \quad (11)$$

As a corollary, we have the following result.

Lemma 6.1. *Let $T \in K[x_1, x_2, x_3]$ and suppose $(D_\alpha^j T)(x) = 0$, $j = 0, \dots, r$. Then for any rational function b with $b(x) \neq \infty$, we have $D_\alpha^j(bT)(x) = 0$, $j = 0, \dots, r$.*

6.2 Defining curve-surface tangency

Definition 6.2. *For $z \in K^3$ and $r \geq 0$, let $I_{z, \geq r}$ be the ideal of polynomials in $K[x_1, x_2, x_3]$ that vanish at z to order $\geq r$.*

For example, if $z = 0$, then $I_{z, \geq r}$ is the ideal generated by the monomials of degree r .

Definition 6.3. *Let $T \in K[x_1, x_2, x_3]$. Let $\gamma \subset K^3$ be an irreducible curve and let $z \in \gamma$ be a regular point of γ . Let $r < \text{char}(K)$. We say that γ is tangent to $Z(T)$ at z to order $\geq r$ if $T/1 \in (I(\gamma))_z + (I_{z, \geq r+1})_z$.*

Remark 6.4. Definition 6.3 abuses notation slightly, since γ being tangent to $Z(T)$ depends on the polynomial T , not merely its zero-set $Z(T)$. This would be a natural place to use the language of schemes, but we will refrain from doing so to avoid introducing more notation.

For example, the x -axis is tangent to the surface $y = x^{r+1}$ at the origin to order r .

We now show that this definition is equivalent to several other definitions. In particular, we will see that being tangent to order r can also be defined using the tangential derivatives D_α .

Theorem 6.5. Let $T \in K[x_1, x_2, x_3]$. Let $\gamma \subset K^3$ be an irreducible curve and let $z \in \gamma$ be a regular point of γ . Let $r < \text{char}(K)$. Suppose that α is associated to γ at z as in Definition 4.1. Then the following are equivalent:

- (i) γ is tangent to $Z(T)$ at z to order $\geq r$. I.e. $T/1 \in (I(\gamma))_z + (I_{z, \geq r+1})_z$.
- (ii) $D_\alpha^j T(z) = 0$, $j = 0, \dots, r$.
- (iii) $T \in I(\gamma) + I_{z, \geq r+1}$.

Before we prove the theorem, we note the following consequence. Condition (ii) depends on the choice of α , but the other conditions don't. Therefore, we get the following corollary:

Corollary 6.6. Let $T \in K[x_1, x_2, x_3]$. Let $\gamma \subset K^3$ be an irreducible curve and let $z \in \gamma$ be a regular point of γ . Let $r < \text{char}(K)$.

Suppose that there exists one α associated to γ at z so that $D_\alpha^j T(z) = 0$, $j = 0, \dots, r$. Then for every α associated to γ at z , $D_\alpha^j T(z) = 0$, $j = 0, \dots, r$.

Proof of Theorem 6.5. We will prove that (iii) \implies (i) \implies (ii) \implies (iii). It is straightforward to see that (iii) \implies (i): just localize both ideals at z .

(i) \implies (ii): First, note that if α is associated to γ at z , then by Lemma 5.4, $I(\gamma)_z = (P_\alpha, Q_\alpha)_z$. In particular, if $T \in (I(\gamma))_z + (I_{z, \geq r+1})_z$ then $T = AP_\alpha + BQ_\alpha + C$, where $A, B \in \mathcal{O}_{K^3, z}$ and $C \in (I_{z, \geq r+1})_z$. By Lemma 6.1 (and the observation that $(D_\alpha^j P_\alpha)(z) = 0$ and $(D_\alpha^j Q_\alpha)(z) = 0$ for all $j \geq 0$), we conclude that $D_\alpha^j(T) = 0$, $j = 0, \dots, r$.

(ii) \implies (iii): Consider the map

$$\begin{aligned} E: K[x_1, x_2, x_3] &\rightarrow K^{r+1}, \\ T &\mapsto (T(z), D_\alpha T(z), \dots, D_\alpha^r T(z)). \end{aligned}$$

(Here z was specified in the statement of Theorem 6.5). E is a linear map. By Corollary 6.1, (P_α, Q_α) is in the kernel of E . $I_{z, \geq r+1}$ is also in the kernel of E . Let $V := K[x_1, x_2, x_3]/((P_\alpha, Q_\alpha) + I_{z, \geq r+1})$. Then $\tilde{E}: V \rightarrow K^{r+1}$ is well-defined.

We will show that \tilde{E} is an isomorphism. By (ii), T is in the kernel of E . Since \tilde{E} is an isomorphism, we see that

$$T \in (P_\alpha, Q_\alpha) + I_{z, \geq r+1} \subset I(\gamma) + I_{z, \geq r+1}.$$

This will show that (ii) \implies (iii). It only remains to check that \tilde{E} is an isomorphism. To do this, we will show that E is surjective and we will show that $\dim_K(V) \leq \dim_K(K^{r+1}) = r + 1$.

Since α is associated to γ at z , $\nabla P_\alpha(z) \times \nabla Q_\alpha(z) \neq 0$. Without loss of generality we can assume that $(1, 0, 0) \cdot \nabla P_\alpha(z) \times \nabla Q_\alpha(z) \neq 0$ (indeed, if this fails then we can replace $(1, 0, 0)$ with $(0, 1, 0)$ or $(0, 0, 1)$, and permute indices accordingly).

Lemma 6.7. Let $\sigma(x) = \pi_1(x - z)$, where $\pi_1: K^3 \rightarrow K$ is the projection to the first coordinate. Then for any $j < \text{char } K$, $(D_\alpha^i \sigma^j)(z) = 0$, $i = 0, \dots, j - 1$, and $(D_\alpha^j \sigma)(z) \neq 0$.

Proof. We can expand $D_\alpha^i \sigma^j$ using the Leibniz rule. If $i < j$, then every term in the expansion will contain a factor of the form $(\pi_1(x - z))^{j-i}$, which evaluates to 0 when $x = z$.

Conversely, we have

$$D_\alpha^j \sigma^j(x) = (\pi_1(\nabla P_\alpha(x) \times \nabla Q_\alpha(x)))^j j! + \text{terms containing a factor of the form } \pi_1(x - z).$$

Evaluating at $x = z$, we conclude

$$\begin{aligned} D_\alpha^j \sigma^j(z) &= (\pi_1(\nabla P_\alpha(z) \times \nabla Q_\alpha(z)))^j j! \\ &\neq 0. \end{aligned}$$

Here we used the assumption that $j < \text{char}(K)$, so $j! \neq 0$, and the assumption that $\pi_1(\nabla P_\alpha(z) \times \nabla Q_\alpha(z)) \neq 0$, so $(\pi_1(\nabla P_\alpha(z) \times \nabla Q_\alpha(z)))^j \neq 0$. \square

Lemma 6.7 implies that the $(r + 1) \times (r + 1)$ matrix

$$\begin{bmatrix} E(1) \\ E(\sigma) \\ E(\sigma^2) \\ \vdots \\ E(\sigma^r) \end{bmatrix}$$

is upper-triangular and has non-zero entries on the diagonal. In particular, E is surjective, and so \tilde{E} is surjective.

It remains to check that $\dim_K(V) \leq r + 1$. Since $\nabla P_\alpha(z) \times \nabla Q_\alpha(z) \neq 0$, $\nabla P_\alpha(z)$ and $\nabla Q_\alpha(z)$ are linearly independent (and in particular, both are non-zero). Thus after a linear change of coordinates, we can assume that z is the origin, $P(x_1, x_2, x_3) = x_2 + P^*(x_1, x_2, x_3)$, and $Q(x_1, x_2, x_3) = x_3 + Q^*(x_1, x_2, x_3)$, with $P^*, Q^* \in I_{z, \geq 2}$.

We will study the successive quotients $I_{z, \geq s} / I_{z, \geq s+1}$. We note that $I_{z, \geq s} / I_{z, \geq s+1}$ is isomorphic (as a vector space) to the homogeneous polynomials of degree s .

Lemma 6.8. For any s ,

$$\frac{(P, Q) \cap I_{z, \geq s}}{I_{z, \geq s+1}} \supseteq \frac{(x_2, x_3) \cap I_{z, \geq s}}{I_{z, \geq s+1}}.$$

Proof. . Suppose that $R \in (x_2, x_3) \cap I_{z, \geq s}$. Since (x_2, x_3) is a homogeneous ideal, the degree s part of R must lie in (x_2, x_3) , and so we get

$$R = R_2 x_2 + R_3 x_3 + R',$$

where R_2, R_3 are homogeneous polynomials of degree $s - 1$, and $R' \in I_{z, \geq s+1}$. Therefore, $R = R_2 P + R_3 Q + R''$, where $R'' \in I_{z, \geq s+1}$. \square

Therefore, we see that

$$\dim \frac{(P, Q) \cap I_{z, \geq s}}{I_{z, \geq s+1}} \geq \dim \frac{(x_2, x_3) \cap I_{z, \geq s}}{I_{z, \geq s+1}} = \dim \frac{I_{z, \geq s}}{I_{z, \geq s+1}} - 1.$$

These dimensions are sufficient to reconstruct $\dim V$. We write $(P, Q)_{\geq s}$ for $I_{z, \geq s} \cap (P, Q)$. We first note that

$$\dim V = \dim \frac{I_{z, \geq 0}}{(P, Q) + I_{z, \geq r+1}} = \sum_{s=0}^r \dim \frac{I_{z, \geq s}}{(P, Q)_{\geq s} + I_{z, \geq s+1}}. \quad (12)$$

Next, we note the short exact sequence

$$\frac{(P, Q)_{\geq s}}{I_{z, \geq s+1}} \rightarrow \frac{I_{z, \geq s}}{I_{z, \geq s+1}} \rightarrow \frac{I_{z, \geq s}}{(P, Q)_{\geq s} + I_{z, \geq s+1}}.$$

Using Lemma 6.8 and this short exact sequence, we see that

$$\dim \frac{I_{z, \geq s}}{(P, Q)_{\geq s} + I_{z, \geq s+1}} \leq 1.$$

Plugging this estimate into equation 12, we get

$$\dim V = \dim \frac{I_{z, \geq 0}}{(P, Q) + I_{z, \geq r+1}} \leq \sum_{s=0}^r 1 = r + 1.$$

□

7 Curve-surface tangency and intersection multiplicity

In this section we will show that if a curve γ is tangent to $Z(T)$ at z to order $\geq r$, then the varieties $Z(T)$ and γ intersect at z with high multiplicity. We defined the intersection multiplicity for a complete intersection in Section 5.2. For a curve γ , we consider a complete intersection $Z(P_\alpha) \cap Z(Q_\alpha) \supset \gamma$, where α is associated to γ at z and adapted to Z (see Definition 4.1 and Lemma 4.2).

