Algebra & Number Theory

Volume 14
2020
No. 8

The dimension growth conjecture, polynomial in the degree and without logarithmic factors

Wouter Castryck, Raf Cluckers, Philip Dittmann and Kien Huu Nguyen

msp

msp

ALGEBRA AND NUMBER THEORY 14:8 (2020)
https://doi.org/10.2140/ant.2020.14.2261

The dimension growth conjecture, polynomial in the degree and without logarithmic factors

Wouter Castryck, Raf Cluckers, Philip Dittmann and Kien Huu Nguyen

We study Heath-Brown's and Serre's dimension growth conjecture (proved by Salberger) when the degree d grows. Recall that Salberger's dimension growth results give bounds of the form $O_{X,\varepsilon}(B^{\dim X+\varepsilon})$ for the number of rational points of height at most B on any integral subvariety X of $\mathbb{P}^n_{\mathbb{Q}}$ of degree $d \geq 2$, where one can write $O_{d,n,\varepsilon}$ instead of $O_{X,\varepsilon}$ as soon as $d \geq 4$. We give the following simplified and strengthened forms of these results: we remove the factor B^{ε} as soon as $d \geq 5$, we obtain polynomial dependence on d of the implied constant, and we give a simplified, self-contained approach for $d \geq 16$. Along the way, we improve the well-known bounds due to Bombieri and Pila on the number of integral points of bounded height on affine curves and those by Walsh on the number of rational points of bounded height on projective curves. This leads to a slight sharpening of a recent estimate due to Bhargava, Shankar, Taniguchi, Thorne, Tsimerman and Zhao on the size of the 2-torsion subgroup of the class group of a degree d number field. Our treatment builds on recent work by Salberger, who brings in many primes in Heath-Brown's variant of the determinant method, and on recent work by Walsh and by Ellenberg and Venkatesh who bring in the size of the defining polynomial. We also obtain lower bounds showing that one cannot do better than polynomial dependence on d.

1. Introduction and main results

1.1. Following a question raised by Heath-Brown [1983, page 227] in the case of hypersurfaces, Serre [1992, page 27; 1989, page 178] twice formulated a question about rational points on a projective variety X of degree d, which was dubbed the dimension growth conjecture by Browning [2009]. The question puts forward concrete upper bounds on the number of such points with height at most B, as a function of B. This dimension growth conjecture is now a theorem due to Salberger [2013] (and others under various conditions on d); moreover, for $d \geq 4$ Salberger obtains complete uniformity in X, keeping only

The authors would like to thank Gal Binyamini, Jonathan Pila, Arne Smeets, Jan Tuitman, and Alex Wilkie for interesting discussions on the topics of the paper; Per Salberger for sharing his preprint with us and for interesting exchanges of ideas; and Floris Vermeulen for a number of helpful remarks on earlier versions of this article. Castryck, Cluckers, and Nguyen were partially supported by the European Research Council under the European Community's Seventh Framework Programme (FP7/2007-2013) with ERC Grant Agreement nr. 615722 MOTMELSUM and thank the Labex CEMPI (ANR-11-LABX-0007-01). Castryck is affiliated on a voluntary basis with the Department of Mathematics: Algebra and Geometry at Ghent University. Cluckers and Dittmann were partially supported by KU Leuven IF C14/17/083. Nguyen is partially supported by the Fund for Scientific Research – Flanders (Belgium) (FWO) 12X3519N.

MSC2010: primary 11D45; secondary 11G35, 14G05.

Keywords: dimension growth conjecture, rational points of bounded height.

d and the dimension of the ambient projective space fixed, thereby confirming a variant that had been proposed by Heath-Brown.

We remove from these bounds the factors of the form B^ε when the degree d is at least 5, without creating a factor $\log B$, while moreover obtaining polynomial dependence on d of the constants. The approach with polynomial dependence on d is implemented in all auxiliary results as well, and this has the pleasant consequence of yielding a more direct and self-contained proof of the dimension growth conjecture for d at least 16 (our treatment of dimension growth for $5 \leq d \leq 15$ is not self-contained and uses [Browning et al. 2006] when $d > 5$ and [Salberger 2013] for $d = 5$). Theorems 2 and 3 below give such improvements to bounds by Walsh [2015] on the number of rational points of bounded height on integral projective curves, and to bounds of Bombieri and Pila [1989, Theorem 5] on the number of integral points of bounded height on affine irreducible curves, with rather low powers of d, compared to [Walkowiak 2005]. Polynomial dependence on d for projective curves as in Theorem 2 is useful for effective versions of Hilbert's irreducibility theorem and for Malle's conjecture; see [Dèbes and Walkowiak 2008; Motte 2018; Walkowiak 2005].

The possibility of polynomial dependence on d came to us via a question raised by Yomdin (see below Remark 3.8 of [Burguet et al. 2015]) in combination with the determinant method with smooth parametrizations as in [Pila 2010], refined in [Cluckers et al. 2020b], and via the work by Binyamini and Novikov [2019, Theorem 6]. The removal of the factor B^ε without needing $\log B$ was recently achieved by Walsh [2015, Theorems 1.1, 1.2, 1.3] who combines ideas by Ellenberg and Venkatesh [2005] with the determinant method based on p-adic approximation (rather than on smooth maps) due to Heath-Brown [2002], refined in [Salberger 2013]. In fact, polynomial dependence on d for the case of projective curves was also achieved in [Motte 2018] and [Walkowiak 2005], with a higher exponent. One cannot achieve dependence on d better than polynomial, as shown by the lower bounds from Proposition 5 below. Let us mention that positive characteristic analogues, over $\mathbb{F}_q[t]$, are obtained in [Cluckers et al. 2020a] and [Sedunova 2017] for curves, and in [Vermeulen 2020] for dimension growth.

1.2. Let us make all this more precise. We study the number

$$N(X, B)$$

of rational points of height at most B on subvarieties X of $\mathbb{P}^n$ defined over $\mathbb{Q}$. Here, the height $H(x)$ of a $\mathbb{Q}$-rational point x in $\mathbb{P}^n$ is given by

$$H(x) = \max(|x_0|, \ldots, |x_n|)$$

for an $(n+1)$-tuple $(x_0, \ldots, x_n)$ of integers x_i which are homogeneous coordinates for x and have greatest common divisor equal to 1.

Salberger [2013] proved the so-called dimension growth conjecture raised as a question by Serre [1992, page 27] following a question of Heath-Brown [1983, page 227].

Dimension growth [Salberger 2013, Theorem 0.1]. *If X is an integral projective variety of degree $d \geq 2$ defined over $\mathbb{Q}$, then*

$$N(X, B) \leq O_{X,\varepsilon}(B^{\dim X+\varepsilon}).$$

One should compare the bound for $N(X, B)$ from this theorem to the trivial upper bound $O_{d,n}(B^{\dim X+1})$ that follows from Lemma 4.1.1 below.

A variant of this question from [Serre 1989, page 178] replaces the factor B^{ε} by $\log(B)^c$ for some c depending on X, see Section 1.4 below.

Heath-Brown [2002] introduces a form of this conjecture with uniformity in X for fixed d and n, and he develops a new variant of the determinant method using p-adic approximation instead of smooth parametrizations as in [Bombieri and Pila 1989; Binyamini and Novikov 2019; Pila 2010; Cluckers et al. 2020b]. In [Salberger 2013], Salberger proves this uniform version of the dimension growth conjecture for $d \geq 4$.

Uniform dimension growth [Salberger 2013, Theorem 0.3]. *For $X \subseteq \mathbb{P}^n_{\mathbb{Q}}$ an integral projective variety of degree $d \geq 4$, one has*

$$N(X, B) \leq O_{d,n,\varepsilon}(B^{\dim X+\varepsilon}).$$

Almost all situations of this uniform dimension growth had been obtained previously in [Heath-Brown 2002] and [Browning et al. 2006], including the case $d = 2$ but without the (difficult) cases $d = 4$ and $d = 5$. Our main contributions are to make the dependence on d polynomial, to remove the factor B^{ε} without having to use factors $\log B$, and to provide relatively self-contained proofs for large degree, with main result as follows.

Theorem 1 (uniform dimension growth). *Given $n > 1$, there exist constants $c = c(n)$ and $e = e(n)$, such that for all integral projective varieties $X \subseteq \mathbb{P}^n_{\mathbb{Q}}$ of degree $d \geq 5$ and all $B \geq 1$ one has*

$$N(X, B) \leq cd^e B^{\dim X}. \tag{1-2-1}$$

As mentioned earlier, one cannot do better than polynomial dependence on d, see the lower bounds from Proposition 5 and Section 6 below.

We heavily rework results and methods of Salberger, Walsh, Ellenberg and Venkatesh, Heath-Brown, and Browning, and use various explicit estimates for Hilbert functions, for certain universal Noether polynomials as in [Ruppert 1986], and for solutions of linear systems of equations over $\mathbb{Z}$ from [Bombieri and Vaaler 1983].

1.3. ***Rational points on curves and hypersurfaces.*** Let us make precise some of our improvements for counting points on curves and surfaces, which are key to Theorem 1. We obtain the following improvement of Walsh's Theorem 1.1 [2015].

Theorem 2 (projective curves). *Given $n > 1$, there exists a constant $c = c(n)$ such that for all $d > 0$ and all integral projective curves $X \subseteq \mathbb{P}^n_{\mathbb{Q}}$ of degree d and all $B \geq 1$ one has*

$$N(X, B) \leq cd^4 B^{2/d}.$$

In view of Proposition 5 below, the exponent 4 of d in Theorem 2 can perhaps be lowered, but cannot become lower than 2 in general. Several adaptations of results and proofs of [Walsh 2015] are key to our treatment and are developed in Section 3.

For affine counting we use the following notation for a variety $X \subseteq \mathbb{A}^n_{\mathbb{Q}}$ and a polynomial f in $\mathbb{Z}[y_1, \ldots, y_n]$:

$$N_{\mathrm{aff}}(X, B) := \#\{x \in \mathbb{Z}^n \mid |x_i| \leq B \text{ for each } i \text{ and } x \in X(\mathbb{Q})\},$$

and

$$N_{\mathrm{aff}}(f, B) := \#\{x \in \mathbb{Z}^n \mid |x_i| \leq B \text{ for each } i \text{ and } f(x) = 0\}.$$

By a careful elaboration of the argument from [Ellenberg and Venkatesh 2005, Remark 2.3] and an explicit but otherwise classical projection argument, we find the following improvement of bounds by Bombieri and Pila [1989, Theorem 5] and later sharpenings by Pila [1995; 1996], Walkowiak [2005], Ellenberg and Venkatesh [2005, Remark 2.3], Binyamini and Novikov [2019, Theorem 6], and others.

Theorem 3 (affine curves). *Given $n > 1$, there exists a constant $c = c(n)$ such that for all $d > 0$, all integral affine curves $X \subseteq \mathbb{A}^n_{\mathbb{Q}}$ of degree d, and all $B \geq 1$ one has*

$$N_{\mathrm{aff}}(X, B) \leq cd^3 B^{1/d}(\log B + d).$$

A variant of Theorem 3 is given in Section 4, where $\log B$ is absent and instead the size of the coefficients of the polynomial f defining the affine planar curve comes in.

It is well-known that Theorems 1, 2, and 3 imply similar bounds for varieties defined and integral over $\overline{\mathbb{Q}}$ (instead of $\mathbb{Q}$), by intersecting with a Galois conjugate and using a trivial bound, see Lemma 4.1.3. The following improves Theorem 0.4 of [Salberger 2013] and is key to Theorem 1. It can be seen as an affine form of the dimension growth theorem, for hypersurfaces.

Theorem 4 (affine hypersurfaces). *Given $n > 2$, there exist constants $c = c(n)$ and $e = e(n)$, such that for all polynomials f in $\mathbb{Z}[y_1, \ldots, y_n]$ whose homogeneous part of highest degree $h(f)$ is irreducible over $\overline{\mathbb{Q}}$ and whose degree d is at least 5, one has*

$$N_{\mathrm{aff}}(f, B) \leq cd^e B^{n-2}.$$

One should compare the bound from this theorem to the trivial upper bound $O_{d,n}(B^{n-1})$ from Lemma 4.1.1.

1.4. ***Example and a question.*** In Serre's example [1989, page 178] of the degree 2 surface in $\mathbb{P}^3$ given by the equation $xy = zw$, the logarithmic factor $\log B$ cannot be dispensed with in the upper bound. Hence, (1-2-1) of Theorem 1 cannot hold for $d = 2$ in general. For $d = 3$, the bound from (1-2-1) remains

wide open since already uniformity in $X \subseteq \mathbb{P}^n$ of degree 3 is not known for the uniform dimension growth with $O_{d,n,\varepsilon}(B^{\dim X+\varepsilon})$ as upper bound (see [Salberger 2015; 2013] for subtleties when $d = 3$). For $d = 4$, one may investigate whether (1-2-1) of Theorem 1 remains true, that is, without involving a factor B^ε or $\log B$.

1.5. ***Lower bounds.*** In Section 6 we discuss the necessity of the polynomial dependence on d in the above theorems.

Proposition 5. *For each integer $d > 0$ there is an integral projective curve $X \subseteq \mathbb{P}^2$ of degree d and an integer $B \geq 1$ such that*

$$\tfrac{1}{5}d^2B^{2/d} \leq N(X, B).$$

In particular, in the statement of Theorem 2 it is impossible to replace the factor d^4 with an expression in d which is $o(d^2)$.

Similarly we show that it is impossible to replace the quartic dependence on d of the bound from Theorem 3 by a function in $o(d^2/\log d)$. We also show that in Theorems 1 and 4 we cannot take $e < 1$ or $e < 2$, respectively.

1.6. ***An application.*** Our bounds with improved exponent can be used as substitutes for those by Salberger, Bombieri and Pila, and Walsh upon which they improve, potentially leading to stronger statements. A very recent example of such an application is Bhargava, Shankar, Taniguchi, Thorne, Tsimerman and Zhao's bound [Bhargava et al. 2020, Theorem 1.1] on the number $h_2(K)$ of 2-torsion elements in the class group of a degree $d > 2$ number field K, in terms of its discriminant Δ_K. Precisely, they show that

$$h_2(K) \leq O_{d,\varepsilon}(|\Delta_K|^{1/2-1/(2d)+\varepsilon}),$$

thereby obtaining a power saving over the trivial bound coming from the Brauer–Siegel theorem. This power saving is mainly accounted for by an application of Bombieri and Pila's bound [1989, Theorem 5]. In Section 4 we explain how our improved bound stated in Theorem 3, or rather its refinement stated in Corollary 4.2.4, allows for removal of the factor $|\Delta_K|^\varepsilon$ as soon as d is odd; if d is even then we can replace it by $\log|\Delta_K|$.

