David HOLMES et Nick ROME

Fields of definition of rational curves of a given degree

Fields of definition of rational curves of a given degree

par David HOLMES et Nick ROME

Résumé. Kontsevich et Manin ont donné une formule pour le nombre N_e de courbes planes rationnelles de degré e passant par $3e-1$ points en position générale dans $\mathbb{P}^2$. Lorsque les coordonnées de ces $3e-1$ points sont des nombres rationnels, l'ensemble de N_e courbes rationnelles correspondant a une structure naturelle de module galoisien. Nous effectuons une étude élémentaire de cette structure et établissons un lien avec les transformations de revêtements de la fibre générique du produit des applications d'evaluation sur l'espace de modules de morphismes.

Nous étudions ensuite le comportement asymptotique du nombre de points rationnels sur les hypersurfaces de petit degré, ce qui nous permet de généraliser nos résultats en remplaçant le plan projectif par une telle hypersurface.

Abstract. Kontsevich and Manin gave a formula for the number N_e of rational plane curves of degree e through $3e-1$ points in general position in the plane. When these $3e-1$ points have coordinates in the rational numbers, the corresponding set of N_e rational curves has a natural Galois-module structure. We make some extremely preliminary investigations into this Galois module structure, and relate this to the deck transformations of the generic fibre of the product of the evaluation maps on the moduli space of maps.

We then study the asymptotics of the number of rational points on hypersurfaces of low degree, and use this to generalise our results by replacing the projective plane by such a hypersurface.

1. Introduction

For a given positive integer e, we write N_e for the finite number of rational (i.e. geometric genus 0) plane curves of degree e through $3e - 1$ points in general position in $\mathbb{P}^2_{\mathbb{C}}$. We see immediately that $N_1 = N_2 = 1$, and the number N_3 of singular plane cubics through 8 points is easily shown to be 12. Zeuthen [23] proved in 1873 that $N_4 = 620$, and Ran [14] and Vainsencher [20] showed in the early 1990s that $N_5 = 87,304$. Around the

same time Kontsevich and Manin [12] proved a general recursive formula

$$N_e = \sum_{\substack{e_A+e_B=e \\ e_A>0, e_B>0}} N_{e_A} N_{e_B} e_A^2 e_B \left(e_B \binom{3e-4}{3e_A-2} - e_A \binom{3e-4}{3e_A-1} \right),$$

allowing the rapid computation of any N_e. Their proof ran via the intersection theory on moduli spaces of stable maps, and has initiated a vast area of research generalising this to curves of higher genera, and to more geometrically interesting targets in place of $\mathbb{P}^2$.

In this paper we take a more arithmetic viewpoint, and ask over what sub-fields of $\mathbb{C}$ we should expect these rational curves to be defined. The most basic version of the question is the following: suppose the $3e-1$ points in general position all have coordinates in the rational numbers $\mathbb{Q}$. Should we then expect any or all of the N_e rational curves to be defined over $\mathbb{Q}$ (i.e. such that their defining equations can be chosen to have rational coefficients, or equivalently to arise by base-change from some curves over $\mathbb{Q}$)? The answer is trivially "yes" if $e = 1$ or 2 (since $N_1 = N_2 = 1$), but we will see later that the answer is "no" for all higher e:

Theorem 1.1. *Let $e > 2$. Then the set of $(3e - 1)$-tuples of points in $\mathbb{P}^2(\mathbb{Q})$ where at least one of the N_e rational curves is defined over $\mathbb{Q}$ forms a thin set.*

The notion of a *thin set* is due to Serre; in Section 2 we will recall the definition and prove a stronger version of the above theorem. The idea of a thin set is that it should contain "few" points; indeed, from the above we easily deduce in Section 2.1:

Corollary 1.2. *Ordering all $(3e - 1)$-tuples of points in $\mathbb{P}^2(\mathbb{Q})$ by height, the proportion of tuples where at least one of the N_e curves is defined over $\mathbb{Q}$ is 0%.*

Analogous questions can be asked about rational curves on hypersurfaces X in $\mathbb{P}^N$ whose degree is low relative to their dimension. A lot is known about the irreducibility and dimension of the relevant moduli spaces, for generic X by work of Harris–Roth–Starr [11], Beheshti–Kumar [1] and Riedl–Yang [15], and for any X by work of Browning-Vishe [5] and Browning–Sawin [4]. This allows us to prove analogously that very few n-tuples of points in X are such that at least one element of the finite set of rational curves through them of suitable degree is defined over $\mathbb{Q}$.

Theorem 1.3. *Let $X \subseteq \mathbb{P}^N$ be a smooth hypersurface of degree d such that $(d - 1)2^d < N$. Fix integers $e > 0$ and $n \geq 0$ such that the expression $(N + 1 - d)e + (N - 4) + n = n(N - 1)$ holds. Then there exists a thin set $A \subseteq X^n(k)$ such that for all $P \in X^n(k) \backslash A$, the corresponding set of rational curves of degree e in X through the points in P contains no curve defined over $\mathbb{Q}$.*

Note that, unlike in the case of target $\mathbb{P}^2$, it is not always the case that we can fix the other variables and then find a value of n which works. This is because we have to arrange that a certain product of evaluation maps is finite so that these sets of rational curves are finite, and this is not always possible for arbitrary choices of N, d and e.

Since weak approximation is known to hold for such hypersurfaces [19], it follows from [17, Theorem 3.5.7] that the set of rational points is not thin. This means that, by the previous theorem, there must exist points $P \in X^n(k)$ for which none of the curves through P are defined over $\mathbb{Q}$. In Section 5 we give a more refined quantitative estimate for the number of points which lie in any given thin set. Combining this with the above theorem yields:

Corollary 1.4. *Under the above hypotheses, and assuming that $X(\mathbb{Q})$ is non-empty, the proportion of n-tuples of points in $X(\mathbb{Q})$ for which at least one of the rational curves is defined over $\mathbb{Q}$ is 0%.*

Informally, this means that "almost all" of the sets of rational curves do not contain any curve defined over $\mathbb{Q}$. In fact, Theorem 5.1 is stronger than this, proving a power saving in the count for rational points in a thin set. The key tool in the proof is a sieve result for points on hypersurfaces which may be thought of as a form of effective strong approximation, and which the authors believe will also be of independent interest.

The questions we ask in this paper seem natural from an arithmetic perspective, but do they have interesting geometric content? As we will see in the proof of Proposition 2.2, what we are really studying is the group of deck transformations of the generic fibre of the product of the evaluation maps on the moduli space of maps to $\mathbb{P}^2$ of given degree. Kontsevich and Manin established that this cover is of degree N_e, but this leaves open the question of the structure of the group of deck transformations.

1.1. Splitting fields. Given a set P of $3e - 1$ $\mathbb{Q}$-points of $\mathbb{P}^2$ in general position, write C_P for the set of N_e (complex) rational plane curves of degree e through P. We write $L_P \subseteq \mathbb{C}$ for the splitting field of the Galois module C_P, i.e. the smallest sub-field of $\mathbb{C}$ such that every curve in C_P arises by base-change from some plane curve over L_P. Naively, we can think of L_P as the field generated by the coefficients of defining equations for the curves, after scaling these equations to have at least one coefficient in $\mathbb{Q}$.