Lemma 7.1. *Let $T \in K[x_1, x_2, x_3]$, $\gamma \in \mathcal{C}_{3,D}$, and $z \in K^3$. Suppose that z is a regular point of γ and $\gamma \not\subset Z(T)$. Let $r \leq \text{char}(K)$ and suppose that γ is tangent to $Z(T)$ at z to order $\geq r$.*

Then for any α that is associated to γ at z and adapted to $Z(T)$, we have

$$\text{mult}_z(P_\alpha, Q_\alpha, T) \geq r + 1. \quad (13)$$

Before we prove Lemma 7.1, we will state a key corollary

Corollary 7.2 (Very very tangent implies trapped). *Let $T \in K[x_1, x_2, x_3]$, $\gamma \in \mathcal{C}_{3,D}$, and $z \in K^3$. Suppose that $D^2(\deg T) < \text{char}(K)$ and z is a regular point of γ . Suppose that γ is tangent to $Z(T)$ at z to order $\geq D^2(\deg T)$. Then $\gamma \subset Z(T)$.*

Proof of Corollary 7.2. Suppose $\gamma \not\subset Z(T)$. Let α be associated to γ at z and adapted to $Z(T)$, as in Definition 4.1 and Lemma 4.2. In particular, $Z(T) \cap Z(P_\alpha) \cap Z(Q_\alpha)$ is a zero-dimensional set. Lemma 4.2 also guarantees that P_α and Q_α have degree at most D . By Lemma 7.1, $\text{mult}_z(P_\alpha, Q_\alpha, T) > D^2(\deg T)$. But this contradicts Bézout's theorem (Theorem 5.5). Thus we must have $\gamma \subset Z(T)$. □

Proof of Lemma 7.1. By Theorem 6.5, we have $D_\alpha^j T(z) = 0$, $j = 0, \dots, r$. We also have $D_\alpha^j P_\alpha(z) = 0$ and $D_\alpha^j Q_\alpha(z) = 0$ for all $j \geq 0$.

Lemma 7.3. *Let $\sigma(x) = \pi_1(x - z)$, as in Lemma 6.7. $1, \sigma(x), \dots, \sigma^r(x)$ are linearly independent elements of $\mathcal{O}_{K^3, z}/(P_\alpha, Q_\alpha, T)_z$.*

Proof. Suppose this was not the case. Then recalling (8), there must exist a linear dependence relation of the form

$$\sum_{i=0}^r d_i \sigma(x)^i = a(x)P_\alpha(x) + b(x)Q_\alpha(x) + c(x)T(x), \quad (14)$$

where $a(x), b(x), c(x)$ are rational functions of x that are not ∞ when $x = z$, and $\{d_i\}$ are elements of K , not all of which are 0.

Let j be the smallest index so that $d_j \neq 0$. Then, using Lemma 6.7, we get

$$\begin{aligned} D_\alpha^j \left(\sum_{i=0}^{r-1} d_i \sigma(z)^i \right) &= D_\alpha^j (d_j \sigma(z)^j) + \sum_{j < i \leq r-1} D_\alpha^j (d_i \sigma(z)^i) \\ &= D_\alpha^j (d_j \sigma(z)^j) \\ &\neq 0. \end{aligned}$$

On the other hand,

$$D_\alpha^j (aP_\alpha)(z) + D_\alpha^j (bQ_\alpha)(z) + D_\alpha^j (cT)(z) = 0,$$

which is again a contradiction. Thus (14) cannot hold. \square

From Lemma 7.3, we conclude that

$$\dim (\mathcal{O}_{K^3, z}/(P_\alpha, Q_\alpha, T)_z) \geq r + 1. \quad (15)$$

Lemma 7.1 now follows from the definition of multiplicity from (7). \square

8 Sufficiently tangent implies trapped

Theorem 8.1. *Let $D \geq 0$. Then there exists $c_1 > 0$ (small) and r_0 (large) so that the following holds. Let K be a closed field and let $T \in K[x_1, x_2, x_3]$ be an irreducible polynomial with $\deg T < c_1 \text{char}(K)$. Then there is a (non-empty) open subset $O \subset Z(T)$ with the following property: if $\gamma \subset K^3$ is an irreducible curve of degree at most D , $z \in O$ is a regular point of γ , and γ is tangent to $Z(T)$ at z to order $\geq r_0$, then $\gamma \subset Z(T)$.*

Remark 8.2. *For example, suppose $K = \mathbb{C}$, $D = 1$ (so γ is a line), and $T = x_1 - x_2^u$, where u is a very large integer (much larger than r_0). Then $O \subset Z(T)$ is the compliment of the set $\{x_1 = 0, x_2 = 0\}$. We will not calculate the value of r_0 corresponding to $D = 1$; however, any number $r_0 \geq 2$ would suffice in this case.*

At any point $z \in Z(T) \setminus O$, if γ is a line tangent to $Z(T)$ at z to order ≥ 2 , then $\gamma \subset Z(T)$. The only such lines are lines of the form $x_1 = a_1; x_2 = a_2$ for some (a_1, a_2) satisfying $a_1 - a_2^u = 0$. On the other hand, any line passing through a point in $\{x_1 = 0, x_2 = 0\}$ and tangent to the 2-plane $x_1 \cdot z = 0$, is tangent to Z to order $u \gg r_0$. Most of these lines will not be contained in Z . This does not contradict the proposition, since $\{x_1 = 0, x_2 = 0\}$ lies outside the set O .

8.1 Defining the tangency functions

Let $T \in K[x_1, x_2, x_3]$ be an irreducible polynomial. Recall that $\alpha \in (K^{\binom{D+3}{3}})^2$ parameterizes pairs of polynomials (P_α, Q_α) of degree at most D , as described in Section 4.

For each $j \geq 0$, define

$$h_j(\alpha, x) := (D_\alpha^j T)(x) \in K[\alpha, x] \quad (16)$$

Lemma 8.3 (Properties of the functions $h_{j,\alpha}$). *The polynomials h_j defined above have the following properties.*

(i) $h_j(\alpha, x)$ is a polynomial in α and x . Its degree in α is $O_j(1)$, and its degree in x is at most $\deg T < c_1 \operatorname{char}(K)$.

(ii) $h_0(\alpha, x) = T(x)$.

(iii) Let γ be an irreducible curve of degree at most D . If z is a regular point of γ , α is associated to γ at z , and $r < \operatorname{char}(K)$, then γ is tangent to $Z(T)$ at z to order r if and only if

$$h_j(\alpha, z) = 0 \quad \text{for } j = 0, \dots, r.$$

(iv) Let γ be an irreducible curve of degree at most D . If z is a regular point of γ , α is associated to γ at z , and

$$h_j(\alpha, z) = 0 \quad \text{for } j = 0, \dots, D^2(\deg T), \quad (17)$$

then $\gamma \subset Z$.

Proof. The first two properties follow immediately from the definition of h_j . The third property is Theorem 6.5. For the last property, (17) implies that γ is tangent to Z at z to order $\geq D^2(\deg T)$. By choosing $c_1(D)$ small enough, we can assume that $D^2 \deg T < \operatorname{char}(K)$. We now apply Corollary 7.2. \square

We would like to find an open set $O \subset Z(T)$ so that for $z \in O$, if $h_j(\alpha, z) = 0$ for j up to some r_0 , then $h_j(\alpha, z)$ is forced to vanish for many more j . This forcing comes from a quantitative version of the ascending chain condition.

8.2 A quantitative Ascending Chain condition

To set up the right framework to apply the ascending chain condition, we introduce the field of fractions of $Z(T)$.

Definition 8.4. Let

$$F_{Z(T)} = \left\{ p/q : p, q \in K[x_1, x_2, x_3]/(T), q \neq 0 \right\}$$

be the field of rational functions on $Z(T)$.

Let ρ_T be the map $K[x] \rightarrow F_{Z(T)}$. We also write ρ_T for the corresponding map $K[\alpha, x] \rightarrow F_{Z(T)}[\alpha]$.

Definition 8.5. Let $\tilde{h}_j = \rho_T(h_j) \in F_{Z(T)}[\alpha]$.

We note that \tilde{h}_j is a polynomial of degree $O_j(1)$ in the variable α .

Definition 8.6. Let \tilde{K} be a field, and let $I \subset \tilde{K}[y_1, \dots, y_N]$ be an ideal. We define

$$\text{complexity}(I) = \min(\deg f_1 + \dots + \deg f_\ell),$$

where the minimum is taken over all representations $I = (f_1, \dots, f_\ell)$.

Proposition 8.7. Let \tilde{K} be a field, let $N \geq 0$, and let $\tau: \mathbb{N} \rightarrow \mathbb{N}$ be a function. Then there exists a number M_0 with the following property. Let $\{I_i\}$ be a sequence of ideals in $\tilde{K}[y_1, \dots, y_N]$, with $\text{complexity}(I_i) \leq \tau(i)$. Then there exists a number $r_0 \leq M_0$ so that $I_{r_0} \in (I_1, \dots, I_{r_0-1})$.

To avoid interrupting the flow of the argument, we will defer the proof of this Proposition to Appendix A. We will use the following special case of Proposition 8.7, which we will state separately:

Corollary 8.8. Let \tilde{K} be a field, let $N \geq 0$, and let $\tau: \mathbb{N} \rightarrow \mathbb{N}$ be a function. Then there exists a number M_0 with the following property. Let $\{f_i\}$ be a sequence of polynomials in $\tilde{K}[y_1, \dots, y_N]$, with $\deg(f_i) \leq \tau(i)$. Then there exists a number $r_0 \leq M_0$ so that $f_{r_0} \in (f_1, \dots, f_{r_0-1})$.

Lemma 8.9. There exists a number r_0 which is bounded by some constant $C(D)$ and a sequence $\tilde{a}_i \in F_{Z(T)}[\alpha]$ so that we have the equality

$$\tilde{h}_{r_0} = \sum_{i=0}^{r_0-1} \tilde{a}_i \tilde{h}_i. \quad (18)$$

This equation holds in $F_{Z(T)}[\alpha]$.

Proof. This is Corollary 8.8 with $f_i = \tilde{h}_i(\alpha)$ and $\tau(i) = \deg \tilde{h}_i = O_i(1)$, $\tilde{K} = F_{Z(T)}$, $N = 2\binom{D+3}{3}$, and $y = \alpha$. \square

Our next goal is to rewrite equation 18 in terms of h_j instead of \tilde{h}_j . To do this, we recall the localization of $K[x]$ at T .

Definition 8.10. Let

$$K[x]_T := \left\{ p/q : p, q \in K[x_1, x_2, x_3], q \notin (T) \right\}.$$

$K[x]_T$ is called the localization of $K[x]$ at T . It is a ring.

The map $\rho_T: K[x] \rightarrow F_{Z(T)}$ extends in a natural way to a ring homomorphism $K[x]_T \rightarrow F_{Z(T)}$. It is surjective: given any $\tilde{p} \in K[x_1, x_2, x_3]/(T)$, and $0 \neq \tilde{q} \in K[x_1, x_2, x_3]/(T)$, we can pick representatives $p \in K[x_1, x_2, x_3]$ and $q \in K[x_1, x_2, x_3] \setminus (T)$, and then $p/q \in K[x]_T$ and $\rho_T(p/q) = \tilde{p}/\tilde{q} \in F_{Z(T)}$.

We write $K[x]_T[\alpha]$ for the ring of polynomials in α with coefficients in the ring $K[x]_T$. (Writing $K[x]_T[\alpha]$ looks a little funny because of all the brackets, but this is the standard notation: if R is a ring, then $R[\alpha]$ are the polynomials in α with coefficients in R , and our ring R is $K[x]_T$.) We also write ρ_T for the natural extension $K[x]_T[\alpha] \rightarrow F_{Z(T)}[\alpha]$, which is also surjective.