Theorem 6. *For all degree $d > 2$ number fields K we have*

$$h_2(K) \leq O_d(|\Delta_K|^{1/2-1/(2d)}(\log|\Delta_K|)^{1-(d \bmod 2)}).$$

It is possible to make the hidden constant explicit, but targeting polynomial growth seems of lesser interest since $|\Delta_K|$ is itself bounded from below by an exponential expression in d, coming from Minkowski's bound.

1.7. ***Structure of the paper.*** In Section 2 we render several results of Salberger [2007] explicit in terms of the degrees and dimensions involved. In Section 3 we similarly adapt the results of Walsh [2015]. Section 4 completes the proofs of our main results in the hypersurface case, which is complemented by

Section 5, in which we discuss projection arguments from [Browning et al. 2006], explicit in the degrees and dimensions, and thus finish the proofs of our main theorems. Finally, in Section 6, we provide lower bounds showing the necessity of polynomial dependence on d in our main results.

2. The determinant method for hypersurfaces

With the aim of improving the results of [Walsh 2015] in the next section, we sharpen some results from Salberger's global determinant method. The main result of this section is Corollary 2.9, which improves on [Salberger 2013, Lemmas 1.4, 1.5] (see also [Walsh 2015, Theorem 2.2]). This mainly depends on making [Salberger 2007, Main Lemma 2.5] in the case of hypersurfaces explicit in its independence of the degree.

Let f be an absolutely irreducible homogeneous polynomial in $\mathbb{Z}[x_0, \dots, x_{n+1}]$ which is primitive, and let X be the hypersurface in $\mathbb{P}^{n+1}_{\mathbb{Q}}$ defined by f. For p a prime number, let X_p denote the reduction of X modulo p, i.e., the hypersurface in $\mathbb{P}^{n+1}_{\mathbb{F}_p}$ described by the reduction of $f \bmod p$.

Lemma 2.1 (Lemma 2.3 of [Salberger 2007], explicit for hypersurfaces). *Let A be the stalk of X_p at some $\mathbb{F}_p$-point P of multiplicity μ and let $\mathfrak{m}$ be the maximal ideal of A. Let $g_{X,P} : \mathbb{Z}_{>0} \to \mathbb{Z}$ be the function given by $g_{X,P}(k) = \dim_{A/\mathfrak{m}} \mathfrak{m}^k/\mathfrak{m}^{k+1}$ for $k > 0$. Then one has*

$$g(k) = \binom{n+k}{n} \text{ for } k < \mu$$

and

$$g(k) = \binom{n+k}{n} - \binom{n+k-\mu}{n} \text{ for } k \geq \mu.$$

In particular,

$$g(k) \leq \frac{\mu k^{n-1}}{(n-1)!} + O_n(k^{n-2})$$

for all $k \geq 1$, where the implied constant depends only on n, as indicated.

Proof. The function g is identical to the Hilbert function of the projectivized tangent cone of X_p at P, which is a degree μ hypersurface in $\mathbb{P}^n$. This gives the explicit expression for g, so it only remains to prove the estimate.

Consider first $k < \mu$. Then

$$g(k) = \binom{n+k}{n} = \frac{k^n}{n!} + \frac{(n+1)k^{n-1}}{2(n-1)!} + O_n(k^{n-2}).$$

Since $\mu > k$, for $k \geq n$ we immediately obtain the desired inequality, and the k between 1 and n are covered by choosing the constant large enough.

Now consider $k \geq \mu$. Write $p(X)$ for the polynomial $\binom{n+X}{n}$ and a_i for its coefficients. Then

$$p(k) - p(k-\mu) = a_n(k^n - (k-\mu)^n) + a_{n-1}(k^{n-1} - (k-\mu)^{n-1}) + O_n(k^{n-2}).$$

Observe that $a_n = 1/n!$, $a_{n-1} = (n+1)/(2(n-1)!) = a_n(n+1)n/2$, and write

$$k^n - (k-\mu)^n = \mu(k^{n-1} + (k-\mu)k^{n-2} + \cdots + (k-\mu)^{n-1})$$

as well as

$$k^{n-1} - (k-\mu)^{n-1} = \mu(k^{n-2} + \cdots + (k-\mu)^{n-2}).$$

Considering $\mu \geq n(n+1)/2$, we have

$$(k-\mu)^i k^{n-1-i} + \frac{(n+1)n}{2}(k-\mu)^{i-1}k^{n-1-i} \leq k^{n-1}$$

for $i \geq 1$, and hence

$$a_n(k^n - (k-\mu)^n) + a_{n-1}(k^{n-1} - (k-\mu)^{n-1}) \leq \frac{\mu}{n!}(k^{n-1} + \cdots + k^{n-1}) = \mu\frac{k^{n-1}}{(n-1)!}$$

as desired.

For μ less than $n(n+1)/2$, one simply bounds $k^{n-1} - (k-\mu)^{n-1} \leq O_n(k^{n-2})$ and the statement follows. □

Lemma 2.2. *Let $c, n, \mu > 0$ be integers. Let $g\colon \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{>0}$ be a function with $g(0) = 1$ and satisfying $g(k) \leq \mu k^{n-1}/(n-1)! + c\mu k^{n-2}$ for $k > 0$. Let $(n_i)_{i\geq 1}$ be the nondecreasing sequence of integers $m \geq 0$ where m occurs exactly $g(m)$ times. Then for any $s \geq 0$ we have*

$$n_1 + \cdots + n_s \geq \left(\frac{n!}{\mu}\right)^{1/n} \frac{n}{n+1} s^{1+1/n} - O_{n,c}(s).$$

This statement is implicitly contained in the proof of [Salberger 2007, Main Lemma 2.5], but we give the full proof to stress that the error term does not depend on μ.

Proof. Note that replacing g by a function which is pointwise larger than g at any point only strengthens the claim, so we may as well assume that

$$g(k) = \frac{\mu}{n!}(k^n - (k-1)^n) + c\mu(k^{n-1} - (k-1)^{n-1})$$

for $k > 0$. Let $G\colon \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$ be given by $G(k) = g(0) + \cdots + g(k) = \frac{\mu}{n!}k^n + c\mu k^{n-1} + 1$. Now

$$\left(\frac{n!}{\mu}\right)^{1/n} \frac{n}{n+1} G(k)^{1+1/n} = \frac{\mu k^{n+1}}{(n-1)!(n+1)} + O_{n,c}(\mu k^n),$$

and

$$0g(0) + \cdots + kg(k) \geq \frac{\mu}{(n-1)!} \sum_{i\leq k} (i^n + O_n(ci^{n-1})) = \frac{\mu}{(n-1)!(n+1)} k^{n+1} + O_{n,c}(\mu k^n).$$

This proves the lemma for $s = G(k)$.

To deduce the result for general $s > 0$, let k be the unique integer with $G(k-1) < s \leq G(k)$, and use

$$n_1 + \cdots + n_s \geq n_1 + \cdots + n_{G(k)} - kg(k) \geq \left(\frac{n!}{\mu}\right)^{1/n} \frac{n}{n+1} G(k)^{1+1/n} - O_{n,c}(\mu k^n)$$
$$\geq \left(\frac{n!}{\mu}\right)^{1/n} \frac{n}{n+1} s^{1+1/n} - O_{n,c}(s). \qquad \square$$

Lemma 2.3. *Consider A as in Lemma 2.1, and let $(n_i(A))_{i\geq 1}$ be the nondecreasing sequence of integers $m \geq 0$ where m occurs exactly $\dim_{A/\mathfrak{m}} \mathfrak{m}^k/\mathfrak{m}^{k+1}$ times. Write $A(s) = n_1(A) + \cdots + n_s(A)$. Then*

$$A(s) \geq \left(\frac{n!}{\mu}\right)^{1/n} \left(\frac{n}{n+1}\right) s^{1+1/n} - O_n(s),$$

where the implied constant only depends on n.

Proof. This is immediate from the last two lemmas. $\square$

As usual, write $\mathbb{Z}_{(p)}$ for the localization of $\mathbb{Z}$ at (the complement of) the prime ideal (p).

Lemma 2.4 (Lemma 2.4 of [Salberger 2007], cited as in the Appendix of [Browning et al. 2006]). *Let R be a noetherian local ring containing $\mathbb{Z}_{(p)}$, $A = R/pR$, and consider ring homomorphisms $\psi_1, \ldots, \psi_s \colon R \to \mathbb{Z}_{(p)}$. Let $r_1, \ldots, r_s$ be elements of R. Then the determinant of the $s \times s$-matrix $(\psi_i(r_j))$ is divisible by $p^{A(s)}$.*

Corollary 2.5 (Main Lemma 2.5 of [Salberger 2007]). *Let $\mathcal{X} \to \operatorname{Spec} \mathbb{Z}$ be the hypersurface in $\mathbb{P}^{n+1}_{\mathbb{Z}}$ cut out by the homogeneous polynomial f as above, so X is the generic fiber of $\mathcal{X}$ and X_p is the special fiber of $\mathcal{X}$ over p.*

Let P be an $\mathbb{F}_p$-point of multiplicity μ on X_p and let $\xi_1, \ldots, \xi_s$ be $\mathbb{Z}$-points on $\mathcal{X}$, given by some primitive integer tuples, with reduction P. Let $F_1, \ldots, F_s$ be homogeneous polynomials in $x_0, \ldots, x_{n+1}$ with integer coefficients.

Then $\det(F_j(\xi_i))$ is divisible by p^e where

$$e \geq \left(\frac{n!}{\mu}\right)^{1/n} \frac{n}{n+1} s^{1+1/n} - O_n(s).$$

Proof. Let P' be the image of P under the closed embedding $X_p \hookrightarrow \mathcal{X}$, and R the stalk of $\mathcal{X}$ at P'. Then R is a noetherian local ring containing $\mathbb{Z}_{(p)}$, and R/pR is the stalk of X_p at P. Since P' is a specialization of all the ξ_i (this is precisely what it means that the ξ_i have reduction P), it makes sense to evaluate an element of R at each ξ_i, giving s ring homomorphisms $R \to \mathbb{Z}_{(p)}$.

The F_i induce $\mathbb{Z}_{(p)}$-valued polynomial functions on an affine neighborhood of P', and hence give elements of R. The statement now follows from the preceding two lemmas. $\square$

Proposition 2.6. *Let $\mathcal{X}$ be as above. Let $\xi_1, \ldots, \xi_s$ be $\mathbb{Z}$-points on $\mathcal{X}$, and $F_1, \ldots, F_s$ be homogeneous polynomials in $n+1$ variables with integer coefficients. Then the determinant Δ of the $s \times s$-matrix*

$(F_i(\xi_j))$ is divisible by p^e, where

$$e \geq (n!)^{1/n} \frac{n}{n+1} \frac{s^{1+1/n}}{n_p^{1/n}} - O_n(s),$$

and where n_p is the number of $\mathbb{F}_p$-points on X_p, counted with multiplicity.

Proof. This is identical to the proof of [Salberger 2013, Lemma 1.4], see also the appendix of [Walsh 2015] — but we have eliminated the dependence of the constant on d. □

Lemma 2.7. *In the situation above, if $p > 27d^4$ and X_p is geometrically integral, i.e., the defining polynomial f has absolutely irreducible reduction modulo p, then $n_p \leq p^n + O_n(d^2 p^{n-1/2})$.*

Proof. By [Cafure and Matera 2006, Corollary 5.6] the number of $\mathbb{F}_p$-points of X_p counted without multiplicity is bounded by

$$\frac{p^{n+1} + (d-1)(d-2)p^{n+1/2} + (5d^2+d+1)p^n - 1}{p-1} \leq p^n + O_n(d^2 p^{n-1/2}).$$

(This uses the lower bound on p and the condition on X_p.)

The singular points of X_p all lie in the algebraic set cut out by f and $\frac{\partial f}{\partial x_0}$, which can be assumed to be nonzero without loss of generality. This is an algebraic set all of whose components have codimension 2 and the sum of the degrees of these components is bounded by d^2. The standard Lang–Weil estimate yields that there are $O_n(d^2 p^{n-1}) \leq O_n(dp^{n-1/2})$ points on this algebraic set and hence at most that many singular points, each of which has multiplicity at most d. Adding this term to the number of points counted without multiplicity yields the claim. □

Lemma 2.8. *In the situation above, with $p > 27d^4$ and X_p geometrically integral, we have $n_p^{1/n}/p - 1 \leq O_n(d^2 p^{-1/2})$.*

Proof. Apply the general inequality $x^{1/n} - 1 \leq x - 1$ for $x \geq 1$. □

We immediately obtain the following from Proposition 2.6.

Corollary 2.9. *The determinant Δ from Proposition 2.6 is divisible by p^e, where*

$$e \geq (n!)^{1/n} \frac{n}{n+1} \frac{s^{1+1/n}}{p + O_n(d^2 p^{1/2})} - O_n(s).$$

This is stated as Theorem 2.2 in [Walsh 2015], but our statement is more precise in terms of the implied constants.

3. Points on projective hypersurfaces à la Walsh

3.1. ***Formulation of main result.*** The following result is the goal of this section and an improvement to Theorem 1.3 of [Walsh 2015]. Call a polynomial f over $\mathbb{Z}$ primitive if the greatest common divisor of its coefficients equals 1. For any f, we write $\|f\|$ for the maximum of the absolute values of the coefficients of f.

Theorem 3.1.1. *Let $n > 0$ be an integer. Then there exists c (depending on n) such that the following holds for all choices of f, d, B. Let f be a primitive irreducible homogeneous polynomial in $\mathbb{Z}[x_0, \dots, x_{n+1}]$ of degree $d \geq 1$, and write X for the hypersurface in $\mathbb{P}^{n+1}_{\mathbb{Q}}$ cut out by f. Choose $B \geq 1$. Then there exists a homogeneous g in $\mathbb{Z}[x_0, \dots, x_{n+1}]$ of degree at most*

$$cB^{(n+1)/(nd^{1/n})} \frac{d^{4-1/n} b(f)}{\|f\|^{1/n \cdot 1/d^{1+1/n}}} + cd^{1-1/n} \log B + cd^{4-1/n},$$

not divisible by f, and vanishing at all points on X of height at most B.

Here the quantity $b(f)$ is defined in Definition 3.2.1; it always satisfies $b(f) \leq O(\max(d^{-2} \log\|f\|, 1))$. The main improvement over [Walsh 2015] lies in the polynomial dependence on the degree d.