The field extension $L_P/\mathbb{Q}$ is necessarily finite and Galois (in other words, the fixed field of the automorphism group of L_P over $\mathbb{Q}$ is $\mathbb{Q}$ itself). We can ask about the degree of L_P over $\mathbb{Q}$ or (for a finer invariant) its Galois group $\mathrm{Gal}(L_P/\mathbb{Q})$. (Harris was the first to study the Galois groups arising in problems from enumerative geometry, see [10] for 4 nice examples of similar problems.) At one extreme we could have $L_P = \mathbb{Q}$, in other words all C_P

are defined over $\mathbb{Q}$. At the other extreme it could have L_P of degree $N_e!$ and Galois group the symmetric group S_{N_e} on N_e objects. We conjecture that the latter occurs "almost always". More precisely, we propose:

Conjecture 1.5. *For all P outside a thin subset of $(\mathbb{P}^2)^{3e-1}(\mathbb{Q})$, we have* $\mathrm{Gal}(L_P/\mathbb{Q}) = S_{N_e}$.

See Section 2 for the definition of a thin set. The conjecture is trivially true for $e = 1$ and 2, and we prove it in Section 3 for $e = 3$.

1.2. Further questions. There are a number of possible variations and extensions on the questions proposed in this note. One can ask whether the 0-dimensional schemes C_p satisfy the Hasse Principle, or whether there is a Brauer–Manin obstruction.

It also seems to be interesting to understand what happens in positive characteristic, but to the authors' knowledge even the number of rational curves has not been determined over $\overline{\mathbb{F}}_p$ (it is clear that the number coincides with that over $\mathbb{C}$ for "large enough" p, but making this "large enough" explicit, and understanding what happens for small p, seems to remain open).

It may well be possible to extend the computations in Section 3 to $e = 4$ or maybe even $e = 5$, though the authors do not have the courage to attempt it. It is clear that other techniques will be needed in the general case.

1.3. Atttribution. Sections 1–4 (excluding 2.1) are due to the first-named author. Sections 5 and 2.1 are due to the second-named author.

1.4. Acknowledgements. Both authors are grateful to Tim Browning for putting them in contact with one another, and for helpful comments. We also would like to thank the referee for their careful reading of the paper, which lead to a number of corrections and improvements.

1.5. Notation. We shall write $\mathbb{Z}_{\mathrm{prim}}^n$ to denote the set of primitive vectors in $\mathbb{Z}^n$. A sum with subscript "dyadic" will refer to a sum whose variables run over powers of 2. As is standard, we will write $f(x) \ll g(x)$ to mean that there exists some constant $c > 0$ such that for all sufficiently large x, we have $|f(x)| \le c|g(x)|$, and $f(x) \asymp g(x)$ to mean $f(x) \ll g(x) \ll f(x)$.

2. Most sets of N_e curves contain no curve defined over the ground field

Let k be a field of characteristic zero, and X/k a reduced separated scheme of finite type (a *variety*). For X an irreducible variety, a subset $A \subseteq X(k)$ is called *thin* if there exists a map of varieties $\pi\colon Y \to X$, not admitting a rational section, and such that $A \subseteq \pi(Y(k))$. The field

k is *Hilbertian* if $\mathbb{P}^1(k)$ is not thin (as a subset of itself). The field $\mathbb{Q}$ is Hilbertian, as is any finitely generated extension; $\mathbb{C}$ is not.

Remark 2.1. If there exists a closed subset $Z \subset X$ with $Z \neq X$ and $A \subset Z(k)$ then we refer to A as a thin set of type *I*. If there is some irreducible variety Y with $\dim(X) = \dim(Y)$ and a generically surjective morphism $\pi : Y \to X$ of degree ≥ 2 with $A \subset \pi(Y(k))$ then A is referred to as a thin set of type *II*. Any thin subset $A \subset X(k)$ may be written as a finite union of thin sets of type *I* and type *II*.

Let $k \subseteq \mathbb{C}$ be a Hilbertian field, and fix a positive integer e. Suppose we are given $P \in (\mathbb{P}^2)^{3e-1}(k)$; we can think of this as a $(3e-1)$-tuple of k-points in $\mathbb{P}^2$, and we write C_P for the set of rational curves of degree e through P defined over $\bar{k}$; in general this set may be infinite. We say P is *transitive* if

- the set C_P has N_e elements (this holds if P is in "general position"), and
- the Galois group $\mathrm{Gal}(\bar{k}/k)$ acts transitively on the set C_P (equivalently, the Galois group of the splitting field L_P of C_P is a transitive subgroup of the symmetric group on N_e elements).

Note that P being transitive implies in particular that none of the curves in C_P is defined over k, for $e > 2$.

Proposition 2.2. *The set of $P \in (\mathbb{P}^2)^{3e-1}(k)$ which are not transitive form a thin set.*

Proof. We may and do assume that $e > 2$, otherwise the result is obvious. The result is immediate from a lemma of Serre, after the standard reformulation of the counting problem into a moduli problem. We write $\mathcal{M}_{0,3e-1}(\mathbb{P}^2, e)$ for the moduli space whose T-points are tuples $(C/T, x_1, \ldots, x_{3e-1}, \varphi)$ with C/T a smooth curve of genus 0, the $x_i \in C(T)$ disjoint sections, and $\varphi \colon C \to \mathbb{P}^2$ is fibrewise generically immersive and satisfies $\varphi^* \mathcal{O}_{\mathbb{P}^2}(1) \cong \mathcal{O}_{\mathbb{P}^1}(e)$. It is easy to check that $\mathcal{M}_{0,3e-1}(\mathbb{P}^2, e)$ is an *irreducible* variety.

This space $\mathcal{M}_{0,3e-1}(\mathbb{P}^2, e)$ comes with evaluation maps ev_i to $\mathbb{P}^2$ for $1 \leq i \leq 3e-1$, sending $(C/T, x_1, \ldots, x_{3e-1}, \varphi)$ to $\varphi \circ x_i$. Together these ev_i induce a map

$$ev \colon \mathcal{M}_{0,3e-1}(\mathbb{P}^2, e) \to (\mathbb{P}^2)^{3e-1},$$

generically finite of degree N_e, and $C_P = ev^{-1}(P)$.

Denote by η the generic point of $(\mathbb{P}^2)^{3e-1}$, then the fibre $ev^{-1}\eta$ is irreducible since $\mathcal{M}_{0,3e-1}(\mathbb{P}^2, e)$ is. Then by [17, Proposition 3.3.5] there exists a thin set $A \subseteq (\mathbb{P}^2)^{3e-1}(k)$ such that for all P outside A, the fibre $ev^{-1}P$ has the expected number N_e of $\bar{k}$-points and is irreducible, so the Galois action is transitive. $\square$

In fact, the same proof shows more: we can choose the thin set A such that for every P outside A, the Galois group of L_P is naturally isomorphic to that of the generic fibre $ev^{-1}\eta/\eta$. So to prove Conjecture 1.5 it would be equivalent to show that the Galois group of the generic fibre $ev^{-1}\eta$ were the full symmetric group S_{N_e}.

2.1. Asymptotics. In this subsection we take $k = \mathbb{Q}$. There are a number of senses in which thin sets contain "few" points. One of them is by counting the number of points up to a given size. For a positive integer B we define $M(B)$ to be the number of points in $(\mathbb{P}^2)^{3e-1}(\mathbb{Q})$ with height bounded by B. We choose to use here an anticanonical height on $(\mathbb{P}^2)^{3e-1}$. If $x = (x_0 : x_1 : x_2) \in \mathbb{P}^2$ and $\mathbf{x} = (x_0, x_1, x_2) \in \mathbb{Z}^3_{\mathrm{prim}}$, then the height of x associated to the anticanonical bundle $\mathcal{O}(3)$ is given by

$$H(x) = \|\mathbf{x}\|^3_\infty,$$

where $\|\mathbf{x}\|_\infty = \max_i |x_i|$. The height on $(\mathbb{P}^2)^{3e-1}$ is then inherited from this since the anticanonical bundle on the product is $\mathcal{O}(3, 3, \ldots, 3)$ and hence an anticanonical height on $(\mathbb{P}^2)^{3e-1}$ is given by a product of the heights on each copy of $\mathbb{P}^2$. If $x \in (\mathbb{P}^2)^{3e-1}(\mathbb{Q})$ there is a representative of x of the form $(\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(3e-1)}) \in (\mathbb{Z}^3_{\mathrm{prim}})^{3e-1}$, the height of x is given by

$$H(x) = \prod_{j=1}^{3e-1} \|\mathbf{x}^{(j)}\|^3_\infty.$$

By the compatibility of Manin's conjecture with taking products (initially observed in [8, Section 1]), we have $M(B) \asymp B(\log B)^{3e-2}$.