We note that $\rho_T(h_i) = \tilde{h}_i$. We pick $a_i \in K[x]_T[\alpha]$ so that $\rho_T(a_i) = \tilde{a}_i$. We can now rewrite Equation 18 in terms of h_i, a_i :

$$\rho_T \left(h_{r_0} - \sum_{i=0}^{r_0-1} a_i h_i \right) = 0.$$

The kernel of $\rho_T: K[x]_T[\alpha] \rightarrow F_{Z(T)}[\alpha]$ is the set

$$\{bT : b \in K[x]_T[\alpha]\}.$$

Therefore, we can choose $b \in K[x]_T[\alpha]$ so that

$$h_{r_0} = bT + \sum_{i=0}^{r_0-1} a_i h_i.$$

Finally, we recall that $T = h_0$. Therefore, after changing the definition of a_0 , we can arrange that

$$h_{r_0} = \sum_{i=0}^{r_0-1} a_i h_i. \quad (19)$$

In this equation, $r_0 \leq C(D)$, $a_i \in K[x]_T[\alpha]$, and the equation holds in $K[x]_T[\alpha]$.

8.3 Trapping the curves

Lemma 8.11. *Let the functions $\{h_i\}$ be as defined in (16), and suppose that (19) holds. Then for all $j = 0, 1, \dots$, we can choose $a_{i,j} \in K[x]_T[\alpha]$ so that*

$$h_j = \sum_{i=0}^{r_0-1} a_{i,j} h_i. \quad (20)$$

Proof. We will prove Lemma 8.11 by induction on j . The case $j \leq r_0 - 1$ is immediate. The case $j = r_0$ is precisely (19). Now assume the theorem has been proved up to some value j . To do the induction step, we will apply the operator D_α to the equation for j in order to get the equation for $j + 1$.

We note that the ring $K[x]_T$ is closed under the action of the partial derivatives ∂_i . Therefore, $K[x]_T[\alpha]$ is closed under the action of D_α . We will make liberal use of the Leibniz rule (11) for the operator D_α , which we recall here: for any $f, g \in K[x]_T[\alpha]$,

$$D_\alpha(fg) = (D_\alpha f)g + f(D_\alpha g).$$

We also recall that $D_\alpha h_j = h_{j+1}$. Therefore, we have

$$\begin{aligned} h_{j+1} &= D_\alpha h_j = D_\alpha \left(\sum_{i=0}^{r_0-1} a_{i,j} h_i \right) \\ &= \sum_{i=0}^{r_0-1} ((D_\alpha a_{i,j}) h_i + a_{i,j} (D_\alpha h_i)) \\ &= \sum_{i=0}^{r_0-1} (D_\alpha a_{i,j}) h_i + \sum_{i=0}^{r_0-2} a_{i,j} h_{i+1} + a_{r_0-1,j} h_{r_0} \\ &= \sum_{i=0}^{r_0-1} (D_\alpha a_{i,j}) h_i + \sum_{i=1}^{r_0-1} a_{i-1,j} h_i + a_{r_0-1,j} \sum_{i=0}^{r_0-1} a_i h_i \\ &= \sum_{i=0}^{r_0-1} a_{i,j+1} h_i, \end{aligned}$$

where

$$a_{i,j+1} = D_\alpha a_{i,j} + a_{i-1,j} + a_{r_0-1,j} a_i, \quad (21)$$

and $a_{-1,j}(x) = 0$ for each index j . This completes the induction. \square

We can now define the open set $O \subset Z(T)$. Let $M = D^2 \deg(T)$. The set O is the subset of $Z(T)$ where none of the denominators involved in $a_{i,j}$ vanishes for $j \leq M$. Let us spell out what this means more carefully. Each $a_{i,j} \in K[x]_T[\alpha]$. Therefore, we can write as a finite combination of monomials in α :

$$a_{i,j} = \sum_I r_{i,j,I} \alpha^I.$$

In this sum, I denotes a multi-index, and $r_{i,j,I} \in K[x]_T$. For each i, j , there are only finitely many values of I in the sum. Each $r_{i,j,I}$ is a rational function $p_{i,j,I}/q_{i,j,I}$, where $q_{i,j,I} \notin (T)$. We let $O \subset Z(T)$ be the set where none of the denominators $q_{i,j,I}$ vanishes, for $0 \leq i \leq r_0 - 1$ and $1 \leq j \leq M$:

$$O = Z \setminus \bigcup_{\substack{j=1,\dots,M \\ i=0,\dots,r_0-1}} Z(q_{i,j,I}). \quad (22)$$

The set O is non-empty by a standard application of the Hilbert Nullstellensatz. Since T is irreducible, the radical of (T) is (T) . Since K is algebraically closed, we can apply the Nullstellensatz, and we see that the ideal of polynomials that vanishes on $Z(T)$ is exactly (T) . We know that each denominator $q_{i,j,I} \notin (T)$. Since T is irreducible, (T) is a prime ideal, and so $\prod q_{i,j,I} \notin (T)$. Therefore, $\prod q_{i,j,I}$ does not vanish on $Z(T)$. This shows that O is not empty.

Now Lemma 8.11 has the following Corollary on the set O :

Corollary 8.12. *Suppose that $z \in O$, $\alpha \in (K^{\binom{D+3}{3}})^2$, and*

$$h_j(\alpha, z) = 0, \quad j = 0, \dots, r_0 - 1. \quad (23)$$

Then $h_j(\alpha, z) = 0$, $j = 0, \dots, M$.

Proof. By Equation 20, we know that for all $j \leq M$,

$$h_j = \sum_{i=0}^{r_0-1} a_{i,j} h_i.$$

Expanding out the $a_{i,j}$ in terms of $p_{i,j,I}$ and $q_{i,j,I}$, we get

$$h_j(\alpha, x) = \sum_{i=0}^{r_0-1} \left(\sum_I \frac{p_{i,j,I}(x)}{q_{i,j,I}(x)} \alpha^I \right) h_i(\alpha, x).$$

At the point $x = z \in O$, the polynomials $q_{i,j,I}$ are all non-zero. By assumption, $h_i(\alpha, z) = 0$ for $i = 0, \dots, r_0 - 1$. Therefore, we see that $h_j(\alpha, z) = 0$ also. \square

We can now prove Theorem 8.1. Let γ be an irreducible curve of degree at most D . Let $z \in O$ be a smooth point of γ , and suppose γ is tangent to Z at z to order $\geq r_0$. Use Lemma 4.2 to choose an α associated to γ at z , as in Definition 4.1. By Theorem 6.5, $h_{j,\alpha}(z) = 0$, $j = 0, \dots, r_0$. But by Corollary 8.12, this implies $h_{j,\alpha}(z) = 0$, $j = 1, \dots, D^2(\deg T)$. Then by item (iv) from Lemma 8.3, $\gamma \subset Z$. This concludes the proof of Theorem 8.1.

8.4 Trapped implies sufficiently tangent

We will also need a converse to Theorem 8.1. We will call this property “trapped implies sufficiently tangent.”

Lemma 8.13. *Let $T \in K[x_1, x_2, x_3]$ and let $\gamma \in \mathcal{C}_{3,D}$ with $\gamma \subset Z(T)$. Let z be a regular point of γ and let α be associated to γ at z . Then*

$$D_\alpha^j T(z) = 0 \quad \text{for all } j \geq 0. \quad (24)$$

Proof. By Lemma 5.4, $(T)_z = (P_\alpha, Q_\alpha)_z$. In particular, we can write $T = \frac{p_1}{q_1} P_\alpha + \frac{p_2}{q_2} Q_\alpha$, where $q_1(z) \neq 0$, $q_2(z) \neq 0$. By Lemma 6.1, we have that $D_\alpha^j T(z) = 0$ for all j . \square

9 Generalized flecnodes and constructible conditions

Let K be a closed field. Let $T \in K[x_1, x_2, x_3]$ with $\deg T < \text{char}(K)$, and consider $Z(T) \subset K^3$. We recall that a point $x \in Z(T)$ is called flecnodal if there is a line L which is tangent to $Z(T)$ at x to order at least 3. We consider the following generalization:

Given a constructible set $\mathcal{C} \subset \mathcal{C}_{3,D}$, and given integers $t, r \geq 1$, with $r < \text{char } K$, we say that a point $x \in K^3$ is (t, \mathcal{C}, r) -flecnodal for T if there are $\geq t$ distinct curves $\gamma_1, \dots, \gamma_t \in \mathcal{C}$ passing through the point x , so that x is a regular point of each of these curves, and each of these curves is tangent (in the sense of Definition 6.3) to $Z(T)$ at x to order $\geq r$. The original definition of a flecnode corresponds to $t = 1$; $\mathcal{C} = \mathcal{C}_{3,1}$, the space of all lines in K^3 ; and $r = 3$.

The flecnode polynomial, discovered by Salmon, is an important tool for studying flecnodes. For each T , Salmon constructed a polynomial $\text{Flec } T$ of degree $\leq 11 \deg T$, so that a point $x \in Z(T)$ is flecnodal if and only if $\text{Flec } T(x) = 0$. Our goal is to generalize this result to (t, \mathcal{C}, r) -flecnodal points.

Our theorem for (t, \mathcal{C}, r) flecnodes is a little more complicated to state, but it is almost equally useful in incidence geometry. Instead of one polynomial $\text{Flec } T$, we will have a sequence of polynomials $\text{Flec}_j T$, where j goes from 1 to a large constant $J(t, \mathcal{C}, r)$. To tell whether a point x is flecnodal, we check whether $\text{Flec}_j T(x)$ vanishes for $j = 1, \dots, J$. Based on that information, we can determine whether x is (t, \mathcal{C}, r) -flecnodal. Here is the precise statement of the theorem.

Theorem 9.1. *For each constructible set $\mathcal{C} \subset \mathcal{C}_{3,D}$ and each pair of integers $t, r \geq 1$ with $r < \text{char } K$, there is an integer $J = J(t, \mathcal{C}, r)$, and a subset $B_{F(t, \mathcal{C}, r)} \subset \{0, 1\}^J$ so that the following holds. For each $1 \leq j \leq J$, and for each $T \in K[x_1, x_2, x_3]$, there are polynomials $\text{Flec}_j T = \text{Flec}_{t, \mathcal{C}, r, j} T \in K[x_1, x_2, x_3]$ so that*

- $\deg \text{Flec}_j T \leq C(t, \mathcal{C}, r) \deg T$.
- x is (t, \mathcal{C}, r) -flecnodal for T if and only if the vector $v(\text{Flec}_j T(x)) \in B_{F(t, \mathcal{C}, r)} \subset \{0, 1\}^J$.

(Recall from Section 2 that $v(y)$ is zero if $y = 0$ and 1 if $y \neq 0$.)

The main tool in the proof is Chevalley’s quantifier elimination theorem, Theorem 2.4. The method is quite flexible and it can also be used to study other variations of the flecnode polynomial.

9.1 The r -jet of a polynomial

The first observation in the proof is that whether a point z is (t, \mathcal{C}, r) -flecnodal for a polynomial T only depends on the point z and the r -jet of T at z . Recall that the r -jet of T at z , written $J^r T_z$ is

the polynomial of degree at most r that approximates T at z to order r . Here is the more formal definition. Recall that for any point $z \in K^n$, $I_{z, \geq r} \subset K[x_1, \dots, x_n]$ is the ideal of polynomials that vanish to order at least r at the point z – see Definition 6.2.