We also immediately obtain the following, which is the essential tool for proving Theorem 2.

Corollary 3.1.2. *For any primitive irreducible polynomial $f \in \mathbb{Z}[x_0, x_1, x_2]$ homogeneous of degree d and any $B \geq 1$ we have*

$$N(f, B) \leq cB^{2/d} \frac{d^4 b(f)}{\|f\|^{1/d^2}} + cd \log B + cd^4 \leq c' d^4 B^{2/d},$$

where c, c' are absolute constants.

Proof. Apply Theorem 3.1.1 to obtain a polynomial g, and then apply Bézout's theorem to the curves defined by f and g. This yields the first inequality. For the second inequality we can use that $b(f)/\|f\|^{1/d^2}$ is bounded because $b(f) \leq O(\max(d^{-2} \log\|f\|, 1))$. □

3.2. ***A determinant estimate.*** In this section we want to use the results of Section 2 for a number of primes simultaneously. It is useful to introduce the following measure of the set of primes modulo which an absolutely irreducible polynomial over the integers ceases to be absolutely irreducible.

Definition 3.2.1. For an integer polynomial f in an arbitrary number of variables we set $b(f) = 0$ if f is not absolutely irreducible, and

$$b(f) = \prod_p \exp\left(\frac{\log p}{p}\right)$$

otherwise, where the product is over those primes $p > 27d^4$ such that the reduction of f modulo p is not absolutely irreducible.

For now we work with a degree d hypersurface in $\mathbb{P}^{n+1}$ defined by a primitive polynomial $f \in \mathbb{Z}[x_0, \dots, x_{n+1}]$ which is absolutely irreducible. We first establish a basic estimate on $b(f)$, showing in particular that it is finite.

Theorem 3.2.2 (explicit Noether polynomials, [Ruppert 1986, Satz 4]). *Let $d \geq 2$, $n \geq 3$. There is a collection of homogeneous polynomials Φ in $\binom{n+d}{n}$ variables over $\mathbb{Z}$ of degree $d^2 - 1$, such that*

$$\|\Phi\|_1 \leq d^{3d^2-3} \left[\binom{n+d}{n} 3^d\right]^{d^2-1}$$

(*where* $\|\cdot\|_1$ *denotes the sum of the absolute values of the coefficients*), *and such that the following holds for any polynomial* F *in* $n+1$ *variables homogeneous of degree* d *over any field*:

- *If* F *is not absolutely irreducible, then all the* Φ *vanish when applied to the coefficients of* F, *reducing modulo the characteristic of the ground field if necessary.*
- *If* F *is absolutely irreducible over a field of characteristic* 0, *then one of the* Φ *does not vanish when applied to the coefficients of* F.

Corollary 3.2.3. $b(f) \le O(\max(d^{-2}\log\|f\|, 1))$.

Proof. Write $\mathcal{P}$ for the set of prime numbers $p > 27d^4$ modulo which f is not absolutely irreducible. There exists a Noether form Φ with coefficients in $\mathbb{Z}$ such that Φ applied to the coefficients of f is nonzero, but is divisible by any prime in $\mathcal{P}$. In particular, the product of such p is bounded by $c := \|\Phi\|_1\|f\|^{\deg\Phi}$. Now

$$\begin{aligned}\log b(f) &= \sum_{p\in\mathcal{P}} \frac{\log p}{p}\\ &\le \sum_{27d^4<p\le\log c} \frac{\log p}{p} + \sum_{\log c<p\in\mathcal{P}} \frac{\log p}{\log c}\\ &\le \max(\log\log c - 4\log d, 0) + O(1) + \frac{\log c}{\log c}\\ &\le \max(\log\log c - 4\log d, 0) + O(1)\\ &\le \max(\log(\deg\Phi\log\|f\|) - 4\log d, \log\log\|\Phi\|_1 - 4\log d, 0) + O(1),\end{aligned}$$

where we have used that the function $\log x - \sum_{p\le x}\log p/p$ is bounded (Mertens' first theorem). Since $\log\log\|\Phi\|_1 - 4\log d$ is bounded above, the claim follows. □

We now adapt [Walsh 2015, Theorem 2.3], keeping track of the dependency on the degree and on $b(f)$.

Lemma 3.2.4. *For any* $x > 0$, $\sum_{p\le x}\log p \le 2x$, *where the sum extends over prime numbers not exceeding* x.

Proof. This is a classical estimate on the first Chebyshev function. □

Lemma 3.2.5. *As* x *varies over positive real numbers we have* $\sum_{p>x}\log p/p^{3/2} = O(x^{-1/2})$, *where the sum extends over prime numbers greater than* x.

Proof. Estimate the density of prime numbers using the prime number theorem and compare the sum with an integral. □

Proposition 3.2.6. *Let* $(\xi_1, \dots, \xi_s)$ *be a tuple of rational points in* X, *let* $F_{li} \in \mathbb{Z}[x_0, \dots, x_{n+1}]$, $1 \le l \le L$, $1 \le i \le s$, *be homogeneous polynomials with integer coefficients, and write* Δ_l *for the determinant of*

$(F_{li}(\xi_j))_{ij}$. Let Δ be the greatest common divisor of the Δ_l, and assume that $\Delta \neq 0$. Then we have the bound

$$\log|\Delta| \geq \frac{n!^{1/n}}{n+1} s^{1+1/n}(\log s - O_n(1) - n(4\log d + \log b(f))).$$

This is a more explicit variant of [Walsh 2015, Theorem 2.3].

Proof. Let $\mathcal{P}$ be the collection of prime numbers p such that either $p \leq 27d^4$ or X_p is not geometrically integral.

We now apply Corollary 2.9 to all prime numbers $p \leq s^{1/n}$ not in $\mathcal{P}$, yielding

$$\log|\Delta| \geq \frac{n!^{1/n} n}{n+1} s^{1+1/n} \sum_{\mathcal{P} \not\ni p \leq s^{1/n}} \frac{\log p}{p + O_n(d^2 p^{1/2})} - O_n(s) \sum_{p \leq s^{1/n}} \log p.$$

The last term is bounded by $O_n(1)s^{1+1/n}$.

In estimating the main term, we may use that $1/(p + O_n(d^2p^{1/2})) \geq 1/p - O_n(d^2)/p^{3/2}$. We can then bound

$$\begin{aligned}
\sum_{\mathcal{P} \not\ni p \leq s^{1/n}} \frac{\log p}{p + O_n(d^2 p^{1/2})} &\geq \sum_{p \leq s^{1/n}} \frac{\log p}{p} - \sum_{p \in \mathcal{P}} \frac{\log p}{p} - O_n(d^2) \sum_{\mathcal{P} \not\ni p \leq s^{1/n}} \frac{\log p}{p^{3/2}} \\
&\geq \frac{\log s}{n} - \sum_{p \leq 27d^4} \frac{\log p}{p} - \log b(f) - O(1) - O_n\left(d^2 \sum_{p > 27d^4} \frac{\log p}{p^{3/2}}\right) \\
&\geq \frac{\log s}{n} - \log(27d^4) - \log b(f) - O(1) - O_n(d^2(27d^4)^{-1/2}) \\
&\geq \frac{\log s}{n} - 4\log d - \log b(f) - O_n(1).
\end{aligned}$$

□

3.3. ***The main estimates.*** We first establish that we can reduce to the case of absolutely irreducible f in the proof of Theorem 3.1.1.

Lemma 3.3.1. *If $f \in \mathbb{Z}[x_0, \ldots, x_{n+1}]$ is homogeneous of degree $d \geq 1$ and irreducible but not absolutely irreducible, then there exists another polynomial $g \in \mathbb{Z}[x_0, \ldots, x_{n+1}]$ of degree d, not divisible by f, which vanishes on all rational zeroes of f.*

Proof. This is established in the first paragraph of Section 4 of [Walsh 2015]. □

Let us now work with a restricted class of homogeneous polynomials f, namely those which are absolutely irreducible and for which the leading coefficient c_f, i.e., the coefficient of the monomial x_{n+1}^d, satisfies

$$c_f \geq \|f\| C^{-nd^{1+1/n}}$$

for some positive constant C which is allowed to depend on n (for this reason the factor n in the exponent is in fact superfluous, but it simplifies the proof write-up below).

The two main results are the following:

Lemma 3.3.2. *For f as above, and B satisfying $\|f\| \le B^{2d(n+1)}$, there exists a homogeneous polynomial g not divisible by f, vanishing at all zeroes of f of height at most B, and of degree*

$$M = O_n(1)B^{(n+1)/(nd^{1/n})}\frac{d^{4-1/n}b(f)}{\|f\|^{n^{-1}d^{-1-1/n}}} + d^{1-1/n}\log B + O_n(d^2).$$

Lemma 3.3.3. *For f as above, and B satisfying $\|f\| \ge B^{2d(n+1)}$, there exists a homogeneous polynomial g not divisible by f, vanishing at all zeroes of f of height at most B, and of degree*

$$M = O_n(d^{4-1/n}).$$

These two lemmas together clearly imply the statement of Theorem 3.1.1, at least for polynomials f satisfying the condition on leading coefficients.

We follow the exposition in [Walsh 2015, Section 4], and prove the two lemmas together. We shall need the following.

Theorem 3.3.4 [Bombieri and Vaaler 1983, Theorem 1]. *Let $\sum_{k=1}^{r} a_{mk}x_k = 0$ $(m = 1, \dots, s)$ be a system of s linearly independent equations in $r > s$ variables $x_1, \dots, x_r$, with coefficients $a_{mk} \in \mathbb{Z}$. Then there exists a nontrivial integer solution $(x_1, \dots, x_r)$ satisfying*

$$\max_{1\le i\le r}|x_i| \le (D^{-1}\sqrt{|\det(AA^\top)|})^{1/(r-s)}.$$

Here $A = (a_{mk})$ is the matrix of coefficients and D is the greatest common divisor of the determinants of the $s \times s$ minors of A.

Proof of Lemmas 3.3.2 and 3.3.3. Fix $B \ge 1$, and let S be the set of rational points on the hypersurface described by f of height at most B. Let $M > 0$ be such that there is no homogeneous polynomial g of degree M, not divisible by f, which vanishes on all points in S; we shall show that M is bounded in terms of $n, B, d, \|f\|$ as stated. Let us assume in the following that M is bigger than some constant (to be specified later) times d^2.

Given an integer D, write $\mathcal{B}[D]$ for the set of monomials of degree D in $n+2$ variables, so $|\mathcal{B}[D]| = \binom{D+n+1}{n+1}$. Write $\Xi \subseteq S$ for a maximal subset which is algebraically independent over monomials of degree M, in the sense that applying all monomials in $\mathcal{B}[M]$ to Ξ yields $s = |\Xi|$ linearly independent vectors. Let A be the $s \times r$ matrix whose rows are these vectors, where $r = |\mathcal{B}[M]| = \binom{M+n+1}{n+1}$; each entry of A is bounded in absolute value by B^M. Since all polynomials in $f \cdot \mathcal{B}[M-d]$ vanish on Ξ, and no polynomials of degree M not divisible by f do by assumption on M, we have $s = |\mathcal{B}[M]| - |\mathcal{B}[M-d]|$.

Now A describes a system of linear equations whose solutions correspond to (the coefficients of) homogeneous polynomials of degree M vanishing on all points in Ξ and therefore all points in S; by assumption, these polynomials are multiples of f and therefore have one coefficient of size at least $c_f \ge \|f\|C^{-nd^{1+1/n}}$ by the assumption on f. Hence Theorem 3.3.4 yields

$$\Delta \le \sqrt{|\det(AA^\top)|}(\|f\|C^{-nd^{1+1/n}})^{s-r},$$

where we write Δ for the greatest common divisor of the determinants of the $s \times s$ minors of A. Taking logarithms, using the estimate $|\det(AA^\top)| \le s!(rB^M)^s$ obtained by estimating the size of the coefficients of $AA^\top$, and using the estimate for Δ obtained from Proposition 3.2.6, this expands as follows:

$$\frac{n!^{1/n}}{n+1} s^{1+1/n}(\log s - O_n(1) - n(4\log d + \log b(f))) \le \frac{\log s!}{2} + \frac{s}{2}\log r + sM\log B - (r-s)(\log\|f\| - nd^{1+1/n}O_n(1))$$

We can use the estimates $\log s! \le s\log s$ and $\log r \le \log(M+1)^{n+1} \le O_n(\log M) \le O_n(\log s)$ to see that the first two terms on the right-hand side are both in $O_n(s^{1+1/n})$ and can hence be neglected by adjusting the constant $O_n(1)$ on the left-hand side. Dividing by Ms now yields:

$$\frac{n!^{1/n}}{n+1}\frac{s^{1/n}}{M}(\log s - O_n(1) - n(4\log d + \log b(f))) \le \log B - \frac{r-s}{Ms}(\log\|f\| - nd^{1+1/n}O_n(1)) \quad (3\text{-}3\text{-}1)$$

The term $s = \binom{M+n+1}{n+1} - \binom{M-d+n+1}{n+1}$ is a polynomial in M and d. We can write

$$s = \frac{dM^n}{n!} + O_n(d^2M^{n-1}),$$

in particular $\log s = \log d + n\log M - O_n(1)$. By rearranging and applying the binomial series, which is legal since d^2/M is bounded above by an adjustable absolute constant, we also obtain

$$\frac{s^{1/n}}{M} = \frac{d^{1/n}}{n!^{1/n}} + O_n\left(\frac{d^2}{M}\right).$$

Thus the left-hand side of the inequality above can be replaced by

$$\frac{d^{1/n}n}{n+1}\left(\log M - O_n(1) - \left(\left(4-\frac{1}{n}\right)\log d + \left(1+O_n\left(\frac{d^{2-1/n}}{M}\right)\right)\log b(f)\right)\right),$$

where we have dropped terms $O_n(d^{2-1/n}\log M/M)$ and $O_n(d^{2-1/n}\log d/M)$ by adjusting the constant in $O_n(1)$.