We define $N(B)$ to be the number of points P of height at most B which are *not* transitive.

Lemma 2.3. *There exists $\gamma \in [0, 1)$ such that*

$$N(B) = O\left(B(\log B)^{3e-3+\gamma}\right).$$

Proof. Let $A \subset (\mathbb{P}^2)^{3e-1}(\mathbb{Q})$ be any non-empty thin set. We will prove that the number of points of height at most B which lie in A can be bounded above by $O(B(\log B)^{3e-3+\gamma})$, from which (along with Proposition 2.2) the result follows. Note that it suffices to just consider the case when A is a thin set of type I or of type II.

We count points in $(\mathbb{P}^2)^{3e-1}(\mathbb{Q})$ by passing to the affine cone $(\mathbb{Z}^3_{\mathrm{prim}})^{3e-1}$. The affine cone of A is

$$A' = \left\{x \in (\mathbb{Z}^3_{\mathrm{prim}})^{3e-1} : (\mathbf{x}^{(1)} : \ldots : \mathbf{x}^{(3e-1)}) \in A\right\}$$

and we denote by $\bar{A}_p$ the reduction of A' modulo a prime p. We will upper bound the number of elements in A' of bounded height (and thus those in A) by the cardinality

$$S(B) := \# \left\{ x \in (\mathbb{Z}^3_{\text{prim}})^{3e-1} : \prod_{j=1}^{3e-1} \|\mathbf{x}^{(j)}\|_\infty \leq B^{1/3} \text{ and } x \bmod p \in \bar{A}_p \right\}.$$

To attack this we first break into dyadic intervals

$$S(B) \leq \sum_{\substack{B_1 \cdots B_{3e-1} \leq B^{1/3} \\ \text{dyadic}}} H(B_1, \ldots, B_{3e-1}),$$

where $H(B_1, \ldots, B_{3e-1})$ is defined to be

$$\# \left\{ x \in (\mathbb{Z}^3_{\text{prim}})^{3e-1} : B_j/2 < \|\mathbf{x}^{(j)}\|_\infty \leq B_j \; \forall \, j, \text{ and } x \bmod p \in \bar{A}_p \right\}.$$

The inner cardinality can be estimated using the multi-dimensional large sieve in lopsided boxes (see e.g. [13, Theorem 4.1]). This gives

$$S(B) \ll \sum_{\substack{B_1 \cdots B_{3e-1} \leq B^{1/3} \\ \text{dyadic}}} \left(\prod_{j=1}^{3e-1} \left(B_j + Q^2 \right)^3 \right) / G(Q),$$

where

$$G(Q) := \sum_{q \leq Q} \mu^2(q) \prod_{p \mid q} \frac{\omega_p}{1 - \omega_p},$$

$$\omega_p := 1 - \frac{\#\bar{A}_p}{\#(\mathbb{F}_p^3 \setminus \{\mathbf{0}\})^{3e-1}}.$$

If A is a thin set of type *II*, then by [17, Theorem 3.6.2], there exists $c \in (0,1)$ and a finite Galois extension $k/\mathbb{Q}$ such that for all sufficiently large primes p which split completely in k, we have

$$\#\bar{A}_p \leq c p^{3(3e-1)} + O(p^{3(3e-1)-1/2}).$$

We denote the set of such sufficiently large, completely splitting primes by $\mathcal{P}$ and let δ be the natural density of such primes (which is strictly greater than 0 by Chebotarev's density theorem). Therefore there exists $\eta < (1-c)/c$ such that for all primes $p \in \mathcal{P}$, we have $\frac{\omega_p}{1-\omega_p} \geq \eta$. Thus

$$G(Q) \gg \sum_{\substack{q \leq Q \\ p \mid q \Rightarrow p \in \mathcal{P}}} \mu^2(q) \eta^{\omega(q)}.$$

This sum is estimated using Wirsing's theorem [22, Satz 1.1]. The Chebotarev density theorem, along with an application of partial summation,

tells us that

$$\sum_{\substack{p \leq Q \\ p \in \mathcal{P}}} \frac{\eta \log p}{p} \sim \eta \delta \log Q.$$

Therefore by [22, Satz 1.1] we have

$$\sum_{\substack{q \leq Q \\ p | q \Rightarrow p \in \mathcal{P}}} \mu^2(q) \eta^{\omega(q)} \sim \frac{Q}{\log Q} \prod_{\substack{p \leq Q \\ p \in \mathcal{P}}} \left(1 + \frac{\eta}{p}\right).$$

By taking the logarithm of the above product, we have

$$\log \left(\prod_{\substack{p \leq Q \\ p \in \mathcal{P}}} \left(1 + \frac{\eta}{p}\right)\right) = \sum_{\substack{p \leq Q \\ p \in \mathcal{P}}} \log \left(1 + \frac{\eta}{p}\right) \gg \delta \eta \log \log Q,$$

where the inequality is again a straightforward consequence of the Chebotarev density theorem. Hence, we conclude that

$$G(Q) \gg Q (\log Q)^{\delta \eta - 1}.$$

When A is a thin set of type I, the Lang–Weil estimate (e.g. [17, Theorem 3.6.1]) tells us that

$$\# \bar{A}_p \ll p^{3(3e-1)-1},$$

from which the bound $G(Q) \gg_\epsilon Q^{2-\epsilon}$ can be deduced in a similar manner. Let $\gamma = 1 - \delta \eta$, then setting $Q = \min_j \{B_j^{1/2}\}$ we get

$$S(B) \ll (\log B)^\gamma \sum_{\substack{B_1 \cdots B_{3e-1} \leq B^{1/3} \\ \text{dyadic}}} (B_1 \cdots B_{3e-1})^3 \min_j \{B_j^{-1/2}\}$$

$$\ll (\log B)^\gamma \sum_{\substack{B_1 \leq B_2 \leq \cdots \leq B_{3e-1} \\ B_1 \cdots B_{3e-1} \leq B^{1/3} \\ \text{dyadic}}} (B_1 \cdots B_{3e-1})^3 B_1^{-1/2}$$

$$\ll B (\log B)^\gamma \sum_{\substack{B_1 \leq B_2 \leq \cdots \leq B_{3e-2} \\ B_1 \cdots B_{3e-2} \leq B^{1/3} \\ \text{dyadic}}} B_1^{-1/2}$$

$$\ll B (\log B)^{3e-3+\gamma} \sum_{\substack{B_1 \leq B^{1/3} \\ B_1 = 2^j \text{ for some } j}} B_1^{-1/2}.$$

This final sum is convergent and so we deduce the claimed bound. $\qquad \square$

In other words, the ratio $N(B)/M(B)$ tends to zero at least as fast as $(\log B)^{\gamma-1}$ as $B \to \infty$.