Definition 9.2. *For any $T \in K[x]$, the r -jet of T at z , $J^r T_z$, is the unique polynomial of degree at most r so that*

$$T - J^r T_z \in I_{z, \geq r+1}.$$

Since we assumed $r < \text{char } K$, the r -jet $J^r T_z$ can be computed with a Taylor series in the usual way, summing over multi-indices I :

$$J^r T_z(x) = \sum_{|I| \leq r} \frac{1}{I!} \nabla_I T(z) (x - z)^I. \quad (25)$$

For any multi-index I with $|I| \leq r$, $\nabla_I T(z) = \nabla_I J^r T_z(z)$.

We can now state our first observation as a formal lemma.

Lemma 9.3. *A point $z \in K^3$ is (t, \mathcal{C}, r) -flecnodal for a polynomial T if and only if z is (t, \mathcal{C}, r) -flecnodal for $J^r T_z$.*

Proof. Suppose that $\gamma \in \mathcal{C}$ and z is a regular point of γ . It suffices to check that γ is tangent to $Z(T)$ at z to order $\geq r$ if and only if γ is tangent to $Z(J^r T_z)$ to order $\geq r$.

By Theorem 6.5, γ is tangent to $Z(T)$ at z to order $\geq r$ if and only if

$$T \in I(\gamma) + I_{z, \geq r+1}.$$

Similarly, γ is tangent to $Z(J^r T_z)$ at z to order $\geq r$ if and only if

$$J^r T_z \in I(\gamma) + I_{z, \geq r+1}.$$

But $J^r T_z$ is defined so that $T - J^r T_z \in I_{z, \geq r+1}$, and so these conditions are equivalent. \square

We now define the set $\text{Flec}_{t, \mathcal{C}, r} \subset K^3 \times \text{Poly}_r(K^3)$

$$\text{Flec}_{t, \mathcal{C}, r} := \{(z, U) \in K^3 \times K[x]_{\leq r} \text{ so that } z \text{ is } (t, \mathcal{C}, r)\text{-flecnodal for } U\}.$$

By Lemma 9.3, z is (t, \mathcal{C}, r) -flecnodal for T if and only if $(z, J^r T_z) \in \text{Flec}_{t, \mathcal{C}, r}$.

9.2 Constructible conditions

Given any subset $Y \subset K^3 \times K[x]_{\leq r}$ we can think of Y as a condition. We say that T obeys Y at z if and only if $(z, J^r T_z) \in Y \subset K^3 \times K[x]_{\leq r}$. If Y is an algebraic set, we say that Y is an algebraic condition, and if Y is a constructible set, we say that Y is a constructible condition.

We will prove below that $\text{Flec}_{t, \mathcal{C}, r}$ is a constructible condition. Any constructible condition Y obeys a version of Theorem 9.1. This follows immediately from the definition of a constructible set, as we now explain.

Lemma 9.4. *Suppose that $Y \subset K^3 \times K[x]_{\leq r}$ is a constructible condition. Then for any polynomial $T : K^3 \rightarrow K$, there is a finite list of polynomials $Y_j T$, $j = 1, \dots, J(Y)$, and a subset $B_Y \subset \{0, 1\}^{J(Y)}$ obeying the following conditions:*

- $\deg Y_j T \leq C(Y) \deg T + C(Y)$.

- The polynomial T obeys condition Y at a point x if and only if $v(Y_j T(x)) \in B_Y$.

Proof. Since Y is a constructible set, there is a finite list of polynomials f_j on $K^3 \times \text{Poly}_k(K^3)$ so that $x \in Y$ if and only if $v(f_j(x)) \in B_Y$. By definition, T obeys condition Y at x if and only if $v(f_j(x, J^k T(x))) \in B_Y$.

We define $Y_j T(y) = f_j(y, J^k T(y))$. So T obeys condition Y at x if and only if $v(Y_j T(x)) \in B_Y$. Note that $J^k T$ is a vector-valued polynomial of degree $\leq \deg T$. (Each coefficient of $J^k T$ is a constant factor times a derivative $\nabla_I T$ for some multi-index I , and each $\nabla_I T$ is a polynomial of degree $\leq \deg T$.) We let $C(Y)$ be the maximal degree of the polynomials f_j . Then $Y_j T$ is a polynomial of degree $\leq C(Y) \deg T + C(Y)$. \square

Therefore, to prove Theorem 9.1, it only remains to show that $\text{Flec}_{t,C,r}$ is constructible.

9.3 Checking constructibility

We will now use Chevalley's theorem, Theorem 2.4, to check that $\text{Flec}_{t,C,r}$ is constructible. We build up to the set $\text{Flec}_{t,C,r}$ in a few steps, which we state as lemmas.

Lemma 9.5. *Let $\mathcal{C} \subset \mathcal{C}_{3,D}$ be a constructible set of complexity C . the set*

$$\{(x, U, \gamma) \in K^3 \times K[x]_{\leq r} \times \mathcal{C} : x \in \gamma_{\text{reg}}, \gamma \text{ tangent to } Z(U) \text{ at } x \text{ to order } \geq r\} \quad (26)$$

is constructible of complexity $O_{r,C,D}(1)$.

Proof. Recall that (4) is the set of triples (x, γ, α) so that α is associated to γ at x (see Definition 4.1). By Lemma 4.2, there exists an α so that $(x, \gamma, \alpha) \in (4)$ if and only if $x \in \gamma_{\text{reg}}$.

By Theorem 6.5, γ is tangent to $Z(U)$ at x to order $\geq r$ if and only if $D_\alpha^j U(x) = 0$ for each $j = 0, \dots, r$.

Consider the set

$$\begin{aligned} \{(x, U, \gamma, \alpha) \in K^3 \times K[x]_{\leq r} \times \mathcal{C} \times (K^{\binom{D+3}{3}})^2 : \\ (x, \gamma, \alpha) \in (4), D_\alpha^j U(x) = 0, j = 1, \dots, r\}. \end{aligned} \quad (27)$$

Since (4) is constructible, it is straightforward to check that this set is constructible. Now let $\pi: (x, U, \gamma, \alpha) \mapsto (x, U, \gamma)$, and note that (26) = $\pi((27))$. By Theorem 2.4, (26) = $\pi((27))$ is constructible of complexity $O_{r,C,D}(1)$. \square

Corollary 9.6. *Let $\mathcal{C} \subset \mathcal{C}_{3,D}$ be a constructible set of complexity C . The set*

$$\begin{aligned} \{(x, U, \gamma_1, \dots, \gamma_t) \in K^3 \times K[x]_{\leq r} \times \mathcal{C}^t : \\ (x, U, \gamma_i) \in (26) \text{ for each } i = 1, \dots, t; \gamma_i \neq \gamma_j \text{ if } i \neq j\} \end{aligned} \quad (28)$$

is constructible of complexity $O_{D,C,r,t}(1)$.

Proof. This follows from Lemma 9.5, using the fact that a Boolean combination of constructible sets is constructible. \square

Remark 9.7. *Though we will not need it here, one could also extend Corollary 9.6 to a collection of constructible sets $\mathcal{C}_1, \dots, \mathcal{C}_t \subset \mathcal{C}_{3,D}$. The version stated above is the special case $\mathcal{C}_1 = \dots = \mathcal{C}_t = \mathcal{C}$.*

Corollary 9.8. *If $1 \leq t, r$ and $r < \text{char } K$, and if $\mathcal{C} \subset \mathcal{C}_{3,D}$ is a constructible set of complexity C , then $\text{Flec}_{t,C,r}$ is constructible of complexity $O_{D,C,r,t}(1)$.*

Proof. Consider the projection

$$\pi: (x, U, \gamma_1, \dots, \gamma_t) \mapsto (x, U) \in K^3 \times K[x]_{\leq r}.$$

We note that $\text{Flec}_{t, \mathcal{C}, r} = \pi((28))$. By Corollary 9.6 and Chevalley's theorem, $\text{Flec}_{t, \mathcal{C}, r}$ is constructible of complexity $O_{D, \mathcal{C}, r, t}(1)$. □

10 Being flecnodal is contagious

In this section, we will explore a corollary of Theorem 9.1. We will prove that an algebraic surface with “too many” (t, \mathcal{C}, r) -flecnodal points must be (t, \mathcal{C}, r) -flecnodal almost everywhere.

Definition 10.1. *We say that a condition holds at almost every point of a variety Z if the subset of Z where the condition fails is contained in a subvariety of lower dimension. For example, a polynomial T obeys Y at almost every point of a curve γ if and only if Y holds at all but finitely many points of γ .*

Proposition 10.2. *For each C, D, t, r , there is a constant C_1 so that the following holds. Let $\mathcal{C} \subset \mathcal{C}_{3, D}$ be a constructible set of complexity $\leq C$. Suppose that $T \in K[x_1, x_2, x_3]$ is irreducible, and that $Z(T)$ contains at least $C_1(\deg T)^2$ algebraic curves in \mathcal{C} , each of which contains at least $C_1 \deg T$ (t, \mathcal{C}, r) -flecnodal points. Then there is a Zariski open subset of $Z(T)$ consisting of (t, \mathcal{C}, r) -flecnodal points.*

Proposition 10.2 follows from the fact that *all* constructible conditions are contagious—they all obey an estimate similar to that in Proposition 10.2.

Lemma 10.3. *Suppose that $Y \subset K^3 \times K[x]_{\leq r}$ is a constructible condition. Then there is a constant $C(Y)$ so that the following holds. Suppose that $\gamma \in \mathcal{C} \subset \mathcal{C}_{3, D}$. Suppose that $T: K^3 \rightarrow K$ is a polynomial. If T obeys condition Y at $> C(Y)D(\deg T + 1)$ points of γ , then T obeys condition Y at all but finitely many points of γ .*

Proof. Let z_1, z_2, \dots be points of γ where T obeys Y . We let $Y_j T$ be the polynomials described in Lemma 9.4, for $j = 1, \dots, J(Y)$. Recall that there is some set $B_Y \subset \{0, 1\}^{J(Y)}$ so that T obeys Y at z if and only if the vector $v(Y_j T(z)) \in B_Y$. In particular, at each point z_k , we have $v(Y_j T(z_k)) \in B_Y$. There are $\leq 2^{J(Y)}$ elements of B_Y . By the pigeon-hole principle, we can choose an element $\beta \in B_Y \subset \{0, 1\}^{J(Y)}$ so that $v(Y_j T(z_k)) = \beta$ holds for at least $2^{-J(Y)} C(Y)(\deg T + 1)(\deg \gamma)$ values of k . For each j , $Y_j T$ is a polynomial of degree $\leq C_1(Y)(\deg T + 1)$. We now choose $C(Y) > C_1(Y)2^{J(Y)}$ so that $v(Y_j T(z_k)) = \beta$ holds for more than $(\deg Y_j T)(\deg \gamma)$ values of k .

If $\beta_j = 0$, then we see that $Y_j T$ vanishes at $> \deg \gamma \deg Y_j T$ points of γ . By Bézout's theorem (Theorem 5.6), $Y_j T$ vanishes on γ . If $\beta_j = 1$, then we see that $Y_j T$ fails to vanish at at least one point of γ . Since γ is irreducible, $Y_j T$ vanishes at only finitely many points of γ .