Let us now estimate $(r-s)/(Ms)$. We have $r - s = (M^{n+1})/((n+1)!) + O_n(dM^n)$, so

$$\frac{r-s}{Ms} = \frac{1}{d(n+1)}\frac{1+O_n(d/M)}{1+O_n(d/M)} = \frac{1}{d(n+1)} + O_n\left(\frac{1}{M}\right).$$

Therefore inequality (3-3-1) becomes

$$\frac{d^{1/n}n}{n+1}\left(\log M - O_n(1) - \left(\left(4-\frac{1}{n}\right)\log d + \left(1+O_n\left(\frac{d^{2-1/n}}{M}\right)\right)\log b(f)\right)\right) \le \log B - \frac{\log\|f\|}{d(n+1)} - O_n\left(\frac{\log\|f\|}{M}\right). \quad (3\text{-}3\text{-}2)$$

Let us now assume that $\|f\| \le B^{2d(n+1)}$ and $M \ge d^{1-1/n}\log B$. Then $\log\|f\| \le 2d(n+1)\log B \le O_n(d^{1/n}M)$, so we can drop the last term on the right-hand side, as well as the $O_n(\log b(f)/M)$ on the

left-hand side. Rearranging yields that

$$\log M \le O_n(1) + \frac{n+1}{d^{1/n}n}\log B - \frac{\log\|f\|}{nd^{1+1/n}} + \left(4-\frac{1}{n}\right)\log d + \log b(f),$$

so we obtain Lemma 3.3.2.

Now, on the other hand, assume that $\|f\| \ge B^{2d(n+1)}$ and $M \ge 4d(n+1)$. Rearranging inequality (3-3-2) yields

$$\begin{aligned}\log M &\le O_n(1) + \left(4-\frac{1}{n}\right)\log d + (1+O_n(d^{-1/n}))\log b(f) - \frac{\log\|f\|}{4nd^{1+1/n}}\\ &\le O_n(1) + \max\left\{3\log d, \left(4-\frac{1}{n}\right)\log d\right\},\end{aligned}$$

where we have used

$$\begin{aligned}O_n(1)\log b(f) - \frac{\log\|f\|}{4nd^{1+1/n}} &\le O_n(1)\max(\log\log\|f\| - 2\log d, 0) - \frac{\log\|f\|}{4nd^{1+1/n}}\\ &\le \max(0, -2\log d + \log(O_n(1)4nd^{1+1/n}))\\ &\le O_n(1)\end{aligned}$$

by Corollary 3.2.3 and the lemma below. This establishes Lemma 3.3.3. □

Lemma 3.3.5. *Let $c > 0$. For any $x > 1$ we have* $\log\log x - \log(x)/c \le \log c + O(1)$.

Proof. Let $C = \sup_{x>1}(\log\log x - \log x)$; note that the supremum exists, since it is taken over a continuous function on $]1,\infty[$ which tends to $-\infty$ at both ends of the interval. Now $\log\log x - \log(x)/c = \log c + \log\log x^{1/c} - \log x^{1/c} \le \log c + C$. □

3.4. ***Finishing the proof.*** We use ideas from [Walsh 2015, Section 3] to finish the proof of Theorem 3.1.1.

Lemma 3.4.1. *Let $f \in \mathbb{C}[x]$ be a polynomial of degree $\le d$, and write $\|f\|$ for the maximal absolute value among the coefficients. There exists an integer a, $0 \le a \le d$, such that $|f(a)| \ge 3^{-d}\|f\|$.*

Proof. This is a statement about the $\|\cdot\|_\infty$-operator norm of the inverse of the Vandermonde matrix with nodes $0, \dots, d$, which can be deduced from [Gautschi 1962, Theorem 1]. □

Lemma 3.4.2. *Let $f \in \mathbb{C}[x_0, \dots, x_{n+1}]$ be homogeneous of degree d. There exist integers $a_0, \dots, a_n$ with $0 \le a_i \le d$ such that $|f(a_0, \dots, a_n, 1)| \ge 3^{-(n+1)d}\|f\|$.*

Proof. Dehomogenize by setting $x_{n+1} = 1$, and then use induction with the preceding lemma. □

Proof of Theorem 3.1.1. Take a nonzero $f \in \mathbb{Z}[x_0, \dots, x_{n+1}]$ homogeneous of degree d. Consider $a_0, \dots, a_n$ as in the last lemma and let $A = I + A_0 \in \mathrm{SL}_{n+2}(\mathbb{Z})$, where I is the $(n+2) \times (n+2)$ identity matrix and A_0 has its last column equal to $(a_0, \dots, a_n, 0)$ and zero everywhere else. Note that $A^{-1} = I - A_0$.

Let $f' = f \circ A$. By construction, the x_{n+1}^d-coefficient of f' is $\geq 3^{-(n+1)d}\|f\|$. Because of the boundedness of the entries of A, we furthermore see that

$$\|f'\| \leq d^d(n+2)^d \binom{n+d+1}{n+1} \|f\| \leq \exp(O_n(d^{1+1/n}))\|f\|.$$

In particular, the x_{n+1}^d-coefficient of f' is greater than $C^{-nd^{1+1/n}}\|f'\|$ for some constant C depending only on n. The polynomial f' is primitive if and only if f is, since they are related by the matrices A, A^{-1} with integer coefficients, and $b(f) = b(f')$. Furthermore, if g' is a homogeneous polynomial in $\mathbb{Z}[x_0, \ldots, x_{n+1}]$ vanishing on all zeroes of f' up to a certain height B', then $g = g' \circ A^{-1}$ is a polynomial of the same degree vanishing on all zeroes of f up to height $B = B'/(d+1)$.

Since either Lemma 3.3.2 or Lemma 3.3.3 applies to f' and B', we obtain the desired statement for f. □

4. Proofs of Theorems 1, 2, 3, 4, 6

4.1. ***On trivial bounds.*** In this subsection, we extend our notation to varieties defined over any field K containing $\mathbb{Q}$, and we write $N(X, B)$ for the number of points in $\mathbb{P}^n(\mathbb{Q}) \cap X(K)$ of height at most B, when X is a subvariety of $\mathbb{P}^n_K$, and similarly we write $N_{\mathrm{aff}}(Y, B)$ for the number of points in $\mathbb{Z}^n \cap Y(K) \cap [-B, B]^n$, when $Y \subseteq \mathbb{A}^n_K$.

Lemma 4.1.1. *Let $X \subseteq \mathbb{A}^n_{\overline{\mathbb{Q}}}$ be a (possibly reducible) variety of pure dimension m and degree d defined over $\overline{\mathbb{Q}}$. Then the number $N_{\mathrm{aff}}(X, B)$ of integral points on X of height at most B is bounded by $d(2B+1)^m$.*

When X is a hypersurface, this is the well-known Schwarz–Zippel bound, and even the general case appears in many places in the literature, albeit often without making the bound completely explicit.

Proof. This is an easy inductive argument using intersections with shifts of coordinate hyperplanes. In fact, the proof of [Browning and Heath-Brown 2005, Theorem 1] automatically gives this stronger statement. □

Corollary 4.1.2. *For an irreducible affine variety X in $\mathbb{A}^n$ of degree d and dimension $< n$ there exists a tuple $(a_1, \ldots, a_n)$ of integers not on X, with $|a_i| \leq d$ for every i. For every irreducible projective variety X in $\mathbb{P}^n$ of degree d and dimension $< n$ there exists a point in $\mathbb{P}^n(\mathbb{Q})$ of height at most d not on X.*

Proof. The affine version is implied by the preceding lemma, and the projective version follows by considering the affine cone. □

Lemma 4.1.3. *Let $X \subseteq \mathbb{A}^n_{\overline{\mathbb{Q}}}$ be an absolutely irreducible variety of dimension m and degree d not defined over $\mathbb{Q}$. Then the number $N_{\mathrm{aff}}(X, B)$ of integral points on X of height at most B is bounded by $d^2(2B+1)^{m-1}$.*

By considering the affine cone over a projective variety, this result also applies to projective varieties of dimension m, with bound $d^2(2B+1)^m$.

Proof. For every field automorphism σ of $\overline{\mathbb{Q}}$, there is a conjugate variety X^σ. Since X is not defined over $\mathbb{Q}$, there exists a σ with $X^\sigma \neq X$. All $\mathbb{Q}$-points of X necessarily also lie on X^σ. Since X^σ has degree d, it is the intersection of hypersurfaces of degree $\leq d$, see for instance [Heintz 1983, Proposition 3]. Let Y be a hypersurface of degree $\leq d$ containing X^σ and not containing X. Then $X \cap Y$ is a variety of pure dimension $m-1$ and degree at most d^2. Now Lemma 4.1.1 gives the result. □

The following allows us to reduce to the geometrically irreducible situation when counting points on varieties.

Corollary 4.1.4. *Let $X \subseteq \mathbb{A}^n$ be an irreducible variety over $\mathbb{Q}$ of dimension m and degree d which is not geometrically irreducible. Then for any $B \geq 1$ we have $N_{\mathrm{aff}}(X, B) \leq d^2(2B+1)^{m-1}$.*

As above, this also applies to projective varieties.

Proof. Let $K/\mathbb{Q}$ be a finite Galois extension over which X splits into absolutely irreducible components, and let Y be one of the components. Since all components are Galois-conjugate, the $\mathbb{Q}$-points on X in fact also lie on Y. Now the preceding lemma applied to Y gives the result. □

Remark 4.1.5. Note that this trivially proves Theorems 1 and 3 for irreducible, but not geometrically irreducible varieties, and similarly for absolutely irreducible varieties defined over $\overline{\mathbb{Q}}$ but not over $\mathbb{Q}$. The same applies for Theorem 2 by considering a projective curve as the union of an affine curve with a finite number of points.

Thus we henceforth only need to concern ourselves with absolutely irreducible varieties defined over $\mathbb{Q}$.

4.2. ***Affine counting.*** Our results for projective hypersurfaces from the last section yield the following result for affine hypersurfaces, by refining the technique given in [Ellenberg and Venkatesh 2005, Remark 2.3].

Proposition 4.2.1. *Fix an integer $n > 0$. Then there exist c and e such that the following holds for all f, B, d. Let $f \in \mathbb{Z}[x_1, \ldots, x_{n+1}]$ be irreducible, primitive and of degree d. For each i write f_i for the degree i homogeneous part of f. Fix $B \geq 1$. Then there is a polynomial g in $\mathbb{Z}[x_1, \ldots, x_{n+1}]$ of degree at most*

$$cB^{1/d^{1/n}} d^{2-1/n} \frac{\min(\log\|f_d\| + d\log B + d^2, d^2 b(f))}{\|f_d\|^{1/n \cdot 1/d^{1+1/n}}} + cd^{1-1/n}\log B + cd^{4-1/n},$$

not divisible by f, and vanishing on all points x in $\mathbb{Z}^{n+1}$ satisfying $f(x) = 0$ and $|x_i| \leq B$.

To prove Proposition 4.2.1 we need the following lemmas:

Lemma 4.2.2 [Browning et al. 2006, Lemma 5]. *Let $f \in \mathbb{Z}[x_1, \ldots, x_{n+2}]$ be a primitive absolutely irreducible polynomial, homogeneous of degree d, defining a hypersurface Z in $\mathbb{P}^{n+1}$. Let $B \geq 1$. Then either the height of the coefficients of f is bounded by $O_n(B^{d\binom{d+n+1}{n+1}})$, or there exists a homogeneous polynomial g of degree d vanishing on all points of Z of height at most B.*

Lemma 4.2.3. *For $F \in \mathbb{Z}[x_1, \dots, x_{n+2}]$ an irreducible primitive homogeneous polynomial and $1 \le y \le \|F\|$ we have*

$$d^{4-1/n} \frac{b(F)}{\|F\|^{1/n\cdot 1/d^{1+1/n}}} \le O_n(1) d^{2-1/n} \frac{\log y + d^2}{y^{1/n\cdot 1/d^{1+1/n}}}.$$

Proof. The function

$$x \mapsto \frac{\log x}{x^{1/n\cdot 1/d^{1+1/n}}}$$

on $(1, \infty)$ is monotonically increasing up to its maximum when $x^{1/n\cdot 1/d^{1+1/n}} = e$, and monotonically decreasing thereafter.

Let us write $x = \|F\|$ and use $d^2 b(F) \le O_n(1)(\log x + d^2)$ by Corollary 3.2.3. By the monotonicity considered above, there is nothing to show when $y^{1/n\cdot 1/d^{1+1/n}} \ge e$. Otherwise,

$$2d^{2-1/n} \frac{\log y + d^2}{y^{1/n\cdot 1/d^{1+1/n}}} \ge 2d^{2-1/n} \frac{d^2}{y^{1/n\cdot 1/d^{1+1/n}}} \ge d^{4-1/n} \left(\frac{1}{e} + \frac{1}{y^{1/n\cdot 1/d^{1+1/n}}} \right),$$

and the left-hand side of the inequality in the statement is always bounded by

$$O_n(1) d^{2-1/n} \frac{\log x + d^2}{x^{1/n\cdot 1/d^{1+1/n}}} \le O_n(1) d^{2-1/n} \left(\frac{n d^{1+1/n}}{e} + \frac{d^2}{x^{1/n\cdot 1/d^{1+1/n}}} \right),$$

yielding the claim. □

As mentioned above, the following proof follows [Ellenberg and Venkatesh 2005, Remark 2.3]; but additionally we bring in the idea of forming the homogeneous polynomial F_H for primes H in the range $(B/2; B]$ to control primitivity.

Proof of Proposition 4.2.1. By applying Lemma 3.3.1 to the homogenization of f, we may assume that f is absolutely irreducible. For each natural number H, consider the polynomial $F_H \in \mathbb{Z}[x_1, \dots, x_{n+2}]$ given by $F_H(x_1, \dots, x_{n+2}) = \sum_{i=0}^{d} H^i f_i x_{n+2}^{d-i}$. Then F_H is an irreducible homogeneous polynomial of degree d. On the other hand, each integral point $(x_1, \dots, x_{n+1}) \in Z(f)(\mathbb{Z})$ gives us a rational point $(x_1, \dots, x_{n+1}, H)$ in $Z(F_H)(\mathbb{Q})$, where $Z(f)$ stands for the hypersurface in $\mathbb{A}^{n+1}$ given by f and $Z(F_H)$ stands for the hypersurface in $\mathbb{P}^{n+1}$ given by F_H.

If B is bounded by some polynomial expression in d (to be determined later), then $B^{1/(nd^{1/n})}$ is bounded by a constant depending only on n; hence we use Theorem 3.1.1 for F_1, by which there exists a number c depending only on n along with a homogeneous polynomial G_1 in $\mathbb{Z}[x_1, \dots, x_{n+2}]$ of degree at most

$$c B^{1/d^{1/n}} d^{4-1/n} \frac{b(F_1)}{\|F_1\|^{1/n\cdot 1/d^{1+1/n}}} + c d^{1-1/n} \log B + c d^{4-1/n},$$

not divisible by F_1, and vanishing at all points on $Z(F_1)(\mathbb{Q})$ of height at most B. Since $b(F_1) = b(f)$ and $\|F_1\| \ge \|f_d\|$, by Lemma 4.2.3 we obtain

$$d^{4-1/n} \frac{b(F_1)}{\|F_1\|^{1/n\cdot 1/d^{1+1/n}}} \le O_n(d^{2-1/n}) \frac{\min(d^2 b(f), \log\|f\| + d^2)}{\|f_d\|^{1/n\cdot 1/d^{1+1/n}}}.$$

Hence the polynomial $g(x_1, \dots, x_{n+1}) = G_1(x_1, \dots, x_{n+1}, 1)$ satisfies our proposition.