3. Splitting fields for $e = 3$

We know that $N_3 = 12$, and by Conjecture 1.5 we should expect that the Galois group is S_{12} for all P outside some thin set; here we verify that. By the same argument as in the proof of Proposition 2.2 it is enough to verify that the Galois group of the splitting field of the generic fibre $L_\eta = ev^{-1}\eta$ is S_{12}. If P is any point in $(\mathbb{P}^2)^8$ with $\#C_P = 12$ (so ev is étale in a neighbourhood of P) then we have a natural injection from the Galois group of L_P to the Galois group of L_η. Hence it suffices to find a single such P for which we can show that the Galois group of L_P is S_{12}.

For readability we will describe our example in affine coordinates, on one of the standard charts of $\mathbb{P}^2$. A little random experimentation brought us to the 8 points $(1, 0), (-3, 1), (3, -3), (-3, 3), (2, -1), (-3, 1), (2, 4), (1, 3)$ (in the first affine patch). The 2-dimensional space of cubics through these eight points is spanned by the cubics

$$x^3 + 5/74y^3 + 28/37x^2 - 10/37xy - 50/37y^2 - 173/37x + 275/74y + 108/37$$

and

$$x^2y - 75/74y^3 + 61/37x^2 + 39/37xy + 10/37y^2 + 227/37x + 463/74y - 288/37.$$

We used SAGE to re-write the generic element of the linear span of these two cubics into Weierstrass form, and to compute the discriminant of the resulting cubic, given by

$$\Delta = -\frac{24953575063474272765882500}{6582952005840035281}t^{12} + \frac{13414288494017281213773412 5}{6582952005840035281}t^{11}$$
$$+ \frac{14211473829551239264075376 25}{26331808023360141124}t^{10} - \frac{72151150791789778224830918 75}{26331808023360141124}t^{9}$$
$$+ \frac{17943310292096345174858538375}{105327232093440564496}t^{8} + \frac{16439749600766827372335403125}{52663616046720282248}t^{7}$$
$$- \frac{37073875099429097905357566 25}{13165904011680070562}t^{6} - \frac{15914630472519837692866331 25}{26331808023360141124}t^{5}$$
$$- \frac{40045577444754207261637275 0}{6582952005840035281}t^{4} - \frac{17709125224492502479842423 75}{52663616046720282248}t^{3}$$
$$- \frac{41930948369778731917638875 0}{6582952005840035281}t^{2} - \frac{12906646230435281098756875}{26331808023360141124}t$$
$$- \frac{8666228358581839593918 75}{105327232093440564496}.$$

A curve of degree 3 is rational if and only if it is not smooth, and the vanishing of the discriminant detects exactly when this non-smoothness occurs. In other words, the scheme of zeros of Δ is isomorphic to the scheme $C_P = ev^{-1}P$, so the splitting field L_P is given by the splitting field of Δ. We computed the Galois group of the latter in MAGMA, and found it to be S_{12} as required.

Remark 3.1. On can alternatively argue using Del Pezzo surfaces (cf. [21, Section 7.3]), though in the end this simply re-phrases the computer search. The blow up of $\mathbb{P}^2$ in 8 points in general position is a del Pezzo surface X

of degree 1, and the strict transforms of the 12 singular cubics give the 12 singular elements of the anticanonical linear system on X. Blowing up the 9th point through which they all pass yields an elliptic surface, and (the strict transforms of) these 12 curves are the singular fibres of the elliptic fibration. Explicitly, the surface X has the equation:

$$y^2 = x^3 + f_2(z,w)x^2 + f_4(z,w)x + f_6(z,w)$$

where f_i has degree i. The 12 points over which the fibres are non-smooth are the zero locus of the discriminant of this elliptic pencil, which is a polynomial $D(z,w)$ of degree 12 in z, w. One can then perform a computer search for polynomials f_i for which $D(z,w)$ has Galois group S_{12}.

4. Hypersurfaces of low degree

4.1. Formalities. We continue to work over a Hilbertian field k with algebraic closure $\bar{k}$. The reader will note that the only properties of the variety $\mathbb{P}^2$ used in the proof of Proposition 2.2 are the following:

  (1) $\mathcal{M}_{0,3e-1}(\mathbb{P}^2; e)$ is an irreducible variety;
  (2) the product of the evaluation maps $ev\colon \mathcal{M}_{0,3e-1}(\mathbb{P}^2; e) \to (\mathbb{P}^2)^{3e-1}$ is generically finite.

This naturally leads us to a generalisation of Proposition 2.2. Let X/k be an irreducible variety, fix a line bundle[1] $\mathcal{L}$ on X, and for each non-negative integer n define a moduli functor $\mathcal{M}_{0,n}(X, \mathcal{L}; e)$ on the category Sch_k of schemes over k, sending T to the set of tuples $(C/T, x_1, \ldots, x_n, \varphi)$ where

  - C/T is a smooth proper curve of genus 0;
  - The $x_i \in C(T)$ are disjoint sections;
  - $\varphi\colon C \to X_T$ is a T-morphism which is generically immersive on each fibre, such that $\varphi^*\mathcal{L}$ has degree e on each fibre of C/T,

modulo isomorphisms over X (such isomorphisms are unique when they exist, so this is a fine moduli space). This functor is not always an irreducible variety (for example, if $\mathcal{L} = \mathcal{O}_X$ and $e = 0$ it is likely to have infinitely many connected components; the quintic 3-fold provides a much less trivial example), but sometimes it is an irreducible variety, for example when X is $\mathbb{P}^2$ and $\mathcal{L} = \mathcal{O}(1)$.

As before we have the evaluation maps $ev_i\colon \mathcal{M}_{0,n}(X, \mathcal{L}; e) \to X$ each sending a tuple $(C/T, x_1, \ldots, x_n, \varphi)$ to $\varphi \circ x_i$, and can take their product $ev\colon \mathcal{M}_{0,n}(X, \mathcal{L}; e) \to X^n$. The set of $\bar{k}$-points of the fibre of ev over a point $P = (p_1, \ldots, p_n) \in X^n(k)$ is exactly the set of rational curves in X over $\bar{k}$, of $\mathcal{L}$-degree e, and passing through all the p_i. In general this set can be infinite, but if ev is generically finite (i.e. the fibre of ev over the generic point of X^n is finite) then, for P outside some proper Zariski closed subset of X^n, these sets are finite and all of the same cardinality, which we shall

---

[1]More generally fix a class in étale cohomology of suitable dimension.

denote $N(X, \mathcal{L}, n, e)$. In this case we say P is *transitive* if indeed the fibre has the "expected" number $N(X, \mathcal{L}, n, e)$ of $\bar{k}$-points, and moreover the natural action of $\mathrm{Gal}(\bar{k}/k)$ on the fibre is transitive. Imitating the proof of Proposition 2.2 one immediately obtains

Proposition 4.1. *Fix a variety X, a line bundle $\mathcal{L}$ on X, and non-negative integers e and n. Assume that*

(1) *$\mathcal{M}_{0,n}(X, \mathcal{L}; e)$ is an irreducible variety;*
(2) *the product of the evaluation maps $ev \colon \mathcal{M}_{0,n}(X, \mathcal{L}; e) \to X^n$ is generically finite.*

Then there exists a thin subset $A \subseteq X^n(k)$ such that all $P \in X^n(k) \setminus A$ are transitive.

Note that we do not exclude the possibility that the generic fibre of ev is empty, but any map from the empty scheme is finite, and for these purposes we consider the unique group action on the empty set to be transitive, making the result vacuous in this case.

Connoisseurs of the empty set will consider this in poor taste. "Transitive" should morally mean "has exactly one orbit", so that the action on the empty set should not be considered transitive. Such readers should add to our result the assumption that the generic fibre of the map ev is non-empty; understanding when this happens is a very interesting problem.