Thus at all but finitely many points of γ , $v(Y_j T) = \beta \in B_Y$. Hence all but finitely many points of γ obey condition Y . □

Lemma 10.4. *Suppose that Y is a constructible condition. Then there is a constant $C(Y)$ so that the following holds. Let $T: K^3 \rightarrow K$ be a polynomial. Suppose that $\gamma_i \in \mathcal{C} \subset \mathcal{C}_{3, D}$, and that T obeys Y at almost every point of each γ_i . Suppose that all the γ_i are contained in an algebraic surface $Z(Q)$ for an irreducible polynomial Q . If the number of curves γ_i is $\geq C(Y)(\deg T + 1) \deg Q$, then T obeys Y at almost every point of $Z(Q)$.*

Proof. Consider one of the curves γ_i . Define $\beta_j(\gamma_i) = 0$ if and only if $Y_j T(x) = 0$ at almost every $x \in \gamma_i$. Then, for almost every point $x \in \gamma_i$, we have $v(Y_j T(x)) = \beta(\gamma_i)$. We must have $\beta(\gamma_i) \in B_Y \subset \{0, 1\}^{J(Y)}$.

By pigeonholing, we can find a $\beta \in B_Y$ so that $\beta(\gamma_i) = \beta$ for at least $2^{-J(Y)} C(Y) (\deg T + 1) \deg Q$ curves γ_i .

Suppose that $\beta_j = 0$. Then $Y_j T$ vanishes on each of these curves γ_i . But $\deg Y_j T \leq C(Y) (\deg T + 1)$. By choosing $C(Y)$ sufficiently large, the number of curves is greater than $(\deg Y_j T) (\deg Q)$. Now by a version of Bézout's theorem (Theorem 5.7), $Y_j T$ and Q must have a common factor. Since Q is irreducible, we conclude that Q divides $Y_j T$ and so $Y_j T$ vanishes on all of $Z(Q)$.

On the other hand, suppose that $\beta_j = 1$. Then we can find at least one point of $Z(Q)$ where $Y_j T$ does not vanish. Since Q is irreducible, $Y_j T$ vanishes only on a lower-dimensional subvariety of $Z(Q)$.

Therefore, at almost every point of $Z(Q)$, $v(Y_j T) = \beta \in B_Y$. Hence, at almost every point of $Z(Q)$, T obeys Y . \square

As a corollary, we see that any constructible condition obeys a version of Proposition 10.2.

Corollary 10.5. *If Y is a constructible condition, then there is a constant $C(Y)$ so that the following holds. Suppose that $T \in K[x_1, x_2, x_3]$ is irreducible, and that $Z(T)$ contains at least $C(Y) (\deg T + 1)^2$ curves from $\mathcal{C} \subset \mathcal{C}_{3,D}$, each of which contains at least $C(Y) D (\deg T + 1)$ points where T obeys Y . Then almost every point of $Z(T)$ obeys Y .*

Proof. By Lemma 10.3, T obeys Y at almost every point of each of the curves above. Then by Lemma 10.4, T obeys Y at almost every point of $Z(T)$. \square

In particular, this result implies Proposition 10.2, by taking $Y = \text{Flect}_{t,\mathcal{C},r} \subset K^3 \times K[x]_{\leq r}$.

11 Properties of doubly ruled surfaces

In this section we will prove Proposition 3.5. For the reader's convenience, we will restate it here.

Proposition 3.5. *Let K be an algebraically closed field, let $Z \subset K^3$ be an irreducible surface, and let $\mathcal{C} \subset \mathcal{C}_{3,D}$ for some $D \geq 1$. Suppose that Z is doubly ruled by curves from \mathcal{C} . Then*

- $\deg(Z) \leq 100D^2$.
- For any $t \geq 1$, we can find two finite sets of curves from \mathcal{C} in Z , each of size t , so that each curve from the first set intersects each curve from the second set.

Here is the idea of the proof. We use the fact that almost every point of Z lies in two curves of \mathcal{C} contained in Z in order to construct the curves in item (2) above. Using these curves, we can bound the degree of Z by imitating the proof that an irreducible surface $Z \subset K^3$ which is doubly ruled by lines has degree at most 2.

There is a technical moment in the proof where it helps to know that a generic point of Z lies in only finitely many curves of \mathcal{C} . This may not be true for \mathcal{C} , but we can find a subset $\mathcal{C}' \subset \mathcal{C}$ where it does hold. In the first section, we explain how to restrict to a good subset of curves \mathcal{C}' .

11.1 Reduction to the case of finite fibers

The main tool we will use is the following theorem:

Theorem 11.1. *Let $Y \subset K\mathbf{P}^{M+N}$ and $W \subset K\mathbf{P}^N$ be quasi-projective varieties, let W be irreducible, and let $\pi: Y \rightarrow W$ be a dominant projection map (or more generally, a dominant regular map). Then there is an open set $O \subset W$ so that the fiber above every point $z \in W$ has dimension $\dim Y - \dim W$ (by convention, a finite but non-empty set has dimension 0; the empty set has dimension -1).*

See e.g. Theorem 9.9 from [12]. In particular, if Y and W are affine varieties then they are quasi-projective, so Theorem 11.1 applies.

Corollary 11.2. *Let $Y \subset K^{M+N}$ be a constructible set, and let $W \subset K^N$ be an irreducible (affine) variety. Suppose that the image of $\pi: Y \rightarrow W$ is dense in W . Then there is an open set $O \subset W$ so that the fiber above every point $z \in W$ has dimension $\dim Y - \dim W$.*

Proof. Select affine varieties $Y_1, Y_2 \subset K^{M+N}$ so that $Y \subset Y_1 \setminus Y_2$ and $\dim Y_2 < \dim Y_1$. Note that if the image of $\pi: Y \rightarrow W$ is dense in W , then the image of $\pi: Y_1 \rightarrow W$ must be dense in W , i.e. $\pi: Y_1 \rightarrow W$ is a dominant map. Let $O_1 \subset Z$ be the open set from Theorem 11.1 applied to the map $Y_1 \rightarrow Z$. If $Y_2 \rightarrow Z$ is not dominant, then let $O = O_1 \setminus \pi(Y_2)$, and we are done.

If $Y_2 \rightarrow Z$ is dominant, let $O_2 \subset Z$ be the open set from Theorem 11.1 applied to the map $Y_2 \rightarrow Z$. Then for all $z \in O = O_1 \cap O_2$, $\pi_{Y_1}^{-1}(z)$ has dimension $\dim Y_1 - \dim W$, and $\pi_{Y_2}^{-1}(z)$ has dimension $\dim Y_2 - \dim W$. Thus $\pi^{-1}(Y)$ has dimension at least $\dim Y_1 - \dim W = \dim Y - \dim W$. But this is the maximum possible dimension of a fiber of π_Y above a point $z \in O \subset O_1$. Thus the fiber of π_Y above every point $z \in O$ has dimension $\dim Y - \dim W$. \square

Lemma 11.3. *Let Z and \mathcal{C} be as in the statement of Proposition 3.5. Define*

$$Y_{Z,\mathcal{C}} = \{(z, \gamma) \in Z \times \mathcal{C} : z \in \gamma, \gamma \subset Z\}, \quad (29)$$

and let $\pi: (z, \gamma) \mapsto z$. Then $Y_{Z,\mathcal{C}}$ is a constructible set. Furthermore, there exists a set $\mathcal{C}' \subset \mathcal{C}$ and an open set $O' \subset Z$ so that for every $z \in O'$, the fiber of the projection $\pi: Y_{Z,\mathcal{C}} \cap (Z \times \mathcal{C}') \rightarrow Z$ above z has finite cardinality, and this cardinality is ≥ 2 . The complexity of \mathcal{C}' is at most $O_{\mathcal{C}}(1)$, where \mathcal{C} is the complexity of \mathcal{C} ; in fact, \mathcal{C}' is obtained by intersecting \mathcal{C} by the union of two linear spaces.

Proof. First, the set $Y_{Z,\mathcal{C}}$ is constructible. By Theorem 2.4, the image of the map $\pi: Y_{Z,\mathcal{C}} \rightarrow Z$ is constructible. By assumption, it is Zariski dense in Z , and on a dense subset, every fiber has cardinality ≥ 2 . If there is an open dense set $O' \subset Z$ where every fiber is finite, then we are done.

Now, suppose that there does not exist an open dense set $O' \subset Z$ where every fiber is finite. Recall that \mathcal{C} is a constructible set, and in particular it is a subset of K^N for some $N \geq 1$. Let H_1, H_2, \dots be a sequence of linear varieties in K^N , with $H_1 \supset H_2 \supset \dots$, and $\text{codim}(H_j) = j$. For each index j , let $\tilde{H}_j = K^3 \times H_j$. Then by Corollary 11.2 we have that for each index j , the fiber of $\pi_j: (Y_{Z,\mathcal{C}} \cap H_j) \rightarrow Z$ above a generic point of Z has dimension $\dim(Y_{Z,\mathcal{C}} \cap H_j) - \dim Z$ if $\dim(Y_{Z,\mathcal{C}} \cap H_j) - \dim Z \geq 0$, and the fiber is empty otherwise. When $j = 0$, this quantity is ≥ 1 by assumption. On the other hand, when $j = N$, then $Y_{Z,\mathcal{C}} \cap H_j = \emptyset$, so the fiber above a generic point of π_N is empty and thus has dimension -1 . Furthermore, since K is algebraically closed,

$$\dim(Y_{Z,\mathcal{C}} \cap H_j) - 1 \leq \dim(Y_{Z,\mathcal{C}} \cap H_{j+1}) \leq \dim(Y_{Z,\mathcal{C}} \cap H_j). \quad (30)$$

Thus there is an index j_0 so that the fiber of π_{j_0} above a generic point of Z is finite and non-empty, and the fiber of π_{j_0+1} above a generic point of Z is empty.

We can repeat this procedure with a second collection $\{\tilde{H}'_j\}$ of hyperplanes so that no variety \tilde{H}'_j contains any irreducible component of $\pi_{j_0}^{-1}(Z)$. Arguing as above, we obtain a second index j'_0 so that the fiber of $\pi_{j'_0}$ above a generic point of Z is finite and non-empty. On the other hand, the fibers of π_{j_0} and $\pi_{j'_0}$ above a generic point of Z are disjoint. Thus the fiber of $\pi: (Y_{Z,\mathcal{C}} \cap (\tilde{H}_{j_0} \cup \tilde{H}'_{j'_0})) \rightarrow Z$ above a generic point of z is finite and has cardinality ≥ 2 . \square

Lemma 11.4. *Let Z be as in the statement of Proposition 3.5 and let \mathcal{C}' be as in Lemma 11.3. Then $Y_{Z,\mathcal{C}} \cap (Z \times \mathcal{C}')$ has dimension 2, and the image of $Y_{Z,\mathcal{C}} \cap (Z \times \mathcal{C}')$ under the projection $(z, \gamma) \mapsto \gamma$ has dimension 1.*

Proof. The first statement follows from Theorem 11.1. The second statement follows from the observation that for a generic $\gamma \in \mathcal{C}'$, the fiber above the projection $(x, \gamma) \mapsto \gamma$ has dimension 1. \square

Throughout the rest of this section, we will fix the set \mathcal{C}' and O' .