For any $B \geq 2$ Bertrand's postulate guarantees the existence of a prime B' in the interval $(B/2, B]$. Moreover, if $B' \nmid f_0$, then $F_{B'}$ is primitive. By Theorem 3.1.1 for $F_{B'}$, there exists a number c depending only on n along with a homogeneous polynomial $G_{B'}$ in $\mathbb{Z}[x_1, \dots, x_{n+2}]$ of degree at most

$$cB^{(n+1)/nd^{1/n}} d^{4-1/n} \frac{b(F_{B'})}{\|F_{B'}\|^{1/n\cdot 1/d^{1+1/n}}} + cd^{1-1/n} \log B + cd^{4-1/n},$$

not divisible by $F_{B'}$, and vanishing at all points on $Z(F_{B'})(\mathbb{Q})$ of height at most B.

It is clear that $\|F_{B'}\| \geq B'^d \|f_d\| \geq 2^{-d} B^d \|f_d\|$, so by Lemma 4.2.3 we have

$$d^{4-1/n} \frac{b(F_{B'})}{\|F_{B'}\|^{1/n\cdot 1/d^{1+1/n}}} \leq O_n(1) \left(\frac{B}{2}\right)^{-1/(nd^{1/n})} d^{2-1/n} \frac{\log \|f_d\| + d \log B + d^2}{\|f_d\|^{1/n\cdot 1/d^{1+1/n}}}.$$

Furthermore $b(F_{B'})$ agrees with $b(F_1)$ up to a factor of $\exp(\log B'/B') \leq O(1)$. Hence we in fact have

$$d^{4-1/n} \frac{b(F_{B'})}{\|F_{B'}\|^{1/n\cdot 1/d^{1+1/n}}} \leq O_n(1) B^{-1/(nd^{1/n})} d^{2-1/n} \frac{\min(\log \|f_d\| + d \log B + d^2, b(f))}{\|f_d\|^{1/n\cdot 1/d^{1+1/n}}}.$$

Thus the polynomial $g(x_1, \dots, x_{n+1}) = G_{B'}(x_1, \dots, x_{n+1}, B')$ is as desired.

From now on, we suppose that $B > 2$ and $B' \mid f_0$ for all primes B' in the interval $(B/2, B]$. Then we have

$$\left(\prod_{\substack{B' \text{ prime} \\ B/2 < B' \leq B}} B' \right) \mid f_0$$

If $f_0 \neq 0$ then we deduce that

$$\sum_{B' \text{prime}, B/2 < B' \leq B} \log B' \leq \log |f_0|.$$

By Lemma 4.2.2, we are done if f_0 is large compared to $B^{d\binom{d+n+1}{n+1}}$, so in the remaining case we have

$$\sum_{B' \text{prime}, B/2 < B' \leq B} \log B' \leq d \binom{d+n+1}{n+1} \log B - O_n(1)$$

Because of the well-known estimate

$$\lim_{x \mapsto +\infty} \frac{\sum_{p \leq x} \log p}{x} = 1,$$

we see that B is necessarily bounded by a certain polynomial in d in this case, so we are done by the discussion above.

If $f(0) = 0$, then by Corollary 4.1.2 there exists an integer point $A = (a_1, \dots, a_{n+1})$ with $f(a_1, \dots, a_{n+1}) \neq 0$ and $|a_i| \leq d$ for all $1 \leq i \leq n+1$. We consider the shifted polynomial $\tilde{f}(x) = f(x+A)$, for which $\tilde{f}(0) \neq 0$, $\|f_d\| = \|\tilde{f}_d\|$, and $b(\tilde{f}) = b(f)$. We apply the above discussion for $\tilde{f}$ and $\tilde{B} = B + d$ to obtain a polynomial $\tilde{g}(x)$ vanishing on all zeroes of $\tilde{f}$ of height at most $\tilde{B}$, and take $g(x) = \tilde{g}(x - A)$. This satisfies the required degree bound since $\tilde{g}$ does. □

Corollary 4.2.4. *There exists a constant c such that for all $d > 0$ and all irreducible affine curves $X \subseteq \mathbb{A}^2_{\mathbb{Q}}$ of degree d, cut out by an irreducible primitive polynomial $f \in \mathbb{Z}[x_1, x_2]$, and all $B \geq 1$ one has*

$$N_{\mathrm{aff}}(X, B) \leq cB^{1/d} \frac{\min(d^2 \log \|f_d\| + d^3 \log B + d^4, d^4 b(f))}{\|f_d\|^{1/d^2}} + cd \log B + cd^4.$$

Proof. Take $n = 1$ in Proposition 4.2.1 and apply Bézout's theorem. □

If the absolute irreducibility of f can be explained by the indecomposability of its Newton polytope, e.g., in the sense of [Gao 2001], then this allows for good bounds on $b(f)$ which get rid of the factor $\log B$. The following instance will be used to prove Theorem 6:

Corollary 4.2.5. *There exists a constant c such that for all affine curves $X \subseteq \mathbb{A}^2_{\mathbb{Q}}$ cut out by a polynomial $f \in \mathbb{Z}[x_1, x_2]$ of the form*

$$c_d x_1^d + c_{d'} x_2^{d'} + \sum_{\substack{i,i' \\ id' + i'd < dd'}} c_{ij} x_1^i x_2^{i'}$$

with $d > d' > 0$ coprime integers and $c_d, c_{d'} \neq 0$, and for all $B \geq 1$, one has

$$N_{\mathrm{aff}}(X, B) \leq cd^4 (\log |c_d c_{d'}| + 1) B^{1/d}.$$

Proof. By dividing out by the greatest common divisor of the coefficients, we may suppose that f is primitive. The presence of the edge $(d, 0)$–$(0, d')$ in the Newton polytope of f is enough to guarantee absolute irreducibility in any characteristic [Gao 2001, Theorem 4.11]. Therefore we can bound

$$b(f) \leq \prod_{p | c_d c_{d'}} \exp\left(\frac{\log p}{p}\right) \leq \log |c_d c_{d'}| + 1$$

through Mertens' first theorem as in Corollary 3.2.3. □

4.3. ***Proofs of our main results.*** We can now prove our main theorems, subject to the following propositions; they allow us to reduce to the case of hypersurfaces throughout, and will be established in Section 5 by projection arguments.

Proposition 4.3.1. *Given a geometrically integral affine variety X in $\mathbb{A}^n$ of dimension m and degree d, there exists a geometrically integral affine variety X' in $\mathbb{A}^{m+1}$ birational to X, also of degree d, such that for any $B \geq 1$ we have*

$$N_{\mathrm{aff}}(X, B) \leq d N_{\mathrm{aff}}(X', c_n d^{e_n} B),$$

where c_n, e_n are constants depending only on n.

For $m = 1$, we can even achieve

$$N_{\mathrm{aff}}(X, B) \leq N_{\mathrm{aff}}(X', c_n d^{e_n} B) + d^2.$$

Proposition 4.3.2. *Given a geometrically integral projective variety X in $\mathbb{P}^n$ of dimension m and degree d, there exists a geometrically integral projective variety X' in $\mathbb{P}^{m+1}$ birational to X, also of degree d, such that for any $B \geq 1$ we have*

$$N(X, B) \leq dN(X', c_n d^{e_n} B),$$

where c_n, e_n are constants depending only on n.

For $m = 1$, we can even achieve

$$N(X, B) \leq N(X', c_n d^{e_n} B) + d^2.$$

Proof of Theorem 2. In the case of a planar curve, i.e., for $n = 2$, Corollary 3.1.2 gives the claim. For the general case, we may assume that the given curve is geometrically integral by Remark 4.1.5, and then reduce to $n = 2$ by applying Proposition 4.3.2 (where $m = 1$). □

Proof of Theorem 3. We may assume that the curve X is geometrically integral by Remark 4.1.5. In the case of a planar curve, i.e., for $n = 2$, Corollary 4.2.4 yields that

$$N(X, B) \leq O_n((d^3 \log B + d^4)B^{1/d}),$$

by observing that

$$\frac{d^2 \log \|f_d\| + d^3 \log B + d^4}{\|f_d\|^{1/d^2}} \leq d^3 \log B + 2d^4.$$

We can reduce the general case to $n = 2$ by applying Proposition 4.3.1 (where $m = 1$), yielding the same estimate. □

Proof of Theorem 6. In the penultimate step of their proof of Theorem 1.1, Bhargava et al. [2020] establish the bound

$$h_2(K) \leq O_{d,\varepsilon}(|\Delta_K|^{1/4+\varepsilon}) + \sum_{\beta \in \mathcal{B}} N_{\mathrm{aff}}(f_\beta, |\Delta_K|^{1/2})$$

where $\mathcal{B} \subseteq \mathcal{O}_K$ is a set of size $O_d(|\Delta_K|^{1/2-1/d})$ and

$$f_\beta = y^2 - N_{K/\mathbb{Q}}(x - \beta) = y^2 - x^d - \text{lower order terms in } x.$$

Theorem 3 implies that

$$N_{\mathrm{aff}}(f_\beta, |\Delta_K|^{1/2}) \leq O_d(|\Delta_K|^{1/(2d)} \log|\Delta_K|),$$

yielding the desired result when d is even. If d is odd then instead of Theorem 3 we apply Corollary 4.2.5 with $d' = 2$, $c_d = -1$, $c_{d'} = 1$ to get rid of the factor $\log|\Delta_K|$. □

For the proof of Theorem 4, we need the following explicit form of Proposition 1 of [Browning et al. 2006] with $D = 1$.

Proposition 4.3.3. *There exists a constant c such that for all $d \geq 3$ and all polynomials $f \in \mathbb{Z}[x_1, x_2, x_3]$ of degree d such that the highest degree part $h(f) = f_d$ of f is irreducible, all finite sets I of curves C of $\mathbb{A}^3_{\mathbb{Q}}$ of degree 1 and lying on the hypersurface defined by f, and all $B \geq 1$ one has*

$$N_{\mathrm{aff}}\left(X \cap \left(\bigcup_{C \in I} C\right), B\right) \leq cd^6 B + \#I.$$

Proof. We write $I = I_1 \cup I_2$ where $I_1 = \{L \in I \mid N_{\mathrm{aff}}(L, B) \leq 1\}$ and $I_2 = \{L \in I \mid N_{\mathrm{aff}}(L, B) > 1\}$. It is clear that $N_{\mathrm{aff}}\big(X \cap \bigcup_{L \in I_1} L\big) \leq \#I_1$. If $L \in I_2$, then there exist $a = (a_1, a_2, a_3)$, $v = (v_1, v_2, v_3) \in \mathbb{Z}^3$ such that $H(a) \leq B$, v is primitive and $L(\mathbb{Q}) = \{a + \lambda v \mid \lambda \in \mathbb{Q}\}$. Since v is primitive we deduce that

$$L(\mathbb{Z}) \cap [-B, B]^3 = \{a + \lambda v \mid \lambda \in \mathbb{Z}, H(a + \lambda v) \leq B\}.$$

So

$$\#(L(\mathbb{Z}) \cap [-B, B]^3) \leq 1 + \frac{2B}{H(v)}.$$

Since $L \in I_2$ we have $H(v) \leq 2B$ and $f_d(v) = 0$. On the other hand, for each point v with $f_d(v) = 0$, there are at most $d(d-1)$ lines $L \in I_2$ in the direction of v, since each such line intersects a generic hyperplane in $\mathbb{A}^3$ in a point which is simultaneously a zero of f and of the directional derivative of f in the direction of v. Put $A_i = \{v \in \mathbb{P}^2(\mathbb{Q}) \mid f_d(v) = 0, H(v) = i\}$ and $n_i = \#A_i$. Then, by Corollary 3.1.2, there exists a constant c independent of f such that $\sum_{1 \leq i \leq k} n_i \leq cd^4 k^{2/d}$. By our discussion,

$$N_{\mathrm{aff}}\left(X \cap \left(\bigcup_{C \in I} C\right), B\right) \leq \#I_1 + (d-1)d \sum_{i=1}^{2B} n_i \left(1 + \frac{2B}{i}\right).$$

On the other hand, summation by parts gives the following:

$$\begin{aligned}\sum_{i=1}^{2B} n_i \left(1 + \frac{2B}{i}\right) &= \sum_{k=1}^{2B-1} \left(\sum_{i=1}^{k} n_i\right)\left(\frac{2B}{k} - \frac{2B}{k+1}\right) + \left(\sum_{i=1}^{2B} n_i\right)\left(1 + \frac{2B}{2B}\right) \\ &\leq cd^4 \left(\sum_{k=1}^{2B-1} k^{2/d} \frac{2B}{k(k+1)} + 2(2B)^{2/d}\right).\end{aligned}$$

Since $d \geq 3$, one has $\sum_{k \geq 1} k^{2/d} \cdot 1/(k(k+1)) < +\infty$ and $B^{2/d} \leq B$. Thus, by enlarging c, we have

$$N_{\mathrm{aff}}\left(X \cap \left(\bigcup_{C \in I} C\right), B\right) \leq cd^6 B + \#I$$

as desired. □

In order to prove Theorem 4, we now first consider the case of a surface in $\mathbb{P}^3$, with proof inspired by the proof of Corollary 7.3 of [Salberger 2013] in combination with the improvements developed above.

Proposition 4.3.4. *There exists a constant c such that for all polynomials f in $\mathbb{Z}[y_1, y_2, y_3]$ whose homogeneous part of highest degree f_d is irreducible over $\overline{\mathbb{Q}}$ and whose degree d is least 5, one has $N_{\mathrm{aff}}(f, B) \leq cd^{14} B$.*

Proof of Proposition 4.3.4 for $d \geq 16$. For any prime modulo which f_d is absolutely irreducible, the reduction of f is likewise absolutely irreducible, so $b(f) \leq b(f_d)$. Applying the usual estimate from Corollary 3.2.3, Proposition 4.2.1 yields for each $B \geq 1$ a polynomial g of degree at most

$$cd^{7/2}B^{1/\sqrt{d}}, \tag{4-3-1}$$

not divisible by f and vanishing on all points x in $\mathbb{Z}^n$ satisfying $f(x) = 0$ and $|x_i| \leq B$, with c an absolute constant. Let C be an irreducible component of the (reduced) intersection of $f = 0$ with $g = 0$. Call this intersection $\mathcal{C}$. If C is of degree $\delta > 1$, then

$$N_{\mathrm{aff}}(C, B) \leq c'\delta^3 B^{1/\delta}(\log B + \delta) \tag{4-3-2}$$

by Theorem 3, for some absolute constant c'.