Suppose that $\mathcal{M}_{0,n}(X, \mathcal{L}; e)$ is an irreducible variety (in particular reduced); if the tangent map to ev is surjective at some point of the source, it follows that ev is dominant (and the converse holds in characteristic zero, by generic smoothness). Surjectivity of the tangent map can be analysed via deformation theory; details can be found in [7, Section 4]. For example, one can show (combining results of [18] and [6]) that, for a general cubic 3-fold the product of evaluation maps $ev \colon \mathcal{M}_{0,n}(X, \mathcal{L}; e) \to X^n$ is dominant whenever $n \leq e - 1$ and $e \geq 2$. Note however that in this setting the dimensions are not equal (see below for a more detailed analysis), so that we do not get a generically finite map.

4.2. Hypersurfaces. For an interesting application of Proposition 4.1 we need an irreducible variety X with two properties. First, it should satisfy the criteria of Proposition 4.1. But we should also ask that $X(k)$ is itself not thin, otherwise the conclusion is vacuous. Such examples are provided by hypersurfaces in projective space of low degree (relative to their dimension).

Fix positive integers N, d and e, and let X be a smooth hypersurface of degree d in $\mathbb{P}^N$; we fix $\mathcal{L} = \mathcal{O}(1)$, and drop it from the notation henceforth. When is $\mathcal{M}_{0,n}(X; e)$ an irreducible variety? Note that $\mathcal{M}_{0,n}(X; e)$ can be built from $\mathcal{M}_{0,0}(X; e)$ by repeatedly taking universal curves (and deleting loci where sections intersect), so $\mathcal{M}_{0,n}(X; e)$ is an irreducible variety if and

only if $\mathcal{M}_{0,0}(X;e)$ is, and their dimensions differ by n. There are two main cases when $\mathcal{M}_{0,0}(X;e)$ is known to be an irreducible variety:

(1) char $k = 0$, $N > 2$ and $d + 2 < N$, and X is generic, by work of Reidl and Yang [15];
(2) $N > 2$ and $(2d - 1)2^{d-1} < N$ by work of Browning and Sawin [4], with no genericity assumptions on X, but assuming char $k = 0$ or char $k > d$.

In these cases it is also known that $\mathcal{M}_{0,0}(X;e)$ is of the "expected" dimension, namely $(N+1-d)e+(N-4)$. Since the dimension of X^n is $n(N-1)$, the map $ev\colon \mathcal{M}_{0,n}(X, \mathcal{L}; e) \to X^n$ is generically finite if and only if we have the equality

$$(N + 1 - d)e + (N - 4) + n = n(N - 1)$$

(it could perhaps happen that the map ev is not dominant, but in this case the generic fibre of ev is empty, so the result is vacuously true as remarked above). We deduce:

Proposition 4.2. *Let $N > 2$, $d > 0$ and $e > 0$ and $n \geq 0$ be integers such that $(N+1-d)e+(N-4)+n = n(N-1)$. Let X be a hypersurface in $\mathbb{P}^N$ of degree d, satisfying one of the assumptions (1) and (2) above. Then there exists a thin set $A \subseteq X^n(k)$ such that all $P \in X^n(k) \setminus A$ are transitive.*

4.3. Asymptotics. We keep the notation of the above section, but restrict now to the case $k = \mathbb{Q}$. A-priori it could be that $A = X^n(\mathbb{Q})$, but using the results from the appendix we can show this is far from the case. First, we must assume that X has at least one rational point (by Birch's result below, this is equivalent to assuming that X is everywhere locally soluble).

Then for a positive integer B, write $\mathbf{M}(B)$ for the number of rational points on X^n of height less than B. Assuming that $N > 2^d(d - 1) - 1$, Birch [2, Theorem 1], combined with the compatibility of Manin's conjecture with products as noted above, shows that there exist $c > 0$ and $\delta > 0$ such that

$$\mathbf{M}(B) = cB(\log B)^{n-1} + O\left(B(\log B)^{n-1-\delta}\right).$$

Now write $\mathbf{N}(B)$ for the number of $P \in X^n(\mathbb{Q})$ which are not transitive. Assume $N > 2^d(2d - 1)$, then by Proposition 4.2 of the preceding section, there exists a thin subset $A \subseteq X^n$ containing all those P which are not transitive. Now we can apply Theorem 5.1 to see that there exists $\gamma \in [0, 1)$ with

$$\mathbf{N}(B) \ll B(\log B)^{n-2+\gamma}$$

Hence the ratio

$$\frac{\mathbf{N}(B)}{\mathbf{M}(B)} \ll \frac{B(\log B)^{n-2+\gamma}}{cB(\log B)^{n-1} + c'B(\log B)^{n-1-\delta}} \ll (\log B)^{\gamma-1}$$

where c' is some positive constant. Summarising, we have

Theorem 4.3. *Let $X/\mathbb{Q}$ be a hypersurface with $N > 2^d(d-1)$. Then there exists $\delta' > 0$ such that*

$$\frac{\#\{P \in X^n(\mathbb{Q}) : H(P) \leq B \text{ and } P \text{ not transitive}\}}{\#\{P \in X^n(\mathbb{Q}) : H(P) \leq B\}} \ll (\log B)^{-\delta'}.$$

Informally, this tells us that most collections of points on a hypersurface X are transitive, thus the sets of curves through them contain no curves defined over $\mathbb{Q}$.

5. Thin Sets on Smooth Hypersurfaces of Low Degree

Let $F \in \mathbb{Z}[x_0, \dots, x_N]$ be a homogeneous form of degree d. Denote by X the projective variety defined by F and assume (for simplicity) that it is smooth. Given $n \in \mathbb{N}$, suppose $A \subset X^n(\mathbb{Q})$ is a non-empty thin set. The purpose of this section is to show that a thin set on X^n contains few points, extending a result of Browning–Loughran [3, Theorem 1.8] on the number of points in a thin subset of a quadric to multiple copies of a general hypersurface (of suitably large dimension).

Theorem 5.1. *If $N > 2^d(d-1)$ and H is the anticanonical height function on X^n described below then $\exists\ \delta, \gamma > 0$ such that*

$$\#\{x \in A : H(x) \leq B\} \ll_{A,X} \begin{cases} B^{1-\delta}(\log B)^\gamma & \text{if } n = 1, \\ B(\log B)^{n-2+\gamma} & \text{if } n \geq 2. \end{cases}$$

Remark 5.2. Let $x \in X^n(\mathbb{Q})$ and $x = (\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(n)})$ for $\mathbf{x}^{(j)} \in \mathbb{Z}_{\text{prim}}^{N+1}$. Since the anticanonical bundle on X is $\mathcal{O}(N+1-d)$ (see e.g [8, Section 1]), an anticanonical height function on X^n is given by

$$H(x) = \prod_{j=1}^{n} \|\mathbf{x}^{(j)}\|_\infty^{N+1-d}.$$

The result is a consequence of a sieve estimate for points on products of a hypersurface lying in some prescribed residue classes. In establishing this estimate we make crucial use of a recent generalisation of Birch's theorem due to Schindler–Sofos [16] (cf. Lemma 5.6).

Fix $m \in \mathbb{N}$. Let

$$\Omega_{p^m} \subset \left\{ (\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(n)}) \in (\mathbb{Z}/p^m\mathbb{Z})^{n(N+1)} : p \nmid \mathbf{x}^{(j)}, F(\mathbf{x}^{(j)}) \equiv 0 \bmod p^m\ \forall\ j \right\}$$

be some non-empty collection of residue classes for each prime p. Denote their relative density by

$$\omega_p := 1 - \frac{\#\Omega_{p^m}}{\#\widehat{X^n}(\mathbb{Z}/p^m\mathbb{Z})} \in [0, 1),$$

where $\widehat{X^n}$ denotes the affine cone of X^n. We will establish Theorem 5.1 using a large sieve type estimate for points of bounded height of the following form.