The following subsets of \mathcal{C}' play an important role in the argument.

Definition 11.5. *Let $X \subset K^3$ be a constructible set. Define*

$$\mathcal{C}^X := \{\gamma \in \mathcal{C}' : \gamma \cap X \neq \emptyset\}$$

and

$$\mathcal{C}_X := \{\gamma \in \mathcal{C}' : \gamma \subset X\}.$$

The notation here is potentially confusing, so we reiterate that these are subsets of \mathcal{C}' . All the curves we consider in the rest of this Section belong to \mathcal{C}' . We are leaving the prime out of the notation just because it is awkward to have to write $(\mathcal{C}')^X$ many times.

The sets \mathcal{C}^X and \mathcal{C}_X are constructible sets.

11.2 Constructible families of curves

Lemma 11.6. *If $\mathcal{C}'' \subset \mathcal{C}'$ is a constructible set of complexity $\leq C$, then*

$$U(\mathcal{C}'') := \bigcup_{\gamma \in \mathcal{C}''} \gamma$$

is a constructible set of complexity $O_{C_0,D,C}(1)$.

Proof. The union $U(\mathcal{C}'')$ is the projection of $Y_{Z,\mathcal{C}} \cap (Z \times \mathcal{C}'') \subset Z \times \mathcal{C}''$ to the Z factor. Since $Y_{Z,\mathcal{C}}$ and \mathcal{C}'' are constructible, $U(\mathcal{C}'')$ is constructible too. \square

Lemma 11.7 (Selecting a curve from a dense family). *Let $Z \subset K^3$ be an irreducible surface, and let $\mathcal{C}'' \subset \mathcal{C}_Z$ be an infinite set of curves. Let $X \subset Z$ be a dense, constructible set. Then there exists a curve $\gamma \in \mathcal{C}''$ so that $\gamma \cap X$ contains all but finitely many points of γ .*

Proof. We note that a constructible subset of Z is either contained in a 1-dimensional subset of Z or else contains a dense open set $O \subset Z$. Since X is a dense constructible subset of Z , there is a finite list of irreducible curves $\beta_j \subset Z$ so that $X \supset Z \setminus \bigcup_j \beta_j$. Since \mathcal{C}'' is infinite, we can choose $\gamma \in \mathcal{C}''$ with γ not equal to any of the curves β_j . Therefore, $\gamma \cap \beta_j$ is finite for each j , and so all but finitely many points of γ lie in X . \square

11.3 Constructing many intersecting curves

Lemma 11.8. *Let Z, C' , and O' be as above. Then we can construct an infinite sequence of curves $\gamma_1, \gamma_2, \dots$ in \mathcal{C}_Z so that for any $\ell \geq 1$,*

1. $\mathcal{C}_Z \cap \mathcal{C}^{\gamma_1 \cap O'} \cap \dots \cap \mathcal{C}^{\gamma_\ell \cap O'}$ is infinite.
2. At most two curves from $\{\gamma_1, \dots, \gamma_\ell\}$ pass through any point $z \in O'$.

Proof. We will prove the theorem by induction on ℓ . We begin with the case $\ell = 1$. By Lemma 11.7, we can choose $\gamma_1 \in \mathcal{C}_Z$ so that $\gamma_1 \cap O'$ is dense in γ_1 . Each point $z \in O'$ lies in at least two curves of \mathcal{C}_Z , so each point of $\gamma_1 \cap O'$ lies in a curve of \mathcal{C}_Z besides γ_1 . Therefore, $\mathcal{C}_Z \cap \mathcal{C}^{\gamma_1 \cap O'}$ is infinite. This checks Property (1) above, and Property (2) is vacuous in the case $\ell = 1$.

Now we do the inductive step of the proof. Suppose that we have $\gamma_1, \dots, \gamma_\ell$ with the desired properties. We have to find $\gamma_{\ell+1}$.

We define

$$\mathcal{C}_\ell := \mathcal{C}_Z \cap \mathcal{C}^{\gamma_1 \cap O'} \cap \dots \cap \mathcal{C}^{\gamma_\ell \cap O'}.$$

Next we define a finite set of undesirable curves B_ℓ . As a warmup, we define D_ℓ to be the set of intersection points of $\gamma_1, \dots, \gamma_\ell$ in O' :

$$D_\ell := \{z \in O' : z \text{ lies in at least two of the curves } \gamma_1, \dots, \gamma_\ell\}.$$

The set B_ℓ is the union of the curves $\{\gamma_i\}_{i=1}^\ell$ together with the union of all the curves of \mathcal{C}_Z that pass through a point of D_ℓ :

$$B_\ell := \left(\bigcup_{i=1}^\ell \gamma_i \right) \bigcup \left(\bigcup_{z \in D_\ell} \mathcal{C}_Z \cap \mathcal{C}^z \right).$$

The set D_ℓ is finite because any two irreducible curves can intersect in only finitely many points. For each $z \in O'$, $\mathcal{C}_Z \cap \mathcal{C}^z$ is finite, and so B_ℓ is finite. We will choose $\gamma_{\ell+1} \notin B_\ell$. This will guarantee that $\gamma_{\ell+1}$ is distinct from the previous curves, and it will also guarantee Property (2) above.

Our process depends on whether $\mathcal{C}_Z \setminus \mathcal{C}_\ell$ is finite or infinite.

Suppose $\mathcal{C}_Z \setminus \mathcal{C}_\ell$ is infinite. By Lemma 11.6, we know that $U(\mathcal{C}_\ell)$ is a constructible subset of Z . By Property (1), we know that \mathcal{C}_ℓ is infinite, and so $U(\mathcal{C}_\ell)$ must be a dense constructible set in Z . Therefore, $U(\mathcal{C}_\ell) \cap O'$ is also dense and constructible. Since $\mathcal{C}_Z \setminus \mathcal{C}_\ell$ is infinite, we can use Lemma 11.7 to choose $\gamma_{\ell+1}$ in $\mathcal{C}_Z \setminus (\mathcal{C}_\ell \cup B_\ell)$ so that

$$|\gamma_{\ell+1} \cap O' \cap U(\mathcal{C}_\ell)| = \infty.$$

Since $\gamma_{\ell+1} \notin \mathcal{C}_\ell$, we see that there are infinitely many curves of \mathcal{C}_ℓ that intersect $\gamma_{\ell+1} \cap O'$. This establishes Property (1), finishing the case that $\mathcal{C}_Z \setminus \mathcal{C}_\ell$ is infinite.

Suppose instead that $\mathcal{C}_Z \setminus \mathcal{C}_\ell$ is finite. Then $O' \setminus U(\mathcal{C}_Z \setminus \mathcal{C}_\ell)$ is a dense, constructible subset of Z . Since \mathcal{C}_ℓ is infinite, we can use Lemma 11.7 to choose $\gamma_{\ell+1}$ in $\mathcal{C}_\ell \setminus B_\ell$ so that

$$|\gamma_{\ell+1} \cap O' \setminus U(\mathcal{C}_Z \setminus \mathcal{C}_\ell)| = \infty.$$

If $z \in O'$, then z lies in two distinct curves of \mathcal{C}_Z . If $z \in O' \setminus U(\mathcal{C}_Z \setminus \mathcal{C}_\ell)$, then z lies in two distinct curves of \mathcal{C}_ℓ . One of these curves may be $\gamma_{\ell+1}$, but one of them must be a different curve. Therefore there are infinitely many curves of \mathcal{C}_ℓ that intersect $\gamma_{\ell+1} \cap O'$. This establishes Property (1) and finishes the induction. \square

We can now give the proof of Proposition 3.5.

Proof. Let γ_i be the curves in Lemma 11.8. Let N be a parameter at our disposal. Let X be a set of N^2 points, with N points on each curve γ_i for $i = 1, \dots, N$. Let Q be a minimal degree polynomial that vanishes on the set X .

Since $\dim \text{Poly}_D(K^3) \geq (1/6)D^3$, we have $\deg Q \leq 3|X|^{1/3} = 3N^{2/3}$. If $D \cdot 3N^{2/3} < N$, then the Bézout theorem (Theorem 5.6) implies that Q vanishes on γ_i for each $i = 1, \dots, N$. Suppose from now on that $N > 27D^3$, which guarantees that Q indeed vanishes on γ_i for each $i = 1, \dots, N$.

Next, we recall that there are infinitely many curves in $\mathcal{C}_Z \cap \mathcal{C}^{\gamma_1 \cap O'} \cap \dots \cap \mathcal{C}^{\gamma_N \cap O'}$. Let γ' be any one of these curves. We recall that any point of O' lies in at most two of the curves γ_i , and so γ' intersects the curves γ_i at at least $N/2$ distinct points. So Q vanishes at at least $N/2$ points of γ' . If $D(\deg Q) < N/2$, then Q must vanish at every point of γ' . Now $\deg Q \leq 3N^{2/3}$ and so it suffices to check that $D \cdot 3N^{2/3} < N/2$. We now suppose that $N > 6^3 D^3$, which guarantees that Q vanishes on all the infinitely many curves $\gamma' \in \mathcal{C}_Z \cap \mathcal{C}^{\gamma_1 \cap O'} \cap \dots \cap \mathcal{C}^{\gamma_N \cap O'}$. At this point, we can choose $N = 6^3 D^3 + 1$.

Suppose that our surface Z is the zero set of an irreducible polynomial T . We now see that $Z \cap Z(Q) = Z(T) \cap Z(Q)$ contains infinitely many distinct curves. By Bézout's theorem, Theorem 5.7, it follows that Q and T must have a common factor. But T is irreducible, so T must divide Q . But then the degree of T is at most the degree of Q , which is at most $3N^{2/3}$ which is at most $200D^2$. This proves the desired bound on the degree of Z .

The second item from Proposition 3.5 follows immediately from Lemma 11.8. For any $\ell \geq 1$, by Lemma 11.8 there are infinitely many curves of \mathcal{C} that intersect each of the curves $\{\gamma_1, \dots, \gamma_\ell\}$. \square

12 Proving Theorem 3.8

We begin with a corollary to Corollary 10.2 and Theorem 8.1:

Corollary 12.1. *Fix $D \geq 1$ and C . Then there exists a number r (large) and c_1 (small) so that for every constructible set $\mathcal{C} \subset \mathcal{C}_{3,D}$ of complexity at most C and every irreducible polynomial $T \in K[x_1, x_2, x_3]$ with $\deg T \leq c_1 \text{char}(K)$, there exists a (Zariski) open subset $O \subset Z(T)$ so that the following holds. If $x \in O$ is (t, \mathcal{C}, r) -flecnodal for T , then there exist (at least) t curves in \mathcal{C} that contain x and are contained in $Z(T)$.*

Lemma 12.2. *Fix $D > 0, C > 0$. Then there are constants c_2, C_3, C_4 so that the following holds. Let k be a field and let K be the algebraic closure of k . Let $\mathcal{C} \subset \mathcal{C}_{3,D}$ be a constructible set of complexity at most C . Let \mathcal{L} be a collection of n irreducible algebraic curves in k^3 whose algebraic closures are elements of \mathcal{C} . Suppose furthermore that $\text{char}(k) = 0$ or $n \leq c_2(\text{char}(k))^2$.*

Let $A > C_3 n^{1/2}$. Suppose that for each $\gamma \in \mathcal{L}$, there are $\geq A$ points $z \in \gamma$ that are incident to some curve from \mathcal{L} distinct from γ . Then there exists an irreducible surface $Z \subset k^3$ with the following properties:

- Z contains at least A/C_4 curves from \mathcal{L} .
- Z is “doubly ruled” by curves from \mathcal{C} in the sense of Definition 3.4 (and hence has degree at most $100D^2$ by Proposition 3.5).