By Proposition 4.3.3, the total contribution of integral curves D of $\mathcal{C}$ of degree 1 is at most

$$c''d^6 B \tag{4-3-3}$$

for some absolute constant c''.

Suppose that $C_1, \ldots, C_k$ are irreducible components of the intersection of $f = 0$ and $g = 0$ and $\deg(C_i) > 1$ for all i. Furthermore, we assume that $\deg(C_i) \leq \log B$ for all $1 \leq i \leq m$ and $\deg(C_i) > \log B$ for all $i > m$. Since the function $\delta \mapsto 4\log_B(\delta) + 1/\delta$ is decreasing in $(0, \log B/4)$ and increasing in $(\log B/4, +\infty)$, by enlarging c', for all $1 \leq i \leq m$ we have

$$N_{\mathrm{aff}}(C_i, B) \leq c' B^{1/2}(\log B + 1). \tag{4-3-4}$$

On the other hand, if $\delta > \log B$ then $B^{1/\delta}$ is bounded, so (4-3-1) and (4-3-2) imply

$$\sum_{m+1 \leq i \leq k} N_{\mathrm{aff}}(C_i, B) \leq c'''d^{14}B^{4/\sqrt{d}} \tag{4-3-5}$$

for some c''' independent of d and B.

Putting the estimates (4-3-1), (4-3-3), (4-3-4), (4-3-5) together proves the proposition when d is at least 16. □

To give a proof of Proposition 4.3.4 for lower values of d than 16, one could try to get a form of Theorem 3 with a lower exponent of the degree and repeat the above proof. We proceed differently: we treat the values for d going from 6 up to 15 by inspecting the proof of [Browning et al. 2006, Theorem 2] in combination with some of the above refinements, and the case of $d = 5$ by using [Salberger 2013, Theorem 7.2] (at the cost of being less self-contained).

Proof of Proposition 4.3.4 with $6 \leq d \leq 15$. Fix $6 \leq d \leq 15$, let $f \in \mathbb{Z}[y_1, y_2, y_3]$ be of degree d with absolutely irreducible homogeneous part of highest degree, and let X be the surface described by f.

In [Browning et al. 2006, Theorem 2], the estimate $N_{\mathrm{aff}}(f, B) \leq O_{d,\varepsilon}(B^{1+\varepsilon})$ is established for every $\varepsilon > 0$. However, using our Theorem 2 and Proposition 4.3.3, we shall show that their proof [Browning

et al. 2006, pages 568–570] in fact gives the bound $N_{\mathrm{aff}}(f, B) \leq O_d(B)$, without any ε, which is sufficient for our purposes.

Specifically, they first consider the case in which Lemma 4.2.2 applies, so all the rational points on X of height up to B lie on a union of irreducible curves with sum of degrees at most d^2. Applying Theorem 2 to those curves of degree ≥ 2 and Proposition 4.3.3 for the contribution of curves of degree 1 yields the claim in this case.

In the remaining case, it is argued that there is an open subset $U \subseteq X$ (specifically consisting of those nonsingular points on X which have multiplicity at most 2 on the tangent plane section at the point) whose complement consists of $O_d(1)$ integral components of degree $O_d(1)$; by the same argument as in the preceding paragraph, the contribution of this complement is $O_d(B)$, so it suffices to estimate $N_{\mathrm{aff}}(U, B)$.

Further, it is argued that the points on U of height at most B are covered by a certain collection of irreducible curves. The subcollection I consisting of those curves of degree at most 2 satisfies $|I| \leq O_{d,\varepsilon}(B^{2/\sqrt{d}+2\varepsilon})$, so our Proposition 4.3.3 and [Browning et al. 2006, Proposition 1] gives a contribution $O_{d,\varepsilon}(B + B^{2/\sqrt{d}+3\varepsilon}) \leq O_d(B)$.

The remaining curves, of which there are no more than $O_{d,\varepsilon}(B^{2/\sqrt{d}})$, all contribute at most $B^{1/3-1/(2\sqrt{d})}$ [Browning et al. 2006, Proposition 2], so their total contribution is

$$O_{d,\varepsilon}(B^{3/(2\sqrt{d})+1/3+\varepsilon}) \leq O_d(B). \qquad \square$$

Theorem 4.3.5 [Salberger 2013, Theorem 7.2]. *Let X be a geometrically integral surface in $\mathbb{P}^3_{\mathbb{Q}}$ of degree d and X_{ns} its nonsingular locus. Suppose that the hyperplane defined by $x_0 = 0$ intersects X properly, and identify $\mathbb{A}^3$ with the open subset of $\mathbb{P}^3$ given by $x_0 \neq 0$. There exists a positive constant c bounded solely in terms of d such that the following holds: for every $B \geq 1$ there exists a set of $O_d(B^{1/\sqrt{d}} \log B + 1)$ geometrically integral curves D_λ on X of degree $O_d(1)$ such that*

$$N_{\mathrm{aff}}\left(X_{\mathrm{ns}} \setminus \bigcup_{\lambda} D_\lambda, B\right) \leq O_d(B^{2/\sqrt{d}+c/\log(1+\log B)}).$$

Proof of Proposition 4.3.4 for $d = 5$. Suppose that the degree d of f is exactly 5, and let X be the surface in $\mathbb{A}^3_{\mathbb{Q}}$ given by f. We may assume that $B \geq 2$. By Theorem 4.3.5, there is $c > 0$ such that for each $B \geq 2$ there is a set $\mathcal{C}$ of at most

$$cB^{1/\sqrt{d}} \log B$$

geometrically integral curves $C \subseteq \mathbb{A}^3_{\mathbb{Q}}$ of degree at most c and lying on X such that

$$N_{\mathrm{aff}}\left(X_{\mathrm{ns}} \setminus \bigcup_{C \in \mathcal{C}} C, B\right) \leq O(B^{2/\sqrt{d}+c/\log(\log B)}) \leq O(B),$$

where X_{ns} is the open subvariety of nonsingular points.

The complement of X_{ns} in X is a union of irreducible curves the sum of whose degrees is bounded by a constant. Applying Theorem 2 to those curves of degree ≥ 2 and Proposition 4.3.3 for the contribution

of curves of degree 1 yields that the complement of X_{ns} contributes at most $O(B)$ points, which is satisfactory for our purposes.

Similarly, the curves in $\mathcal{C}$ of degree 1 contribute at most $O(cB^{1/\sqrt{d}}\log B + B) \le O(B)$ points by Proposition 4.3.3, and the curves in $\mathcal{C}$ of degree ≥ 2 each contribute at most $O(B^{1/2+\varepsilon})$ by Theorem 3, again giving a contribution of size $O(B)$. This proves the claim. □

Remark 4.3.6. We see that Proposition 4.3.4 for fixed $d \ge 6$, and therefore also Theorems 1 and 4 for fixed degree, already follow from combining [Browning et al. 2006] with the results of [Walsh 2015] and Proposition 4.3.3. Similarly, for fixed degree $d \ge 5$ one can use the results of [Salberger 2013]. However, keeping track of the dependence on d in Section 3 permits us to use a considerably simpler argument for fixed $d \ge 16$ than in the works cited, and to furthermore obtain polynomial dependence on d.

It remains to prove Theorems 1 and 4. This closely follows [Browning et al. 2006, Lemma 8, Theorem 3]. The proofs are based on Proposition 4.3.4 and the following lemma.

Lemma 4.3.7. *Let $n \ge 3$ and $X \subseteq \mathbb{P}^n_{\mathbb{Q}}$ be a geometrically integral hypersurface of degree d. Then there exists a nonzero form $F \in \mathbb{Z}[y_0, \dots, y_n]$ of degree at most $(n+1)(d^2-1)$ such that $F(A) = 0$ whenever the hyperplane section $H_A \cap X$ is not geometrically integral, where $A \in (\mathbb{P}^n)^*$ and $H_A \subseteq \mathbb{P}^n$ denotes the hyperplane cut out by the linear form associated with A.*

Proof. Suppose that X is given by f, a geometrically irreducible form of degree d. For $A \in (\mathbb{P}^n)^*$ write $A = (a_0 : a_1 : \cdots : a_n) \in (\mathbb{P}^n)^*$. Assuming $a_0 \ne 0$, one has that $H_A \cap X$ is not geometrically integral if and only if

$$f\left(-\frac{a_1}{a_0}x_1 - \cdots - \frac{a_n}{a_0}x_n, x_1, \dots, x_n\right)$$

is reducible. Since $n \ge 3$ and since X is geometrically integral, we have for a generic choice of $B \in (\mathbb{P}^n)^*$ that $H_B \cap X$ is also geometrically integral. Hence Theorem 3.2.2 implies that there exists a nonzero form F_0 in $\mathbb{Z}[y_1, \dots, y_n]$ of degree at most $d^2 - 1$ such that $F_0(a_1, \dots, a_n) = 0$. Similarly, if $a_i \ne 0$, we produce a nonzero form F_i in $\mathbb{Z}[y_0, \dots, y_{i-1}, y_{i+1}, \dots, y_n]$ such that $F_i(a_0, \dots, a_{i-1}, a_{i+1}, \dots, a_n) = 0$. So $F = \prod_{i=0}^n F_i$ is as we want. □

Proof of Theorem 4. Let $n \ge 3$ and $X \subseteq \mathbb{A}^n_{\mathbb{Q}}$ be a geometrically integral hypersurface of degree $d \ge 5$ described by a polynomial $f \in \mathbb{Z}[x_1, \dots, x_n]$ with absolutely irreducible highest degree part. We proceed by induction on n, where the base case $n = 3$ is Proposition 4.3.4.

Now assume that $n > 3$ and the theorem holds for all lower n. Let $f_d = h(f)$ be the homogeneous part of highest degree, which describes a hypersurface in $\mathbb{P}^{n-1}$. By Lemma 4.3.7 and Corollary 4.1.2, there exists $A = (a_1, \dots, a_n)$ such that the hyperplane section $\{f_d = 0\} \cap \{\sum a_i x_i = 0\}$ is geometrically integral of degree d, with all a_i having absolute value at most $n(d^2-1)$.

Now

$$N_{\mathrm{aff}}(f, B) \le \sum_{|k| \le n^2(d^2-1)B} N_{\mathrm{aff}}\left(\{f = 0\} \cap \left\{\sum a_i x_i = k\right\}, B\right).$$

For each k, the variety $\{f = 0\} \cap \left\{\sum a_i x_i = k\right\}$ is a hypersurface in the affine plane $\left\{\sum a_i x_i = k\right\}$, which after a change of variables is described by a polynomial $g \in \mathbb{Z}[x_1, \ldots, x_{n-1}]$ whose homogeneous part of highest degree is absolutely irreducible by the construction of A. Now the induction hypothesis finishes the proof. □

Proof of Theorem 1. We may assume that the variety in question is geometrically irreducible by Remark 4.1.5, and can reduce to consideration of a hypersurface by Proposition 4.3.2. Hence let $n \geq 3$ and consider an absolutely irreducible polynomial $f \in \mathbb{Z}[x_0, \ldots, x_n]$ homogeneous of degree $d \geq 5$.

Then f defines not only a projective hypersurface X in $\mathbb{P}^n$, but also an affine hypersurface in $\mathbb{A}^{n+1}$, the cone of X. We now trivially have

$$N(f, B) \leq N_{\mathrm{aff}}(f, B),$$

so Theorem 4 finishes the proof. □

Remark 4.3.8. Using the explicit exponents obtained in Proposition 4.3.4 and in the proof of Proposition 4.3.2 in Section 5, we can conservatively estimate $e(n) \leq 2n + 8$ for the exponent in Theorem 4, and $e(n) \leq 2n^3$ for the exponent in Theorem 1.

5. Reduction to hypersurfaces via projection

In this section we prove Propositions 4.3.1 and 4.3.2, which allowed us to reduce to the case of hypersurfaces in the proofs of our main theorems. This is an elaboration of familiar projection arguments, which classically show that every variety is birational to a hypersurface, and which are used in the proofs of [Browning et al. 2006, Theorem 1] and [Pila 1995, Theorem A]. The additional difficulty for us is that we have to keep track of the dependence on the degree of the variety throughout. Our main auxiliary result is:

Lemma 5.1. *Given a geometrically irreducible subvariety $X \subseteq \mathbb{P}^n$ of dimension $m < n - 1$ and degree d, one can find an $(n - m - 2)$-plane Λ disjoint from X and an $(m+1)$-plane Γ, both defined over $\mathbb{Q}$, such that $\Lambda \cap \Gamma = \varnothing$, such that the corresponding projection map $p_{\Lambda,\Gamma} : \mathbb{P}^n \setminus \Lambda \to \Gamma$ satisfies*

$$H(p_{\Lambda,\Gamma}(P)) \leq c_n d^{2(n-m-1)^2} H(P) \tag{5-1}$$

for all $P \in \mathbb{P}^n(\mathbb{Q}) \setminus \Lambda$, and such that $p_{\Lambda,\Gamma}|_X$ is birational onto its image. Here c_n is an explicit constant depending only on n.

Because Λ is disjoint from X, the statement that $p_{\Lambda,\Gamma}|_X$ is birational onto its image is equivalent to saying that $p_{\Lambda,\Gamma}(X)$ is again a variety of degree d; see [Harris 1992, Example 18.16].

In order to prove Lemma 5.1, we first concentrate on finding an appropriate Λ, which we think of as living in the Grassmannian $\mathbb{G}(n - m - 2, n)$ consisting of all $(n - m - 2)$-planes in $\mathbb{P}^n$. It is well-known that the latter has the structure of an $(m+2)(n-m-1)$-dimensional irreducible projective variety through the Plücker embedding

$$P_{n-m-2,n} : \mathbb{G}(n - m - 2, n) \hookrightarrow \mathbb{P}^\nu : \Lambda \mapsto \det(P_1, \ldots, P_{n-m-1}),$$

where $\nu = \binom{n+1}{n-m-1} - 1$ and $(P_1, \ldots, P_{n-m-1})$ is the $(n-m-1) \times (n+1)$ matrix whose rows are coordinates for $n-m-1$ independent points $P_i \in \Lambda$. Here and throughout this section, for a matrix M whose number of rows does not exceed its number of columns, we write $\det(M)$ to denote the tuple consisting of its maximal minors, with respect to some fixed ordering.