Lemma 5.3. *There exist $\delta_1, \delta_2 > 0$ such that*

$$\#\{x \in X(\mathbb{Q}) : H(x) \leq B \text{ and } x \bmod p^m \in \Omega_{p^m} \; \forall \, p\} \ll \frac{B}{\min\{G(B^{\delta_1}), B^{\delta_2}\}},$$

where

$$G(Q) = \sum_{q \leq Q} \mu^2(q) \prod_{p \mid q} \frac{\omega_p}{1 - \omega_p}.$$

Remark 5.4. This theorem is analogous to [3, Theorem 1.7] and all the results derived for quadrics concerning fibrations, zero loci of Brauer group elements and friable divisors could also be generalised to the setting of smooth hypersurfaces of low degree in a similar fashion.

In general we will need to look at products of hypersurfaces, to deal with the resulting height condition we break into dyadic intervals as in the proof of Lemma 2.3. Then we need to investigate the subset $\mathbf{N}(X^n, \mathbf{B}, \Omega)$ defined by

$$\#\left\{x \in \widehat{X^n}(\mathbb{Q}) : B_j/2 < \|\mathbf{x}^{(j)}\|_\infty \leq B_j \text{ and } \mathbf{x}^{(j)} \bmod p^m \in \Omega_{p^m} \; \forall \, p, j\right\},$$

where $(\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(n)})$ is a representative of x in $(\mathbb{Z}_{\text{prim}}^{N+1})^n$. We have the following analogous estimate for products.

Theorem 5.5. *Suppose $N > 2^d(d-1)$. Then for any $\epsilon > 0$ and any $Q \geq 1$, one has*

$$\mathbf{N}(X^n, \mathbf{B}, \Omega) \ll_{\epsilon, X} (B_1 \cdots B_n)^{N+1-d} \left(\frac{1}{G(Q)} + E_1 + E_2\right),$$

where

$$E_1 = \min_j\{B_j\}^{-\frac{1}{2}} Q^{m(2d-2n+1)+2+\epsilon}$$

$$E_2 = \min_j\{B_j\}^{-\frac{(N+1)2^{-d}-(d-1)}{4d}+\epsilon} Q^{2-m(d+2n)+\frac{5md(N+1)}{2^{d-1}(d-1)}+\frac{(N+1)m2^{-d}-m(d-1)}{2d}-\epsilon}.$$

Now assuming Theorem 5.5, we'll demonstrate how to establish the main result.

Proof of Theorem 5.1. For each p denote by $\bar{A}_p$ the reduction modulo p of the affine cone of A (as in the proof of lemma Lemma 2.3) and by $\bar{A}$ the collection of all these reductions. We start by breaking into dyadic intervals

$$\#\{x \in A : H(x) \leq B\} \leq \sum_{\substack{B_1 \cdots B_n \leq B^{\frac{1}{N+1-d}} \\ \text{dyadic}}} \mathbf{N}(X^n, \mathbf{B}, \bar{A}).$$

It suffices to prove the estimate in Theorem 5.1 when A is either a type I or type II thin set. This will follow from the $m = 1$ case of Theorem 5.5. If A is a type I thin set then there is some proper, Zariski closed subset

$Z \subset X^n$ which describes it. By [3, Lemma 3.8] for all primes p, we have $\#Z(\mathbb{F}_p) \ll_Z p^{n(N+1)-1}$. It follows that there exists a constant $c > 0$ such that $\omega_p \geq 1 - \frac{c}{p}$, and thus $\frac{\omega_p}{1-\omega_p} \geq \frac{p}{c} - 1$. This means

$$G(Q) \geq \sum_{q \leq Q} \mu^2(q) q \prod_{p|q} \left(\frac{1}{c} - \frac{1}{p} \right) \gg_{\epsilon, Z} Q^{2-\epsilon}.$$

Similarly, if A is a type II thin set then [3, Lemma 3.8] implies there is a positive density set of primes $\mathcal{P}$ and a constant $\eta > 0$ such that $\frac{\omega_p}{1-\omega_p} \geq \eta$, for large enough $p \in \mathcal{P}$. It follows, as in the proof of Lemma 2.3, that there exists $\gamma \in [0, 1)$ such that

$$G(Q) \gg_{\epsilon, \mathcal{P}} Q(\log Q)^{-\gamma}.$$

In either case, Theorem 5.5 (with $m = 1$) implies that

$$\mathbf{N}(X^n, \mathbf{B}, \bar{A}) \ll_{A, X} (B_1 \cdots B_n)^{N+1-d} \left(Q^{-1}(\log Q)^\gamma + E_1 + E_2 \right).$$

Now setting $Q = \min_j \{B_j\}^\delta$ for $\delta > 0$ sufficiently small gives the bound

$$\#\{x \in A : H(x) \leq B\}$$
$$\ll_{A, X} (\log B)^\gamma \sum_{\substack{B_1 \cdots B_n \leq B^{\frac{1}{N+1-d}} \\ \text{dyadic}}} (B_1 \cdots B_n)^{N+1-d} \min_j B_j^{-\delta},$$

from which the result follows. $\qquad\square$

The rest of this section is dedicated to the proof of Theorem 5.5. We count points $x \in X^n(\mathbb{Q})$ via their representatives $\mathbf{x} = (\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(n)}) \in \mathbb{Z}^{n(N+1)}$ where the $\mathbf{x}^{(j)}$ are primitive vectors with $F(\mathbf{x}^{(j)}) = 0$. Passing to the affine cone, we see that we may bound $\mathbf{N}(X^n, \mathbf{B}, \Omega)$ by

$$\#\left\{ \mathbf{x} \in \left(\mathbb{Z}_{\text{prim}}^{N+1} \right)^n : B_j/2 < \|\mathbf{x}^{(j)}\| \leq B_j, F(\mathbf{x}) = 0 \text{ and } \mathbf{x} \bmod p^m \in \Omega_{p^m} \ \forall \, p \right\}.$$

This quantity can be bounded above using the Selberg sieve. Let

$$P(Q) = \prod_{\substack{p < Q \\ \omega_p > 0 \\ p \nmid \text{disc}(F)}} p \quad \text{and} \quad \Lambda(\mathbf{x}) = \prod_{\substack{p | P(Q) \\ \mathbf{x} \bmod p^m \in \Omega_{p^m}^C}} p,$$

where $\Omega_{p^m}^C = \widehat{X^n} \left(\mathbb{Z}/p^m\mathbb{Z} \right) \setminus \Omega_{p^m}$.