Before proving Lemma 12.2, we will show how it implies Theorem 3.8. For the reader's convenience, we will recall the theorem here.

Theorem 3.8. Fix $D > 0, C > 0$. Then there are constants c_1, C_1, C_2 so that the following holds. Let k be a field and let K be the algebraic closure of k . Let $\mathcal{C} \subset \mathcal{C}_{3,D}$ be a constructible set of complexity at most C . Let \mathcal{L} be a collection of n irreducible algebraic curves in k^3 , with $\mathcal{L} \subset \mathcal{C}$ (see Definition 3.7). Suppose furthermore that $\text{char}(k) = 0$ or $n \leq c_1(\text{char}(k))^2$.

Then for each number $A > C_1 n^{1/2}$, at least one of the following two things must occur:

- There are at most $C_2 A n$ points in k^3 that are incident to two or more curves from \mathcal{L} .
- There is an irreducible surface $Z \subset k^3$ that contains at least A curves from \mathcal{L} . Furthermore, \hat{Z} is doubly ruled by curves from \mathcal{C} . See Definition 3.4 for the definition of doubly ruled, and see Proposition 3.5 for the implications of this statement.

Proof of Theorem 3.8 using Lemma 12.2.

Definition 12.3. Let \mathcal{L} be a collection of curves in k^3 . Define

$$\mathcal{P}_2(\mathcal{L}) = |\{x \in k^3 : x \text{ is incident to at least two curves from } \mathcal{L}\}|.$$

Let D and C be as in the statement of Theorem 3.8. Fix a field k , a constructible set $\mathcal{C} \subset \mathcal{C}_{3,D}$ (of complexity at most C), and a number A . We will prove the theorem by induction on n , for all $n \leq \min(C_1^{-2} A^2, c_1(\text{char } K)^2)$. The case $n = 1$ is immediate. Now, suppose the statement has been proved for all collections of curves in \mathcal{C} of size at most $n - 1$.

Applying Lemma 12.2 (with the value $A' = C_4 A$), we conclude that either there is an irreducible surface Z that is doubly ruled by curves from \mathcal{C} and that contains at least $A'/C_4 = A$ curves from \mathcal{L} , or there is a curve $\gamma \in \mathcal{L}$ so that $|\mathcal{P}_2(\mathcal{L}) \cap \gamma| < C_4 A$. If the former occurs then we are done.

If the latter occurs, then let $\mathcal{L}' = \mathcal{L} \setminus \{\gamma_0\}$. Then $|\mathcal{L}'| = n - 1$, so the collection \mathcal{L}' satisfies the induction hypothesis. Thus if we select $C_2 \geq C_4$, we have

$$\begin{aligned} \mathcal{P}_2(\mathcal{L}) &< \mathcal{P}_2(\mathcal{L}' \setminus \{\gamma_0\}) + C_4 A \\ &\leq C_2 A (n - 1) + C_4 A \\ &\leq C_2 A n. \end{aligned} \tag{31}$$

This closes the induction and establishes Theorem 3.8. □

Proof of Lemma 12.2.

Proposition 12.4 (Degree reduction). For every $D \geq 1$, there are constants C_5, C_6 so that the following holds. Let \mathcal{L} be a collection of n irreducible curves of degree $\leq D$ in k^3 , and let $A \geq C_5 n^{1/2}$. Suppose that for each $\gamma \in \mathcal{L}$, there are $\geq A$ points $z \in \gamma$ that are incident to some curve from \mathcal{L} distinct from γ . Then there is a polynomial P of degree at most $C_6 n/A$ whose zero-set contains every curve from \mathcal{L} .

We will prove Proposition 12.4 in Appendix B.

Now, factor $P = P_1 \dots P_\ell$ into irreducible components. For $j = 1, \dots, \ell$, define

$$\mathcal{L}_j = \{\ell \in \mathcal{L} : \ell \subset Z(P_j), \ell \not\subset Z_i \text{ for any } i < j\}.$$

Note that for each index j and each curve $\gamma \in \mathcal{L}_j$,

$$|\{p \in k^3 : p \in \gamma \cap \gamma', \text{ for some } \gamma' \in \mathcal{L}_i, i \neq j\}| < \deg P < A/2, \tag{32}$$

provided $A > (2C_6 n)^{1/2}$. Thus each curve γ is incident to at least $A/2$ other curves γ' that lie in the same set \mathcal{L}_j (and are therefore contained in the same surface Z_j).

By pigeonholing, exists an index j with

$$|\mathcal{L}_j| \geq \frac{A}{2C_6} \quad (33)$$

and

$$\begin{aligned} |\mathcal{L}_j| &\geq \frac{1}{2} \frac{n}{(\deg P)^2} (\deg Z_j)^2 \\ &\geq \frac{1}{2} \frac{n}{(C_6 n/A)^2} (\deg Z_j)^2 \\ &\geq \left(\frac{A^2}{2C_6^2 n} \right) (\deg Z_j)^2. \end{aligned} \quad (34)$$

Select A_4 (from the statement of Lemma 12.2) to be larger than $2C_6$, and let Z_0 be this irreducible component.

By Lemma 8.13, for each curve $\gamma \in \mathcal{L}_j$, there are at least $A/2$ points on γ that are $(2, \mathcal{C}, r)$ -flecnodal. Thus by Proposition 10.2, for each $r > 0$, there is a Zariski open set $O_r \subset Z_0$ consisting of $(2, \mathcal{C}, r)$ -flecnodal points. If we select r sufficiently large (depending on D , where $\mathcal{C} \subset \mathcal{C}_{3,D}$) and if $\frac{A^2}{2C_6^2 n}$ is sufficiently large (depending on r) (this can be guaranteed if we select C_3 from the statement of Lemma 12.2 to be sufficiently large depending on D), then by Corollary 12.1, there exists a Zariski open set $O \subset Z_0$ so that for every point $x \in O$, there are two curves from \mathcal{C} passing through x contained in Z . In other words, Z_0 is doubly ruled by curves from \mathcal{C} , as in Definition 3.4. \square

A A quantitative ascending chain condition

In this section we will prove Proposition 8.7. For the reader's convenience, we re-state it here:

Proposition 8.7. *Let \tilde{K} be a field, let $N \geq 0$, and let $\tau: \mathbb{N} \rightarrow \mathbb{N}$ be a function. Then there exists a number M_0 with the following property. Let $\{I_i\}$ be a sequence of ideals in $\tilde{K}[x_1, \dots, x_N]$, with $\text{complexity}(I_i) \leq \tau(i)$. Then there exists a number $r_0 \leq M_0$ so that $I_{r_0} \subset I_1 + \dots + I_{r_0-1}$.*

A.1 Reverse lexicographic order

Definition A.1. *Given two $(N+1)$ -tuples $\ell = (\ell_0, \dots, \ell_N)$, $\ell' = (\ell'_0, \dots, \ell'_N)$, we say $\ell \prec \ell'$ if $\ell \neq \ell'$, and one of the following holds*

- $\ell_N < \ell'_N$,
- $\ell_N = \ell'_N$ and $\ell_{N-1} < \ell'_{N-1}$,
- \vdots
- $\ell_N = \ell'_N, \ell_{N-1} = \ell'_{N-1}, \dots, \ell_1 = \ell'_1$, and $\ell_0 < \ell'_0$.

We will only use \prec to compare two tuples of the same length. The relation \prec is transitive.

Definition A.2. *If ℓ is a tuple, we define $|\ell| = |\ell_0| + \dots + |\ell_N|$. In our applications, the entries will always be non-negative. We will use $\mathbf{0}$ to denote the tuples whose entries are all 0s (the length of the tuple should be apparent from context).*

Lemma A.3 (length of chains). *Let $N \geq 0$ and let $\tau: \mathbb{N} \rightarrow \mathbb{N}$ (in our applications, we will have something like $N = 3$, $\tau(t) = 100t^3$). Then there exists a number M_0 with the following property. Let $\{\ell_i\}$ be a sequence of $(N + 1)$ -tuples of non-negative integers. Suppose that the sequence is weakly monotonically decreasing under the \prec order. Suppose furthermore that for each index i , $|\ell_i| \leq \tau(i)$. Then there exists some $r_0 \leq M_0$ so that $\ell_{r_0-1} = \ell_{r_0}$.*

A.2 Hilbert functions and Hilbert polynomials

Let \tilde{K} be a field, and let $I \subset \tilde{K}[x_1, \dots, x_N]$ be an ideal. We define $I_{\leq t}$ to be the set of all polynomials in I that have degree at most t ; this set has the structure of a \tilde{K} -vector space. We define the Hilbert function

$$H_I(t) = \dim_{\tilde{K}}(\tilde{K}[x_1, \dots, x_N]_{\leq t} / I_{\leq t}). \quad (35)$$

Theorem A.4 (Hilbert). *There exists a polynomial $HP_I \in \mathbb{R}[t]$ so that for all $t \in \mathbb{N}$ sufficiently large, $HP_I(t) = H_I(t)$. Furthermore, $HP_I(t)$ is an integer for all $t \in \mathbb{N}$.*

Definition A.5. *If $I \subset \tilde{K}[x_1, \dots, x_N]$, let $\ell_I = (\ell_0, \dots, \ell_N)$, where $\ell_j = j! \text{coeff}(HP_I, j)$. Here $\text{coeff}(HP_I, j) = \frac{1}{j!} HP_I^{(j)}(0)$ is the coefficient of t^j in the polynomial HP_I .*

Lemma A.6. *Let I be an ideal. Then ℓ_I is a tuple of non-negative integers.*

Proof. This follows from the Maucaulay representation of a Hilbert polynomial (see i.e. [1, Prop 1.3] for further details). \square

Proposition A.7. *If $I \subset I'$, then $\ell'_I \preceq \ell_I$. If furthermore $\ell_I = \ell'_I$, then $I = I'$.*

Proof. If $I \subset I'$, then $H_I(t) \leq H_{I'}(t)$, and this establishes the first statement. On the other hand, if $\ell_I = \ell'_I$ then $H_I(t) = H_{I'}(t)$ for all sufficiently large t , and this immediately implies $I = I'$. \square

Lemma A.8 (Quantitative bounds on coefficients of Hilbert Polynomials). *Let $I \subset \tilde{K}[x_1, \dots, x_N]$. Then $|\ell_I|$ is bounded by a function that depends only on N and $\text{complexity}(I)$. i.e. the sum of the coefficients of the Hilbert polynomial of the ideal (f_1, \dots, f_ℓ) is controlled by ℓ and the maximal degree of f_1, \dots, f_ℓ .*

We can now prove Proposition 8.7. Let $\tilde{I}_j = (I_1 + \dots + I_j)$, so $\tilde{I}_j \subset \tilde{I}_{j+1}$ for each index j . By Lemma A.8, there is a function $\tilde{\tau}_j$ (depending only on N and τ) so that $|\ell_{\tilde{I}_j}| \leq \tilde{\tau}(j)$. Thus by Lemma A.3 applied to $\tilde{\tau}$, there is a number M_0 (depending only on N and τ) so that $\ell_{\tilde{I}_{r_0-1}} = \ell_{\tilde{I}_{r_0}}$ for some $r_0 \leq M_0$. We conclude that $\tilde{I}_{r_0-1} = \tilde{I}_{r_0}$ and thus $I_{r_0} \subset (I_1 + \dots + I_{r_0-1})$.