Fixing such a $\Lambda \in \mathbb{G}(n-m-2)$ and independent points $P_1, \ldots, P_{n-m-1} \in \Lambda$, we can also consider the map

$$\pi_\Lambda : \mathbb{P}^n \setminus \Lambda \to \mathbb{P}^\mu : P \mapsto \det(P, P_1, \ldots, P_{n-m-1}),$$

where $\mu = \binom{n+1}{n-m} - 1$. Writing $\pi_\Lambda = (\pi_{\Lambda,0}, \ldots, \pi_{\Lambda,\mu})$ we see that the nonzero $\pi_{\Lambda,j}$ can be viewed as linear forms whose coefficients are coordinates of $P_{n-m-2,n}(\Lambda)$, modulo sign flips. Note that $\pi_{\Lambda,j}(P) = 0$ for all j if and only if $P \in \Lambda$. In particular π_Λ is well-defined and easily seen to factor as

$$\mathbb{P}^n \setminus \Lambda \xrightarrow{p_{\Lambda,\Gamma}} \Gamma \hookrightarrow \mathbb{P}^\mu \tag{5-2}$$

for all $(m+1)$-planes Γ such that $\Gamma \cap \Lambda = \varnothing$.

Another theoretical ingredient we need is the Chow point F_X associated with an irreducible m-dimensional degree d variety $X \subseteq \mathbb{P}^n$. This is an irreducible multihomogeneous polynomial of multidegree $(d, d, \ldots, d)$ in $m+1$ sets of $n+1$ variables such that for all tuples $(H_1, H_2, \ldots, H_{m+1})$ of $m+1$ hyperplanes in $\mathbb{P}^n$ one has $F_X(H_1, \ldots, H_{m+1}) = 0$ if and only if $H_1 \cap H_2 \cap \cdots \cap H_{m+1} \cap X \neq \varnothing$. See e.g., [Gelfand et al. 1994, Chapter 4].

Lemma 5.2. *Let X be a geometrically irreducible degree d subvariety of $\mathbb{P}^n$ having dimension $m < n-1$ and consider*

$$G_X = \{\Lambda \in \mathbb{G}(n-m-2, n) \mid \Lambda \cap X = \varnothing \text{ and } \pi_\Lambda|_X \text{ is birational onto its image}\}$$

with π_Λ as above. This is a dense open subset of $\mathbb{G}(n-m-2, n)$ whose complement, when viewed under the Plücker embedding, is cut out by hypersurfaces of degree less than $(m+1)^2 d^2$.

Proof. Given a hyperplane $H \subseteq \mathbb{P}^\mu$ we abusively write $H \circ \pi_\Lambda$ for $\pi_\Lambda^{-1}(H) \cup \Lambda$, since this is the hyperplane in $\mathbb{P}^n$ cut out by the precomposition of π_Λ with the linear form associated with H. Define a multihomogeneous degree $(d, d, \ldots, d)$ polynomial $R_{X,\Lambda}$ in $m+1$ sets of $\mu+1$ variables by letting

$$R_{X,\Lambda}(H_1, H_2, \ldots, H_{m+1}) = F_X(H_1 \circ \pi_\Lambda, H_2 \circ \pi_\Lambda, \ldots, H_{m+1} \circ \pi_\Lambda).$$

Note that its coefficients are degree $(m+1)d$ polynomial expressions in the coordinates of $P_{n-m-2,n}(\Lambda)$. We will show that

$$G_X = \{\Lambda \in \mathbb{G}(n-m-2, n) \mid R_{X,\Lambda} \text{ is absolutely irreducible}\}, \tag{5-3}$$

which implies that the complement of G_X is precisely the vanishing locus of the Noether irreducibility polynomials from Theorem 3.2.2 evaluated in these coefficients. This indeed yields expressions in the coordinates of $P_{n-m-2,n}(\Lambda)$ of degree less than $(m+1)^2 d^2$, where we note that not all these expressions

can vanish identically, since generic Λ's do not meet X and generic projections are known to be birational [Harris 1992, page 224].

We now prove (5-3). First note that $\Lambda \cap X \neq \varnothing$ implies that $R_{X,\Lambda}$ vanishes identically. Indeed, if $P \in \Lambda$ then all hyperplanes of the form $H \circ \pi_\Lambda$ pass through P, so if moreover $P \in X$ we see that $R_{X,\Lambda}$ is identically zero. We can therefore assume that $\Lambda \cap X = \varnothing$. This ensures that $\pi_\Lambda(X)$ is an irreducible projective variety of dimension m; see [Harris 1992, page 134], so we can consider its Chow point $F_{\pi_\Lambda(X)}$, which is an irreducible multihomogeneous polynomial of multidegree

$$(\deg(\pi_\Lambda(X)), \deg(\pi_\Lambda(X)), \ldots, \deg(\pi_\Lambda(X)))$$

in the same $m+1$ sets of $\mu+1$ variables as in the case of $R_{X,\Lambda}$. It has the property that for all tuples $(H_1, \ldots, H_{m+1})$ of hyperplanes in $\mathbb{P}^\mu$ we have $F_{\pi_\Lambda(X)}(H_1, \ldots, H_{m+1}) = 0$ if and only if $H_1 \cap \cdots \cap H_{m+1} \cap \pi_\Lambda(X) \neq \varnothing$. But in this case $\pi_\Lambda^{-1}(H_1) \cap \cdots \cap \pi_\Lambda^{-1}(H_{m+1}) \cap X \neq \varnothing$ so that $R_{X,\Lambda}(H_1, \ldots, H_{m+1}) = 0$. Conversely, if $R_{X,\Lambda}(H_1, \ldots, H_{m+1}) = 0$ then there exists a point $P \in H_1 \circ \pi_\Lambda \cap \cdots \cap H_{m+1} \circ \pi_\Lambda \cap X$, which since $\Lambda \cap X = \varnothing$ implies that $\pi_\Lambda(P) \in H_1 \cap \cdots \cap H_{m+1} \cap \pi_\Lambda(X)$ and hence that $F_{\pi_\Lambda(X)}(H_1, \ldots, H_{m+1}) = 0$. We conclude that $F_{\pi_\Lambda(X)}$ and $R_{X,\Lambda}$ have the same vanishing locus and because the former polynomial is irreducible there must exist some $r \geq 1$ such that

$$R_{X,\Lambda} = F_{\pi_\Lambda(X)}^r.$$

In particular $R_{X,\Lambda}$ is irreducible if and only if $r = 1$. But this is true if and only if $\pi_\Lambda(X)$ has degree d, which as we know holds if and only if $\pi_\Lambda|_X$ is birational onto its image. □

Lemma 5.3. *Using the assumptions and notation from Lemma 5.2, there exists an $(n-m-2)$-plane $\Lambda \in G_X(\mathbb{Q})$ such that*

$$H(\Lambda) \leq ((m+1)^2 d^2)^{n-m-1}(n-m-1)!$$

when considered under the Plücker embedding.

Proof. Consider the rational map

$$\pi : (\mathbb{P}^n)^{n-m-1} \dashrightarrow \mathbb{P}^\nu : (P_1, \ldots, P_{n-m-1}) \mapsto \det(P_1, \ldots, P_{n-m-1})$$

which is well-defined on the open U consisting of tuples of independent points. Observe that $\pi(U) = \mathbb{G}(n-m-2, n)$. By Lemma 5.2 there exists a polynomial F of degree less than $(m+1)^2 d^2$ which vanishes on the complement of G_X but which does not vanish identically on $\mathbb{G}(n-m-2, n)$. The polynomial

$$Q := F\left(\det\begin{pmatrix} x_{10} & x_{11} & \cdots & x_{1n} \\ x_{20} & x_{21} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n-m-1,0} & x_{n-m-1,1} & \cdots & x_{n-m-1,n} \end{pmatrix}\right)$$

is multihomogeneous of multidegree $(\deg(F), \ldots, \deg(F))$ in the $n-m-1$ blocks of $n+1$ variables corresponding to the rows of the displayed matrix. Clearly Q vanishes on the complement of U, while it is

not identically zero because $Q(P_1, \dots, P_{n-m-1}) = F(\pi(P_1, \dots, P_{n-m-1}))$ for any tuple of independent points P_i.

Write

$$Q = \sum_j Q_j(x_{10}, \dots, x_{1n}) R_j(x_{20}, \dots, x_{n-m-1,n})$$

for nonzero Q_j and linearly independent polynomials R_j. Lemma 4.1.1 helps us to find a point $P_1 \in \mathbb{P}^n(\mathbb{Q})$ of height at most $\deg(F)$ such that $Q_1(P_1) \neq 0$. By the linear independence of the R_j one sees that $Q(P_1, x_{20}, \dots, x_{n-m-1,n})$ is not identically zero. Repeating the argument eventually yields a tuple of points $P_1, P_2, \dots, P_{n-m-1}$ of height at most $\deg(F)$ such that $Q(P_1, \dots, P_{n-m-1}) \neq 0$. In particular this tuple of points belongs to U, i.e., they are independent, and $\pi(P_1, P_2, \dots, P_{n-m-1}) \in G_X(\mathbb{Q})$. From this the lemma follows easily. □

Proof of Lemma 5.1. Let Λ be the $\mathbb{Q}$-rational $(n-m-2)$-plane produced by the proof of Lemma 5.3. In particular $\Lambda \cap X = \varnothing$ and $\pi_\Lambda|_X$ is birational onto its image. Then for all $(m+1)$-planes Γ such that $\Gamma \cap \Lambda = \varnothing$ the projection map $p_{\Lambda,\Gamma}|_X$ is also birational onto its image, thanks to the factorization from (5-2).

The proof of Lemma 5.3 moreover shows that Λ can be assumed to be the linear span of rational points $P_1, \dots, P_{n-m-1} \in \mathbb{P}^n$ satisfying $H(P_i) \leq (m+1)^2 d^2 =: B_1$. By Lemma 5.4 below we can find linear forms $L_1, L_2, \dots, L_{n-m-1}$ with integral coefficients whose absolute value is bounded by

$$B_2 := \sqrt{(n-m-2)!(n+1)}\, B_1^{n-m-2}$$

such that L_i vanishes on $P_1, \dots, P_{i-1}, P_{i+1}, \dots, P_{n-m-1}$ but not on P_i. Together these linear forms cut out an $(m+1)$-plane Γ such that $\Gamma \cap \Lambda = \varnothing$. Furthermore

$$p_{\Lambda,\Gamma}(P) = P - \frac{L_1(P)}{L_1(P_1)} P_1 - \cdots - \frac{L_{n-m-1}(P)}{L_{n-m-1}(P_{n-m-1})} P_{n-m-1} \tag{5-4}$$

for all $P \in \mathbb{P}^n \setminus \Lambda$. So we have

$$H(p_{\Lambda,\Gamma}(P)) \leq (n-m)((n+1)B_1B_2)^{n-m-1} H(P) = c d^{2(n-m-1)^2} H(P) \tag{5-5}$$

for some constant c that is easily bounded by an expression purely in n. □

Lemma 5.4. *Let $B, r, s \in \mathbb{Z}_{\geq 1}$ be integers such that $s < r$. Consider a linear system of linearly independent equations $\sum_{k=1}^r a_{ik} x_k = 0$ for $i = 1, \dots, s$, where all a_{ij} are integers satisfying $|a_{ij}| \leq B$. There exists a nonzero tuple of integers $(x_1, x_2, \dots, x_r)$ violating the first equation but satisfying all other equations such that*

$$|x_i| \leq \sqrt{(s-1)!r}\, B^{s-1} \tag{5-6}$$

for all i.

Proof. This follows from [Bombieri and Vaaler 1983, Theorem 2], which strengthens Theorem 3.3.4. It ensures the existence of $r-s+1$ linearly independent tuples of integers $(x_1, x_2, \dots, x_r)$ satisfying the

last $s-1$ equations and meeting the bound (5-6). Since the space of solutions to the full linear system of s equations has dimension $r-s$, at least one of these tuples must violate the first equation. □

We can now prove Propositions 4.3.1 and 4.3.2, reducing the situation of a general variety to a hypersurface.

Proof of Proposition 4.3.2. Let X be a geometrically integral projective variety in $\mathbb{P}^n$ of dimension m and degree d, where we may assume that $n > m+1$. We consider a projection $p_{\Lambda,\Gamma}$ as in Lemma 5.1. By dropping appropriately chosen coordinates, its image X' can be viewed as a hypersurface in $\mathbb{P}^{m+1}$, birational to X and hence also of degree d. In each fiber of $p_{\Lambda,\Gamma}$ there are at most d points. The height relation from Lemma 5.1 now immediately implies

$$N(X, B) \leq dN(X', c_n d^{2(n-m-1)^2} B)$$

for all $B \geq 1$. This proves the claim for $m > 1$. For $m = 1$, consider the normalization $\tilde{X} \to X$ and compose it with the morphism $X \to X'$ induced by $p_{\Lambda,\Gamma}$ to find a resolution of singularities $\tilde{X} \to X'$. The latter map is one-to-one away from the singular points of X', which together have no more than $(d-1)(d-2)$ preimages by [Kunz 2005, Theorem 17.7(b)]. But then the same claims must apply to $X \to X'$, yielding the stronger bound

$$N(X, B) \leq N(X', c_n d^{2(n-2)^2} B) + d^2,$$

as wanted. □

Proof of Proposition 4.3.1. Let X be a geometrically integral affine variety in $\mathbb{A}^n$ of dimension m and degree d, where we may assume that $m < n-1$. Let Z be the projective closure of X in $\mathbb{P}^n$; we apply Lemma 5.1 and shall argue later that we can take the $(n-m-2)$-plane Λ to be contained in the hyperplane $\mathbb{P}^{n-1}$ at infinity. Let $Z' \subseteq \Gamma$ be the image of Z under the projection $p_{\Lambda,\Gamma}$. As above, by dropping some coordinates we can view Γ as $\mathbb{P}^{m+1} = \mathbb{A}^{m+1} \sqcup \mathbb{P}^m$ where $p_{\Lambda,\Gamma}(\mathbb{P}^{n-1} \setminus \Lambda)$ corresponds to $\mathbb{P}^m$. In particular $p_{\Lambda,\Gamma}$ maps X to the affine part $X'_0 = Z' \cap \mathbb{A}^{m+1}$ of Z'.