Define a sequence $\mathcal{A} = (a_\lambda)$ of non-negative numbers, supported on finitely many integers λ, by

$$a_\lambda = \sum_{\substack{\mathbf{x} \in (\mathbb{Z}_{\text{prim}}^{(N+1)})^n \\ F(\mathbf{x}^{(j)})=0 \\ \Lambda(\mathbf{x})=\lambda}} \prod_{j=1}^n \prod_{i=0}^N W\left(\frac{x_i^{(j)}}{B_j} \right),$$

for W some appropriate smooth, compactly supported weight function. Then,

$$\sum_{(\lambda, P(Q))=1} a_\lambda = \sum_{\substack{\mathbf{x} \in (\mathbb{Z}_{\mathrm{prim}}^{(N+1)})^n \\ F(\mathbf{x}^{(j)})=0 \\ (\Lambda(\mathbf{x}), P(Q))=1}} \prod_{j=1}^{n} \prod_{i=0}^{N} W\left(\frac{x_i^{(j)}}{B_j}\right)$$

$$= \sum_{\substack{\mathbf{x} \in (\mathbb{Z}_{\mathrm{prim}}^{(N+1)})^n \\ F(\mathbf{x}^{(j)})=0 \\ \mathbf{x} \bmod p^m \in \Omega_{p^m} \forall p | P(Q)}} \prod_{j=1}^{n} \prod_{i=0}^{N} W\left(\frac{x_i^{(j)}}{B_j}\right).$$

Theorem 5.5 will follow from a suitable upper bound for the a_λ sum. This is achieved by an appeal to Selberg's upper bound sieve as expressed in [9, Theorem 7.1]. In order to apply this, we need an expression of the form

$$\sum_{\lambda \equiv 0 \bmod q} a_\lambda = g(q)Y + r_k(\mathcal{A}),$$

for a constant Y and suitable multiplicative function g and small remainder term $r_q(\mathcal{A})$. This information will be provided by the following result of Schindler–Sofos [16, Lemma 2.1].

Lemma 5.6. *Let $g \in \mathbb{Z}[x_0, \ldots, x_N]$ a polynomial of degree $d \geq 2$. Fix $R > 0$ and $\mathbf{z} \in \mathbb{Z}^{N+1}$. If $N > 2^d(d-1)$, then one has*

$$\sum_{\substack{\mathbf{x} \in \mathbb{Z}^{N+1} \\ g(\mathbf{x})=0}} \prod_{i=0}^{N} W\left(\frac{x_i}{R} - z_i\right) - \mathfrak{S}\mathfrak{J}_W$$

$$\ll_\epsilon R^{N-d+\frac{1}{2}} + \|g\|^{\frac{5(N+1)}{2^d(d-1)} - \frac{3}{2}} R^{N+1-d+\epsilon - \frac{(N+1)2^{-d}-(d-1)}{4d}},$$

where

$$\mathfrak{J}_W = \int_{-\infty}^{\infty} \int_{\mathbb{R}^{N+1}} e(\gamma g(\mathbf{u})) \prod_{i=0}^{N} W\left(\frac{u_i}{R}\right) \mathrm{d}\mathbf{u}\mathrm{d}\gamma$$

$$\mathfrak{S} = \prod_p \sigma_p(g).$$

Here σ_p is the local density defined as

$$\sigma_p(g) := \lim_{\ell \to \infty} p^{-\ell N} \#\{\mathbf{x} \bmod p^\ell : g(\mathbf{x}) \equiv 0 \bmod p^\ell\}.$$

Let $M = q^m$ and $\Omega_M = \prod_{p^m || M} \Omega_{p^m}$. Then for $q \mid P(Q)$, we have

$$
\sum_{\lambda \equiv 0 \bmod q} a_\lambda = \sum_{\substack{\mathbf{x} \in (\mathbb{Z}^{(N+1)}_{\text{prim}})^n \\ F(\mathbf{x}^{(j)}) = 0 \\ \mathbf{x} \bmod M \in \Omega_M^C}} \prod_{j=1}^n \prod_{i=0}^N W\left(\frac{x_i^{(j)}}{B_j}\right)
$$

$$
= \sum_{\mathbf{a} \in \Omega_M^C} \sum_{\substack{\mathbf{y} \in (\mathbb{Z}^{(N+1)}_{\text{prim}})^n \\ F(\mathbf{a}^{(j)} + M\mathbf{y}^{(j)}) = 0}} \prod_{j=1}^n \prod_{i=0}^N W\left(\frac{a_i^{(j)} + My_i^{(j)}}{B_j}\right)
$$

$$
= \sum_{\mathbf{a} \in \Omega_M^C} \prod_{j=1}^n \sum_{\substack{\mathbf{y}^{(j)} \in (\mathbb{Z}^{(N+1)}_{\text{prim}})^n \\ F(\mathbf{a}^{(j)} + M\mathbf{y}^{(j)}) = 0}} \prod_{i=0}^N W\left(\frac{a_i^{(j)} + My_i^{(j)}}{B_j}\right).
$$

Now this is in a form where we may apply Lemma 5.6, setting $R = \frac{B_j}{M}$, $z_i = \frac{a_i^{(j)}}{B_j}$ and $g(\mathbf{y}^{(j)}) = F(\mathbf{a}^{(j)} + M\mathbf{y}^{(j)})$. Therefore the inner sum over $\mathbf{y}^{(j)}$ can be written as

$$
\mathfrak{S}\mathfrak{J}_{W,h_j} + O\left(\left(\frac{B_j}{M}\right)^{N-d+\frac{1}{2}} + M^{\frac{5d(N+1)}{2^d(d-1)} - \frac{3d}{2}}\left(\frac{B_j}{M}\right)^{N+1-d+\epsilon - \frac{(N+1)2^{-d} - (d-1)}{4d}}\right).
$$

Observe that

$$
\mathfrak{J}_{W,B_j} = \frac{B_j^{N+1-d}}{M^{N+1}} \int_{-\infty}^\infty \int_{\mathbb{R}^{N+1}} e(\beta F(\mathbf{u})) \prod_{i=0}^N W(u_i) \, \mathrm{d}\mathbf{u} \, \mathrm{d}\beta =: \frac{B_j^{N+1-d}}{M^{N+1}} \mathfrak{J}.
$$

The local factors σ_p in the singular series are given by

$$
\sigma_p((F(\mathbf{a}^{(j)} + p^m \mathbf{y}^{(j)}))
$$
$$
= \lim_{\ell \to \infty} p^{-\ell N} \# \left\{\mathbf{y} \bmod p^\ell : F(\mathbf{a}^{(j)} + p^m \mathbf{y}^{(j)}) \equiv 0 \bmod p^\ell\right\}.
$$

If $p \nmid M$ then $\sigma_p(F(\mathbf{a}^{(j)} + p^m \mathbf{y}^{(j)})) = \sigma_p$, where σ_p is the usual Hardy–Littlewood density associated to F. If p divides M, it cannot divide $\mathrm{disc}(F)$. Let

$$
\mathbf{N}(\ell) := \#\{\mathbf{y} \bmod p^\ell : F(\mathbf{a}^{(j)} + p^m \mathbf{y}) \equiv 0 \bmod p^\ell\},
$$

it follows via Hensel's lemma that for $\ell > m$ we have $\mathbf{N}(\ell) = p^N \mathbf{N}(\ell - 1)$, and thus $\sigma_p(F(\mathbf{a}^{(j)} + p^m \mathbf{y})) = p^m$. Hence, the singular series factorises as

$$
\mathfrak{S} = \prod_{p \nmid M} \sigma_p \prod_{p^m || M} p^m,
$$

for any $\mathbf{a}^{(j)}$. Therefore

$$\frac{\mathfrak{S}}{M^{N+1}} = \prod_p \sigma_p \prod_{p^m || M} \frac{1}{p^{mN} \sigma_p}.$$

It follows from Hensel's lemma (as above) that

$$\#\widehat{X}(\mathbb{Z}/p^\ell\mathbb{Z}) = p^N \#\widehat{X}(\mathbb{Z}/p^{\ell-1}\mathbb{Z})$$

for any $\ell > 1$. Using this and Deligne's bound, we conclude

$$\frac{\mathfrak{S}}{M^{N+1}} = \prod_p \sigma_p \prod_{p^m || M} \frac{1}{\#\widehat{X}\left(\mathbb{Z}/p^m\mathbb{Z}\right)\left(1 + O(p^{-N/2+1/2})\right)}$$

$$= c_1 \prod_{p^m || M} \frac{1}{\#\widehat{X}\left(\mathbb{Z}/p^m\mathbb{Z}\right)},$$

for some absolute constant c_1. Taking the product over all j we get a main term of size

$$\#\Omega_M^C c_1^n \mathfrak{J}^n \prod_{p^m || M} \frac{1}{\#\widehat{X^n}\left(\mathbb{Z}/p^m\mathbb{Z}\right)} (B_1 \cdots B_n)^{N+1-d}.$$