B Degree reduction

In this section we will prove Proposition 12.4. The proof is similar to arguments found in [5].

We will require several Chernoff-type bounds for sums of Bernoulli random variables. For convenience, we will gather them all here.

Theorem B.1 (Chernoff). *Let X_1, \dots, X_N be iid Bernoulli random variables with $\mathbf{P}(X_i = 1) = p$, $\mathbf{P}(X_i = 0) = 1 - p$. Then*

$$\mathbf{P}\left(\frac{1}{N} \sum_{i=1}^N X_i \leq p - \epsilon\right) \leq \left(\left(\frac{p}{p - \epsilon}\right)^{p - \epsilon} \left(\frac{1 - p}{1 - p + \epsilon}\right)^{1 - p + \epsilon}\right)^N,$$

$$\mathbf{P}\left(\frac{1}{N} \sum_{i=1}^N X_i \geq p + \epsilon\right) \leq \left(\left(\frac{p}{p + \epsilon}\right)^{p + \epsilon} \left(\frac{1 - p}{1 - p - \epsilon}\right)^{1 - p - \epsilon}\right)^N.$$

Corollary B.2. *Let X_1, \dots, X_N be iid Bernoulli random variables with $\mathbf{P}(X_i = 1) = p$, $\mathbf{P}(X_i = 0) = 1 - p$. Suppose $p \geq N^{-1}$. Then*

$$\mathbf{P}\left(\sum_{i=1}^N X_i \leq \frac{pn}{100}\right) \leq 1/2, \quad (36)$$

$$\mathbf{P}\left(\sum_{i=1}^N X_i \geq 100pn\right) \leq 1/4. \quad (37)$$

Proposition B.3. *Let X_1, \dots, X_N be iid Bernoulli random variables with $\mathbf{P}(X_i = 1) = \mathbf{P}(X_i = 0) = 1/2$. Suppose $N \geq 100$. Then*

$$\mathbf{P}\left(\sum X_i < \frac{99}{100} \frac{N}{2}\right) < \frac{1}{4}. \quad (38)$$

Proposition B.4 (Polynomial interpolation). *Let \mathcal{L}_1 be a collection of n irreducible degree curves of degree $\leq D$ in k^3 . Then there is a polynomial $P \in k[x_1, x_2, x_3]$ of degree at most $100Dn^{1/2}$ that contains all of the curves in \mathcal{L}_1 .*

We are now ready to prove Proposition B.3. For the readers convenience we will re-state it here.

Proposition 12.4. *For every $D \geq 1$, there are constants C_0, C_1 so that the following holds. Let \mathcal{L} be a collection of n irreducible curves of degree $\leq D$ in k^3 , and let $A \geq C_0n^{1/2}$. Suppose that for each $\gamma \in \mathcal{L}$, there are $\geq A$ points $z \in \gamma$ that are incident to some curve from \mathcal{L} distinct from γ . Then there is a polynomial P of degree at most C_1n/A whose zero-set contains every curve from \mathcal{L} .*

Proof. For each D we will prove the result by induction on n . The case $n \leq 10^3$ follows from Proposition B.3, provided we take $C_1 \geq 10^{5/2}D$. Now assume the result has been proved for all sets $\tilde{\mathcal{L}}$ of size at most $n - 1$.

For each curve $\gamma \in \mathcal{L}$, choose a set $\mathcal{P}_\gamma \subset \mathcal{P}_2(\mathcal{L})$ of size A . Each point in \mathcal{P}_γ is hit by at least one curve from \mathcal{L} . Furthermore, no curve from \mathcal{L} can intersect γ in more than D^2 points. Thus we can select a set \mathcal{P}'_γ of size A/D^2 and a collection $\mathcal{L}_\gamma \subset \mathcal{L}$ of size A/D^2 so that each curve is incident to γ at exactly one point of \mathcal{P}'_γ , and no two curves from \mathcal{L}_γ are incident to γ at the same point of \mathcal{P}'_γ .

Let $p = C_2n/A^2$, where $C_2 = C_2(D)$ is a constant to be chosen later. Let $\mathcal{L}' \subset \mathcal{L}$ be a subset of \mathcal{L} obtained by choosing each curve in \mathcal{L} with probability p . By (37) from Corollary B.2, we have

$$\mathbf{P}\left(|\mathcal{L}'| > 100p|\mathcal{L}|\right) < 1/4. \quad (39)$$

By (36) from Corollary B.2, for each $\gamma \in \mathcal{L}$ we have

$$\mathbf{P}\left(|\mathcal{L}_\gamma \cap \mathcal{L}'| < \frac{p|\mathcal{L}_\gamma|}{100}\right) < 1/2.$$

Since the above events are independent, by Proposition B.3 we have

$$\mathbf{P}\left(\left|\left\{\gamma \in \mathcal{L}: |\mathcal{L}_\gamma \cap \mathcal{L}'| < \frac{p|\mathcal{L}_\gamma|}{100}\right\}\right| < \frac{99}{200}|\mathcal{L}|\right) < 1/4.$$

Thus, we can select a set $\mathcal{L}' \subset \mathcal{L}$ so that

$$|\mathcal{L}'| \leq 100p|\mathcal{L}|,$$

and

$$\left|\left\{\gamma \in \mathcal{L}: |\mathcal{L}_\gamma \cap \mathcal{L}'| > \frac{p|\mathcal{L}_\gamma|}{100}\right\}\right| > \frac{99}{200}|\mathcal{L}|. \quad (40)$$

Using Proposition B.4, we can find a polynomial $P_1 \in k[x_1, x_2, x_3]$ of degree $\leq 100D(100p|\mathcal{L}|)^{1/2}$ that contains every line from \mathcal{L}' . If $C_2 = C_2(D)$ is chosen sufficiently large, then

$$D(\deg P) + 1 < \frac{p|\mathcal{L}_\gamma|}{100}.$$

Thus if $|\mathcal{L}_\gamma \cap \mathcal{L}'| > \frac{p|\mathcal{L}_\gamma|}{100}$ then $\gamma \subset Z(P)$. Let $\mathcal{L}_1 := \{\gamma \in \mathcal{L}: \gamma \subset Z(P)\}$. Let $\tilde{\mathcal{L}} := \mathcal{L} \setminus \mathcal{L}_1$.

By (40), $|\mathcal{L}_1| \geq \frac{99}{200}|\mathcal{L}|$, and thus $|\tilde{\mathcal{L}}| \leq \frac{101}{200}|\mathcal{L}|$. If $\gamma \in \tilde{\mathcal{L}}$ then γ can intersect $Z(P_1)$ in at most $D(\deg P_1)$ places. This implies

$$|\gamma \cap \mathcal{P}_2(\mathcal{L}_1)| < D(\deg P) + 1 < \frac{1}{100}A,$$

provided $C_2 = C_2(D)$ is chosen sufficiently small depending on D .

But recall that $|\gamma \cap \mathcal{P}_2(\mathcal{L})| \geq A$. This means that for each curve $\gamma \in \tilde{\mathcal{L}}$,

$$|\gamma \cap \mathcal{P}_2(\tilde{\mathcal{L}})| \geq \frac{99}{100}A.$$

Since $|\tilde{\mathcal{L}}| \leq \frac{101}{200}|\mathcal{L}|$, we have

$$\begin{aligned} \frac{99}{100}A &\geq \frac{99}{100}C_0n^{1/2} \\ &\geq \frac{99}{100}C_0\left(\frac{99}{100}\right)^{1/2}|\tilde{\mathcal{L}}|^{1/2} \\ &\geq C_0|\tilde{\mathcal{L}}|^{1/2}. \end{aligned} \quad (41)$$

Thus we can apply the induction hypothesis to $\tilde{\mathcal{L}}$ (with $\tilde{A} = \frac{99}{100}A$) to conclude that there is a polynomial P_2 of degree

$$\begin{aligned} \deg P_2 &\leq C_1|\tilde{\mathcal{L}}|/\tilde{A} \\ &\leq C_1\frac{100}{99}\frac{101}{200}|\mathcal{L}|/A \\ &\leq \frac{2}{3}C_1\frac{|\mathcal{L}|}{A} \end{aligned}$$

that vanishes on $\tilde{\mathcal{L}}$. Thus if we let $P = P_1P_2$, then P vanishes on every curve of \mathcal{L} , and

$$\begin{aligned} \deg P &\leq 100(100p|\mathcal{L}|)^{1/2} + \frac{2}{3}C_1\frac{|\mathcal{L}|}{A} \\ &\leq (10^4C_2 + \frac{2}{3}C_1)\frac{|\mathcal{L}|}{A}. \end{aligned} \quad (42)$$

If we select C_1 sufficiently large depending on C_2 (recall that C_2 is a sufficiently large absolute constant), then $(10^4C_2 + \frac{2}{3}C_1) \leq C_1$, and this completes the induction. \square

References

- [1] M. Chardin, G. Moreno-Socías. Regularity of lex-segment ideals: some closed formulas and applications. *Proc. AMS.* 131(4):1093–1102. 2002.
- [2] W. Fulton. *Intersection theory*. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. Springer-Verlag, Berlin, second edition, 1998.
- [3] M. Green, I. Morrison. The equations defining Chow varieties. *Duke Math. J.* 53:733–747. 1986.
- [4] L. Guth. Distinct distance estimates and low degree polynomial partitioning. *Discr. Comput. Geom.* 53(2):428–444. 2015.
- [5] L. Guth, N. Katz. Algebraic Methods in Discrete Analogs of the Kakeya Problem. *Adv. Math.* 225(5): 2828–2839. 2010. Also in arXiv:0812.1043.
- [6] — On the Erdős distinct distance problem in the plane. *Ann of Math.* 181(1): 155–190. 2015. Also in arXiv:1011.4105.
- [7] J. Harris. *Algebraic geometry: a first course*. Springer, New York, NY. 1995.
- [8] N. Katz. The flecnode polynomial: a central object in incidence geometry. arXiv:1404.3412. 2014.
- [9] J. Kollar. Szemerédi-Trotter-type theorems in dimension 3. arXiv:1405.2243. 2014.
- [10] J. Landsberg. *Cartan for Beginners: Differential Geometry Via Moving Frames and Exterior Differential Systems*. American Mathematical Society. 2003.
- [11] H. Matsumura. *Commutative Algebra*, second edition. W. A. Benjamin Co., New York NY. 1980.
- [12] J.S. Milne. Algebraic Geometry. (v6.00). Available at www.jmilne.org/math. 2014.
- [13] G. Salmon. *A Treatise on the Analytic Geometry of Three Dimensions*, Vol. 2, 5th edition. Hodges, Figgis And Co. Ltd. 1915.
- [14] H. Schenck. *Computational Algebraic Geometry*. Cambridge University Press. 2003.
- [15] M. Sharir, N. Solomon. Incidences between points and lines in three dimensions. arXiv:1501.02544. 2015.