Consider $P_1, P_2, \ldots, P_{n-m-1}$ and $L_1, L_2, \ldots, L_{n-m-1}$ as in the proof of Lemma 5.1. Let $P \in X$ be a point having integer coordinates; when considered as a projective point of Z its coordinate at infinity is 1. Since the coordinates at infinity of the P_i are 0, the projection formula (5-4) shows that $p_{\Lambda,\Gamma}(P) \in Z'$ admits integer coordinates such that the coordinate at infinity is

$$L_1(P_1)L_2(P_2)\cdots L_{n-m-1}(P_{n-m-1}),$$

regardless of the choice of P. As a consequence, this is a multiple of the denominators appearing among the coordinates of $p_{\Lambda,\Gamma}(P)$ when viewed as an affine rational point of X'_0. Therefore, postcomposing with a coordinate scaling map $\mathbb{A}^{m+1} \to \mathbb{A}^{m+1}$, we obtain another variety X' in $\mathbb{A}^{m+1}$ such that every integral point P of X is mapped to an integral point of X' whose height satisfies the same upper bound as in (5-5). All fibers of this map $X \to X'$ have at most d points, and in the case of curves the map is even one-to-one away from the singular points on X'. So we can conclude as in the proof of Proposition 4.3.2.

It remains to argue why we can take Λ in the hyperplane at infinity. We first claim that the "good set" G_Z from Lemma 5.2 has a nonempty intersection with the Grassmannian parametrizing $(n-m-2)$-planes Λ contained in $\mathbb{P}^{n-1}$. Indeed, it is apparent that the generic such Λ does not intersect the $(m-1)$-dimensional set $Z \cap \mathbb{P}^{n-1}$ and hence satisfies $\Lambda \cap Z = \varnothing$. Furthermore, the argument from [Harris 1992, page 224] showing that generic projections are birational leaves enough freedom to draw the same conclusion when restricting to projections from planes at infinity. More precisely, if $m = n-2$ then it suffices to project from a point outside the cone spanned by Z and some random point $q \in Z$. Since this cone is irreducible of dimension at most $m+1 = n-1$ and since $Z \not\subseteq \mathbb{P}^{n-1}$, the generic point at infinity indeed meets this requirement. If $m < n-2$ then the desired conclusion follows by applying the foregoing argument to $n-m-1$ successive projections from points.

So we can redo the proof of Lemma 5.3 starting from a polynomial F of degree less than $(m+1)^2 d^2$ which vanishes on the complement of G_X but which does not vanish identically on the Grassmannian of $(n-m-2)$-planes that are contained in the hyperplane at infinity; we just argued that such an F exists. Then one can proceed with the same polynomial Q as before, but with zeroes substituted for the variables $x_{10}, x_{20}, \ldots, x_{n-m-1,0}$. □

6. Lower bounds

We conclude with some lower bounds showing that one cannot make the dependence on d subpolynomial. Our main auxiliary tool is the following lemma.

Lemma 6.1. *For each pair of integers $d \geq 1$, $n \geq 2$ there exists an absolutely irreducible degree d polynomial $f \in \mathbb{Q}[x_1, x_2, \ldots, x_n]$ which vanishes at all integral points $(r_1, r_2, \ldots, r_n)$ for which $|r_i| \leq \lfloor (d-1)/2n \rfloor$ for all i.*

Proof. The lemma is immediate if $d = 1$, so we can assume that $d \geq 2$. We claim that there exists a polynomial

$$x_1^d + x_2^d + \cdots + x_{n-1}^d + x_n^{d-1} + \sum_{0 \leq i_1, \ldots, i_n \leq \lfloor (d-1)/n \rfloor} a_{i_1,\ldots,i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

which vanishes simultaneously at the integral points $(r_1, r_2, \ldots, r_n)$ satisfying

$$\left\lfloor \frac{d-1}{2n} \right\rfloor - \left\lfloor \frac{d-1}{n} \right\rfloor \leq r_i \leq \left\lfloor \frac{d-1}{2n} \right\rfloor$$

for all i. From this the lemma follows, because indeed $\lfloor (d-1)/2n \rfloor - \lfloor (d-1)/n \rfloor \leq -\lfloor (d-1)/2n \rfloor$ and because the polynomial is absolutely irreducible, as its Newton polytope is indecomposable; see e.g., [Gao 2001, Theorem 4.11]. To verify the claim, note that every point $(r_1, r_2, \ldots, r_n)$ imposes a linear condition on the coefficients $a_{i_1,\ldots,i_n}$, together resulting in a linear system of $(\lfloor (d-1)/n \rfloor + 1)^n$ equations in the same number of unknowns. It suffices to see that the matrix corresponding to its linear part is nonsingular. But this matrix is the n-th Kronecker power of the Vandermonde matrix $(r^i)_{r,i}$ where r and

i range over

$$\left\{\left\lfloor\frac{d-1}{2n}\right\rfloor-\left\lfloor\frac{d-1}{n}\right\rfloor,\dots,\left\lfloor\frac{d-1}{2n}\right\rfloor\right\}\quad\text{and}\quad\left\{0,\dots,\left\lfloor\frac{d-1}{n}\right\rfloor\right\},$$

respectively. Therefore its determinant is a power of the determinant of this Vandermonde matrix, from which the desired conclusion follows. □

Proof of Proposition 5. If $d=1,2$ then we let X be a line or conic through a coordinate point, respectively, so that we can take $B=1$. If $d\geq 3$ then we consider the affine curve defined by the polynomial f from the proof of the foregoing lemma for $n=2$. Let X be its projective closure, which has an extra height 1 point at infinity. With $B=\lfloor(d-1)/2\rfloor-\lfloor(d-1)/4\rfloor$ one observes that

$$N(X,B)\geq\left(\left\lfloor\frac{d-1}{2}\right\rfloor+1\right)^2+1\geq\frac{d^2}{4}=\frac{d^2}{5}\cdot\frac{5}{4}\geq\frac{d^2}{5}\cdot B^{2/d}.$$ □

Note that using the same f and B one also finds that

$$N_{\mathrm{aff}}(f,B)\geq\left(\left\lfloor\frac{d-1}{2}\right\rfloor+1\right)^2\geq\frac{d^2}{4\log d}B^{1/d}\log B$$

for all $d\geq 3$, confirming our claim that, in the statement of Theorem 3, it is impossible to replace the quartic dependence on d by any expression which is $o(d^2/\log d)$. In arbitrary dimension, the same reasoning shows that there exists a positive constant $c=c(n)$ such that for all integers $d>0$ we can find an absolutely irreducible degree d polynomial $f\in\mathbb{Q}[x_1,x_2,\dots,x_n]$ along with an integer $B\geq 1$ such that

$$N_{\mathrm{aff}}(f,B)\geq cd^2B^{n-2}\quad\text{and}\quad N(X,B)\geq cdB^{\dim X},$$

where $X\subseteq\mathbb{P}^n_{\mathbb{Q}}$ denotes the integral degree d hypersurface defined by the homogenization of f. This shows that Theorems 1 and 4 cannot hold with $e<1$ or $e<2$, respectively.

References

[Bhargava et al. 2020] M. Bhargava, A. Shankar, T. Taniguchi, F. Thorne, J. Tsimerman, and Y. Zhao, "Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves", *J. Amer. Math. Soc.* (online publication August 2020).

[Binyamini and Novikov 2019] G. Binyamini and D. Novikov, "Complex cellular structures", *Ann. of Math.* (2) **190**:1 (2019), 145–248. MR Zbl

[Bombieri and Pila 1989] E. Bombieri and J. Pila, "The number of integral points on arcs and ovals", *Duke Math. J.* **59**:2 (1989), 337–357. MR Zbl

[Bombieri and Vaaler 1983] E. Bombieri and J. Vaaler, "On Siegel's lemma", *Invent. Math.* **73**:1 (1983), 11–32. MR Zbl

[Browning 2009] T. D. Browning, *Quantitative arithmetic of projective varieties*, Progr. Math. **277**, Birkhäuser, Basel, 2009. MR Zbl

[Browning and Heath-Brown 2005] T. D. Browning and D. R. Heath-Brown, "Counting rational points on hypersurfaces", *J. Reine Angew. Math.* **584** (2005), 83–115. MR Zbl

[Browning et al. 2006] T. D. Browning, D. R. Heath-Brown, and P. Salberger, "Counting rational points on algebraic varieties", *Duke Math. J.* **132**:3 (2006), 545–578. MR Zbl

[Burguet et al. 2015] D. Burguet, G. Liao, and J. Yang, "Asymptotic h-expansiveness rate of C^∞ maps", *Proc. Lond. Math. Soc.* (3) **111**:2 (2015), 381–419. MR Zbl

[Cafure and Matera 2006] A. Cafure and G. Matera, "Improved explicit estimates on the number of solutions of equations over a finite field", *Finite Fields Appl.* **12**:2 (2006), 155–185. MR Zbl

[Cluckers et al. 2020a] R. Cluckers, A. Forey, and F. Loeser, "Uniform Yomdin–Gromov parametrizations and points of bounded height in valued fields", *Algebra Number Theory* **14**:6 (2020), 1423–1456. MR

[Cluckers et al. 2020b] R. Cluckers, J. Pila, and A. Wilkie, "Uniform parameterization of subanalytic sets and Diophantine applications", *Ann. Sci. École Norm. Sup.* (4) **53**:1 (2020), 1–42.

[Dèbes and Walkowiak 2008] P. Dèbes and Y. Walkowiak, "Bounds for Hilbert's irreducibility theorem", *Pure Appl. Math. Q.* **4**:4 (2008), 1059–1083. MR Zbl

[Ellenberg and Venkatesh 2005] J. Ellenberg and A. Venkatesh, "On uniform bounds for rational points on nonrational curves", *Int. Math. Res. Not.* **2005**:35 (2005), 2163–2181. MR Zbl

[Gao 2001] S. Gao, "Absolute irreducibility of polynomials via Newton polytopes", *J. Algebra* **237**:2 (2001), 501–520. MR Zbl

[Gautschi 1962] W. Gautschi, "On inverses of Vandermonde and confluent Vandermonde matrices", *Numer. Math.* **4** (1962), 117–123. MR Zbl

[Gelfand et al. 1994] I. M. Gelfand, M. M. Kapranov, and A. V. Zelevinsky, *Discriminants, resultants, and multidimensional determinants*, Birkhäuser, Boston, 1994. MR Zbl

[Harris 1992] J. Harris, *Algebraic geometry: a first course*, Grad. Texts in Math. **133**, Springer, 1992. MR Zbl

[Heath-Brown 1983] D. R. Heath-Brown, "Cubic forms in ten variables", *Proc. Lond. Math. Soc.* (3) **47**:2 (1983), 225–257. MR

[Heath-Brown 2002] D. R. Heath-Brown, "The density of rational points on curves and surfaces", *Ann. of Math.* (2) **155**:2 (2002), 553–595. MR Zbl

[Heintz 1983] J. Heintz, "Definability and fast quantifier elimination in algebraically closed fields", *Theoret. Comput. Sci.* **24**:3 (1983), 239–277. MR Zbl

[Kunz 2005] E. Kunz, *Introduction to plane algebraic curves*, Birkhäuser, Boston, 2005. MR Zbl

[Motte 2018] F. Motte, "On the Malle conjecture and the Grunwald problem", preprint, 2018. arXiv

[Pila 1995] J. Pila, "Density of integral and rational points on varieties", pp. 183–187 in *Columbia University Number Theory Seminar* (New York, 1992), Astérisque **228**, Soc. Math. France, Paris, 1995. MR Zbl

[Pila 1996] J. Pila, "Density of integer points on plane algebraic curves", *Int. Math. Res. Not.* **1996**:18 (1996), 903–912. MR Zbl

[Pila 2010] J. Pila, "Counting rational points on a certain exponential-algebraic surface", *Ann. Inst. Fourier* (*Grenoble*) **60**:2 (2010), 489–514. MR Zbl

[Ruppert 1986] W. Ruppert, "Reduzibilität ebener Kurven", *J. Reine Angew. Math.* **369** (1986), 167–191. MR Zbl

[Salberger 2007] P. Salberger, "On the density of rational and integral points on algebraic varieties", *J. Reine Angew. Math.* **606** (2007), 123–147. MR Zbl

[Salberger 2013] P. Salberger, "Counting rational points on projective varieties", submitted, 2013.

[Salberger 2015] P. Salberger, "Uniform bounds for rational points on cubic hypersurfaces", pp. 401–421 in *Arithmetic and geometry* (Bonn, Germany, 2013), edited by L. Dieulefait et al., Lond. Math. Soc. Lect. Note Ser. **420**, Cambridge Univ. Press, 2015. MR Zbl

[Sedunova 2017] A. Sedunova, "On the Bombieri–Pila method over function fields", *Acta Arith.* **181**:4 (2017), 321–331. MR Zbl

[Serre 1989] J.-P. Serre, *Lectures on the Mordell–Weil theorem*, Aspects Math. **E15**, Vieweg & Sohn, Braunschweig, Germany, 1989. MR Zbl

[Serre 1992] J.-P. Serre, *Topics in Galois theory*, Res. Notes in Math. **1**, Jones and Bartlett, Boston, 1992. MR Zbl

[Vermeulen 2020] F. Vermeulen, "Points of bounded height on curves and the dimension growth conjecture over $\mathbb{F}_q[t]$", preprint, 2020. arXiv

[Walkowiak 2005] Y. Walkowiak, "Théorème d'irréductibilité de Hilbert effectif", *Acta Arith.* **116**:4 (2005), 343–362. MR Zbl

[Walsh 2015] M. N. Walsh, "Bounded rational points on curves", *Int. Math. Res. Not.* **2015**:14 (2015), 5644–5658. MR Zbl

Communicated by Jonathan Pila
Received 2020-02-04 Accepted 2020-04-23

wouter.castryck@kuleuven.be *KU Leuven, imec-COSIC, Leuven, Belgium*
Ghent University, Department of Mathematics: Algebra and Geometry, Ghent, Belgium
raf.cluckers@univ-lille.fr *University of Lille, CNRS, UMR 8524 – Laboratoire Painlevé, Lille, France*
KU Leuven, Department of Mathematics, Leuven, Belgium
philip.dittmann@tu-dresden.de *Technische Universität Dresden, Institut für Algebra, Dresden, Germany*
kien.nguyenhuu@kuleuven.be *KU Leuven, Department of Mathematics, Leuven, Belgium*
Thang Long Institute of Mathematics and Applied Sciences, Hanoi, Vietnam

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2020 is US $415/year for the electronic version, and $620/year (+$60, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 14 No. 8 2020

1937-0652(2020)14:8;1-U