Therefore, there exists a constant c_2 (depending at most on W and F) such that

$$\sum_{\lambda \equiv 0 \bmod q} a_\lambda = c_2 g(q)(B_1 \cdots B_n)^{N+1-d} + O\left(r_q(\mathcal{A})\right),$$

where

$$g(q) = \prod_{p|q} \frac{\#\Omega_{p^m}^C}{\#\widehat{X^n}\left(\mathbb{Z}/p^m\mathbb{Z}\right)} = \prod_{p|q} \omega_p.$$

The remainder term $r_q(\mathcal{A})$ is given by $\#\Omega_M^C \left(\frac{B_1 \cdots B_n}{M^n}\right)^{N+1-d}$ multiplied by

$$\left(\frac{\min_j\{B_j\}}{M}\right)^{-\frac{1}{2}} M^{-d(n-1)}$$

$$+ M^{\frac{5d(N+1)}{2^d(d-1)} - \frac{3d}{2} - d(n-1)} \left(\frac{\min_j\{B_j\}}{M}\right)^{-\frac{(N+1)2^{-d}-(d-1)}{4d} + \epsilon}.$$

We estimate $\#\Omega_M^C$ using the following simple bound

$$\#\Omega_M^C \ll \prod_{p^m || M} \#\widehat{X^n}(\mathbb{Z}/p^m\mathbb{Z}) \ll M^{nN}.$$

It just remains to compute the error terms

$$\frac{(B_1 \cdots B_n)^{N+1-d}}{\min_j\{B_j\}^{1/2}} \sum_{q \leq Q^2} \tau_3(M) q^{m(d+\frac{1}{2}-n(N+1))} \#\Omega_{q^m}^C$$

$$\ll_\epsilon \frac{(B_1 \cdots B_n)^{N+1-d}}{\min_j\{B_j\}^{1/2}} \sum_{q \leq Q^2} q^{m(d+\frac{1}{2}-n)+\frac{\epsilon}{2}}$$

$$\ll_\epsilon \frac{(B_1 \cdots B_n)^{N+1-d}}{\min_j\{B_j\}^{1/2}} Q^{m(2d-2n+1)+2+\epsilon}$$

and

$$\frac{(B_1 \cdots B_n)^{N+1-d}}{\min_j\{B_j\}^{\frac{(N+1)2^{-d}-(d-1)}{4d}-\epsilon}}$$

$$\times \sum_{q \leq Q^2} \tau_3(M) q^{m\left(\frac{5d(N+1)}{2^d(d-1)} - \frac{d}{2} - n(N+1) + \frac{(N+1)2^{-d}-(d-1)}{4d} - \epsilon\right)} \#\Omega_{q^m}^C$$

$$\ll_\epsilon \frac{(B_1 \cdots B_n)^{N+1-d}}{\min_j\{B_j\}^{\frac{(N+1)2^{-d}-(d-1)}{4d}-\epsilon}} Q^{2-m(d+2n)+\frac{5md(N+1)}{2^{d-1}(d-1)}+\frac{(N+1)m2^{-d}-m(d-1)}{2d}-\epsilon}.$$

This finishes the proof of Theorem 5.5.

References

[1] R. BEHESHTI & N. MOHAN KUMAR, "Spaces of rational curves on complete intersections", *Compos. Math.* **149** (2013), no. 6, p. 1041-1060.

[2] B. J. BIRCH, "Forms in many variables", *Proc. R. Soc. Lond., Ser. A* **265** (1962), p. 245-263.

[3] T. BROWNING & D. LOUGHRAN, "Sieving rational points on varieties", *Trans. Am. Math. Soc.* **371** (2019), no. 8, p. 5757-5785.

[4] T. BROWNING & W. SAWIN, "Free rational curves on low degree hypersurfaces and the circle method", https://arxiv.org/abs/1810.06882, 2018.

[5] T. BROWNING & P. VISHE, "Rational curves on smooth hypersurfaces of low degree", *Algebra Number Theory* **11** (2017), no. 7, p. 1657-1675.

[6] I. COSKUN & E. RIEDL, "Normal bundles of rational curves on complete intersections", *Commun. Contemp. Math.* **21** (2019), no. 2, article ID 1850011 (29 pages).

[7] O. DEBARRE, *Higher-dimensional algebraic geometry*, Universitext, Springer, 2001.

[8] J. FRANKE, Y. I. MANIN & Y. TSCHINKEL, "Rational points of bounded height on Fano varieties", *Invent. Math.* **95** (1989), no. 2, p. 421-435.

[9] J. FRIEDLANDER & H. IWANIEC, *Opera De Cribro*, Colloquium Publications, vol. 57, American Mathematical Society, 2010.

[10] J. HARRIS, "Galois groups of enumerative problems", *Duke Math. J.* **46** (1979), no. 4, p. 685-724.

[11] J. HARRIS, M. ROTH & J. STARR, "Rational curves on hypersurfaces of low degree", *J. Reine Angew. Math.* **571** (2004), p. 73-106.

[12] M. KONTSEVICH & Y. I. MANIN, "Gromov–Witten classes, quantum cohomology, and enumerative geometry", *Commun. Math. Phys.* **164** (1994), no. 3, p. 525-562.

[13] E. KOWALSKI, *The large sieve and its applications*, Cambridge Tracts in Mathematics, vol. 175, Cambridge University Press, 2008.

[14] Z. RAN, "Enumerative geometry of singular plane curves", *Invent. Math.* **97** (1989), no. 3, p. 447-465.

[15] E. RIEDL & D. YANG, "Kontsevich spaces of rational curves on Fano hypersurfaces", *J. Reine Angew. Math.* **748** (2019), p. 207-225.

[16] D. SCHINDLER & E. SOFOS, "Sarnak's saturation problem for complete intersections", *Mathematika* **65** (2019), no. 1, p. 1-56.

[17] J.-P. SERRE, *Topics in Galois theory*, A K Peters, 2016.

[18] M. SHEN, "On the normal bundles of rational curves on Fano 3-folds", *Asian J. Math.* **16** (2012), no. 2, p. 237-270.

[19] C. SKINNER, "Forms over number fields and weak approximation", *Compos. Math.* **106** (1997), no. 1, p. 11-29.

[20] I. VAINSENCHER, "Enumeration of n-fold tangent hyperplanes to a surface", *J. Algebr. Geom.* **4** (1995), no. 3, p. 503-526.

[21] A. VÁRILLY-ALVARADO & D. ZYWINA, "Arithmetic E_8 lattices with maximal Galois action", *LMS J. Comput. Math.* **12** (2009), p. 144-165.

[22] E. WIRSING, "Das asymptotische Verhalten von Summen über multiplikative Funktionen. II", *Acta Math.* **18** (1967), p. 411-467.

[23] H. G. ZEUTHEN, "Almindelige Egenskaber ved systemer af plane Kurver", *Kjobenhavn. Vidensk. Selsk.* **IV** (1873), p. 285-393.

David HOLMES
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
2300RA Leiden, Netherlands
E-mail: `holmesdst@math.leidenuniv.nl`

Nick ROME
School of Mathematics
University of Bristol
Bristol, BS8 1TW, UK
E-mail: `nick.rome@bristol.ac.uk`